No. _____

IN THE

Supreme Court of the United States

ERIK A. HENTZEN,

Petitioner,

v.

UNITED STATES,

Respondent.

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Sixth Circuit

PETITION FOR A WRIT OF CERTIORARI

Trevor W. Wells
Counsel of Record
REMINGER CO., L.P.A.
707 E. 80th Place, Suite 103
Merrillville, IN 46410
(219) 663-3011
twells@reminger.com

Counsel for Petitioner

QUESTION(S) PRESENTED

Can *Strickland v. Washington*'s "prejudice prong," be satisfied by a showing that constitutionally inadequate representation at the trial-court level "actually had an adverse effect on the defense" because it materially impaired the defendant's prospects of obtaining relief from an error on appeal? More specifically, where Petitioner's direct appeal from a judgment imposing a twenty-year prison sentence for child-pornography offenses resulted in a determination that the district court had erroneously permitted the Government to admit a prejudicial "grooming video," but that the error was harmless in light of what the reviewing court believed to be overwhelming evidence of the Petitioner's guilt, did Petitioner independently satisfy *Strickland* by sufficiently demonstrating that, if his trial counsel had been adequately prepared to expose the objectively false digital-computer-forensics evidence with which the Government inundated the jury, the evidentiary record in connection with which the Sixth Circuit Court of Appeals assessed the trial court's evidentiary-admission error would have been fundamentally different to a degree that "undermine[s] confidence" that the circuit court would have found that error harmless?

PARTIES TO THE PROCEEDING

The caption identifies all parties. No corporate-disclosure statement is required by Sup. Ct. R. 29.6.

STATEMENT OF RELATED CASES

Petitioner Hentzen and his counsel are unaware of any directly related proceedings other than those proceedings appealed here.

TABLE OF CONTENTS

APPENDICES

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner Erik A. Hentzen respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Sixth Circuit in this case.

OPINIONS BELOW

The Sixth Circuit's unpublished opinion (Pet. App. 1a) is at 2023 WL 8629076. The Eastern District of Kentucky's Order and Judgment (Pet. App. 23a, 57a) are also unpublished.

JURISDICTION

The Sixth Circuit issued its judgment on December 13, 2023. Pet. App. 1a. It denied a timely petition for rehearing *en banc* on February 1, 2024. *Id.* 155a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

Petitioner Hentzen's petition involves his rights under the Sixth Amendment to the United States Constitution:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the

> witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defense.

U.S. Const. amend. VI (emphasis added).

STATEMENT OF THE CASE

Trial and Direct Appeal (*Hentzen I*)

Following a jury trial in the United States District Court for the Eastern District of Kentucky, the Petitioner was convicted of receipt and possession of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (a)(4) and was sentenced to 20 years' imprisonment.

Prior to his arrest, Petitioner was a 25-year-old studying business and economics at the University of Kentucky who had a unique, even obsessive, interest in computer technology. In his apartment in Lexington, Kentucky, he owned seven computers and 17 computer-related devices that collectively could store seventeen *terabytes* – or 17,000 gigabytes – of data, *see United States v. Hentzen*, 638 F. App'x 427, 428 (6th Cir. 2015) ("*Hentzen I*") – which was characterized at trial as "almost as much as the Library of Congress holds." Petitioner collected and accumulated extensive music and video files, including a large quantity of legal adult pornography, using, among other means, various peer-to-peer networks, including eDonkey, which he accessed using a software client named eMule. *Id*.

The Kentucky Attorney General's Cyber Crimes Unit monitors peer-to-peer networks searching for persons sharing and distributing child pornography. It uses automated software to search networks for

keywords it associates with child pornography and documents the internet-protocol ("IP") addresses of computers that share files with those keywords and that otherwise match the "digital fingerprints" of known child-pornography files. Between September and November of 2012, one of the Unit's agents discovered that a particular IP address belonging to an unsecured internet router in the apartment of another resident of Petitioner's apartment building had listed as available for sharing a number of files believed to contain child pornography. Although law enforcement was never able to download any file appearing as available from download from that IP address, the files were ultimately traced to a running laptop in Petitioner's apartment. *Id.*[1]

The agents suspected that as many as seven of the thirty recently downloaded files on Petitioner's laptop

---

[1] Although the Cyber Crimes Unit Examiner Bell claimed at trial that, when they executed the search warrant at Petitioner's apartment, he could see downloading activity "on the screen of that laptop when [he] pulled it out and looked at it" – which later became the excuse for the on-site use of software known as OS Triage that the Government contends is the reason for all the post-seizure time-stamp activity that Petitioner's expert in the post-conviction proceedings maintained reflected a breach of foundational evidence-collection protocols and called the integrity of the evidence into question – the photographs taken by the Cyber Crimes Unit reflect that they actually encountered a lock-screen and could not have seen any of the downloading activity they claimed to have seen until after Petitioner voluntarily provided his password to them. None of the lower courts' written analyses addressed this fact – or, for that matter, the fact that, the Cyber Crime Unit's on-scene post-seizure activity on Petitioner's computer system overwrote other time stamps and destroyed potentially exculpatory evidence.

appeared to constitute child pornography. They therefore seized all of Petitioner's computers and devices and submitted them for forensic examination, which the investigators testified at trial located suspected contraband-pornography files, *i.e.*, over six thousand video files and five hundred still images that contained keywords (in their titles or even just in metadata) that the Government's witnesses associated with child pornography. They also found a digital catalogue for child pornography and three copies of an animated virtual video depicting a child engaging in sexual activity with an adult man. *See id.*

At trial, Petitioner stipulated that child-pornography files had been found on his computers and/or devices and that the files had been transported in interstate commerce over the Internet. The only contested issue for trial was the scienter element of the offenses, *i.e.*, whether Petitioner knew that the files contained child pornography when he downloaded and possessed them. *Id.* at 429.

The Government was unable to produce any evidence to show that the Petitioner had ever opened, interacted with, or viewed any of the NCMEC-confirmed child-pornography files located on his computer system (and, in fact, law enforcement's on-scene interaction with Petitioner's computers immediately following their seizure actually destroyed potential exculpatory evidence that would have conclusively shown Petitioner had never viewed the recently-downloaded child-pornography files that the Government introduced as Exhibits 1A – 1D at trial). And, lacking the type(s) of evidence that prosecutors ordinarily use to circumstantially prove a culpable

mental state in child-pornography prosecutions,[2] the Government attempted to satisfy its burden of proof on this dispositive scienter element with circumstantial evidence ostensibly grounded in digital-computer forensics including (1) that two of the files linked to suspicious keywords had been opened in Internet Explorer; (2) that a folder containing some of the files had been opened using a view that would show thumbnails of the videos and images, and (3) a document that represented Petitioner's last 30 searches on eMule, which the Government contended debunked the Petitioner's defense because those terms included commonly found child sexual abuse keywords that the Government maintained had been entered individually by Petitioner. *Id.* at 429.

The Government also developed a trial theme premised upon Petitioner's alleged "deception" and/or attempts to hide his child-pornography downloading,

---

[2] *See, e.g. United States v. Sammons*, 55 F.4th 1062, 1075 (6th Cir. 2022) (confession); *United States v. Muick*, 167 F.3d 1162, 1166 (7th Cir. 1999) (defendant's computer contained a "computer directory called 'Kiddie Porn'"); *United States v. Sheldon*, 755 F.3d 1047, 1050 (9th Cir. 2017) (prior conviction for child pornography); *United States v. Fabiano*, 169 F.3d 1299, 1306-08 (10th Cir. 1999) (five months of trolling Preteen chat room where child pornography images were openly traded). Notably, on appeal, the Government asserted in its brief that Petitioner "frequented websites with a child-pornography connection[,]" but the panel observed that "[n]one of its citations support this statement, and our review of the record reveals no other evidence that Hentzen did so." *Hentzen I*, 638 F. App'x at 432, n.2. Although this was neither the first nor the last time that the Government played fast-and-loose with the facts in its prosecution of Petitioner, to date it is the only time that any court has called the Government out for doing so.

which, in part, rested on a claim that eMule was installed on only one laptop computer they had found "on the keyboard tray, running while closed." *Hentzen I*, 638 F. App'x at 428. The AUSA emphasized this "fact" twice during the Government's opening statement and twice again during its closing. The Government also solicited testimony from its investigator regarding this allegedly lone eMule installation twice more during the presentation of evidence. And when Petitioner himself testified to the contrary and explained that the program had, in fact, been installed on other computers, the Government confronted him on cross-examination with its investigators' "expert" account and testimony about the single installation.

Petitioner testified in his own defense and maintained that he did not know that any of the files he was downloading contained child pornography. *Id.* at 429-30. He explained his belief/theory that the contraband-pornography files must have inadvertently come to be on his computers and devices either (1) when he copied all of the media files on his friends' computers to his hard drives in connection with his business of repairing their computers, or (2) in trawling the Internet and other sources for media files and downloading massive amounts of data unrelated to child pornography, he must have carelessly assembled search terms that cast a net of enormous breadth and ended up unintentionally capturing files containing child pornography. *Id.* at 430.

As to the latter, Petitioner specifically testified that he would visit an adult-pornography website and then visit the "top 100 searches" link, which was essentially a series of specialized, pornography-targeting

keywords, which he would then copy and paste into a text file that he would copy into the eMule search box so that he could download any files that the program told him he did not already have. *See id*. Petitioner testified that he had downloaded at least 100,000 media files – most of which he had never viewed – and that he did not generally look at the file names because he was primarily focused on the sizes of the files located and how quickly he could download them. *Id.* After verifying that files were not corrupted and were virus-free, he would move them to a new folder he had labeled "sorted, seen, keep, good, something of that nature." *Id.* Although Petitioner generally used his own router to download these media files, when there was an issue with his router, his computer automatically connected to the nearest unsecured router. *Id.*

In rebuttal, the Government presented the above-referenced testimony about the last thirty searches and the files that were still in the process of downloading to Petitioner's laptop when it was seized. *Id.* For some of those files, there was no evidence of any other download started at the same time. The examiner opined that those files had been downloaded individually.

Petitioner's motions for a judgment of acquittal at the close of the Government's case and again at the close of all evidence were denied. After approximately five hours of deliberation, the jury returned guilty verdicts on both counts. *Id.*

Petitioner appealed to the United States Court of Appeals for the Sixth Circuit, which was unpersuaded by Petitioner's contention that the evidence was insufficient to support his convictions. More specifically, the panel concluded that, based on the

evidentiary record from trial, which the reviewing court understood as showing that Petitioner "had entered as search terms the names of child pornography studios and the name of a child pornography series," that Petitioner's "internet history showed that two still images of child pornography had been opened in the Internet Explorer browser[,]" and that "evidence from the computer's 'link files' suggested that child pornography files had been opened from his external hard drive," a "rational juror could infer that Hentzen knew that he was receiving child pornography – because he was searching for the names of child pornography studios – and that he knew that he possessed child pornography – because he had viewed it." *Id.* at 431-32.

The Sixth Circuit found, however, that the district court had erred by allowing the Government to introduce, as Fed. R. Evid. 404(b) evidence, an animated "grooming" video depicting non-contraband "virtual" child pornography.[3] Its admission was error primarily because the panel found no "independent evidence that [Petitioner] knew he had the animated video on his computer"[4] After noting that "[w]hether

---

[3] "During the trial, the video was introduced as a 'thing[ ] that would indicate a user's interest in children' and described as a 'grooming video' that would be used 'for grooming small children to accept sexual conduct with adults.' The title of the video, 'New!!Pthlolal—Show This Training Video To Your Daughter To Get Her Ready!!-Hussy,' was also presented to the jury." *Hentzen I*, 638 F. App'x at 429.

[4] The Sixth Circuit recognized that Petitioner's Brobdingnagian-scale digital collection made any usual generalizations about

improperly admitted 404(b) evidence 'substantially swayed' a jury 'generally depends on whether the properly admissible evidence of the defendant's guilt was overwhelming[,]" *Id.* at 435, and referencing the Government's "reliance on evidence that Hentzen knew of the child pornography, including the evidence from his browser history and his search terms," *id.* (emphasis added), however, the panel ultimately concluded "that the erroneous admission of the video did not materially affect the jury's verdict." *Id.*

Petitioner filed a timely petition for rehearing *en banc*, which was denied. Petitioner then unsuccessfully petitioned this Court to grant certiorari. *See Hentzen v. United States*, 577 U.S. 1144 (2016).

Motion to Vacate, Summary Dismissal, and Appeal (Hentzen II)

Petitioner then timely filed a motion under 28 U.S.C. 2255 asking the trial court to vacate the judgment. Among other things, Petitioner argued that his trial counsel was ineffective because of his "failure to properly investigate and sufficiently comprehend the Government's digital computer forensics evidence to permit the defense to subject the prosecution's case to meaningful adversarial testing" (which general contention was further described in four subparagraphs

---

multiple files inapplicable. As such, the fact that three copies of this video were found had little, if any, consequence for the issue of whether Petitioner knew of them because they were just three needles in an enormous haystack. *See Hentzen I*, 638 F. App'x at 433 ("In the context of [Petitioner's] nearly unlimited hard drive capacity, three copies of a file in an unopened folder would be virtually unnoticeable.").

and detailed in more than 100 paragraphs describing trial counsel's specific deficiencies). Petitioner supported his claims with more than 400 pages of argument and attachments,[5] including his own affidavit and the affidavit of Andy Cobb, a defense-retained Ph.D computer scientist expert witness, who opined that "the investigators breached universally accepted procedures of digital forensic data collection and analysis" and "altered the integrity of the evidence after taking custody of Mr. Hentzen's hard drives by, at a minimum, opening and viewing video files on Mr. Hentzen's Sony Vaio computer before creating forensic copies/images of the hard drive" in a manner that "would have changed the last access timestamp of numerous files including the video files themselves." Dr. Cobb's affidavit further explained that (a) the documentation showed "several thousand files with timestamps after 9:15 a.m. on 3/22/2013, suggesting a

---

[5] Although the then-assigned Magistrate Judge admitted to being "confounded" as to the purpose of some of the material contained within the attachments, *United States v. Hentzen*, 2017 WL 11482342, at *13 (E.D. Ky. Sept. 19, 2017), Petitioner had filed voluminous exhibits illustrating flaws in the Government's keyword-association analysis by visually demonstrating his analysis and research showing that the questioned search terms had crossover/non-CSA-associated applications (for example some of the keywords are themselves adult-pornography websites operating on the internet as .info and .com domains, which would have provided a solid answer to the rhetorical question that the AUSA asked at trial about "who is searching for this stuff unless they are looking for child pornography?" (emphasis added)) and that the data accompanying the Cyber Crimes Unit's forensic report reflected a high "false positives" rate, *i.e.*, non-contraband files labeled as suspected child pornography because of keywords attached to them.

variety of activity on the system after the systems were taken into custody by the investigators[,]" (b) the "[i]mproper digital evidence handling calls into question any conclusion made after custodial transfer" because the breaches in protocol were "foundational to reliable forensic conclusions," and (3) that the Government's misstatement of facts related to the Windows XP operating system ("OS"), including on topics such as .lnk files/shortcuts, files allegedly opened in Internet Explorer, and thumbs.db files, "further bring into question the credibility of certain evidence."

After some procedural litigation, including the Government's unsuccessful attempt to have Petitioner's detailed and evidenced § 2255 motion stricken pursuant to a local rule provision governing the length of criminal motions, the Magistrate Judge's recommended that that Petitioner's § 2255 motion be summarily denied without an evidentiary hearing.[6] Over a year later, the district court summarily overruled Petitioner's

---

[6] The Magistrate's recommendation included what amounts to a without-an-evidentiary-hearing factual finding that simply accepted the Government's assertion that it was "impossible[,]"2017 WL 11482342, at *12, for Petitioner's trial counsel to have possessed a copy of the forensic data that was described in both Petitioner's and the Dr. Cobb's affidavits (and which, at evidentiary hearing that actually occurred almost four years later, it was conclusively proven – and tacitly conceded by the Government – trial counsel did actually possess). The Magistrate's Recommendation also otherwise dismissed Petitioner's affidavit as "not credible[,]" *see, e.g.*, *id.* at *21-22 – apparently, in part because the Magistrate Judge was "suspicious" and "leery of specter of abuse" because Petitioner sought relief under § 2255 at the very end of the statutory limitations period. *Id.* at *13 n.4

objections, adopted that recommendation, and refused to issue a Certificate of Appealability. *United States v. Hentzen*, 2018 WL 4705549 (E.D. Ky. Oct. 1. 2018).

The summary denial accomplished little more than delaying by a few years the evidentiary hearing that was objectively always required to resolve the claims in Petitioner's § 2255 motion. After Petitioner sought and obtained a certificate of appealability from the Sixth Circuit, the Government immediately capitulated and agreed that the judgment should be reversed and remanded for an evidentiary hearing, and, shortly thereafter, the Sixth Circuit vacated and remanded. *See Hentzen v. United States*, 2019 WL 13457690 (May 17, 2019) (*Hentzen II*).

Evidentiary Hearing, Denial of Relief, and Appeal (*Hentzen III*)

After some initial procedural wrangling about the scope of the remand, *see* Pet. App. 61a-68a, the planned evidentiary-hearing date in May 2020 was lost to the COVID pandemic, *see* Pet. App. 68a, but commenced eventually commenced over a year later in late August 2021. *Id.*

At the evidentiary hearing, Dr. Andy Cobb, who, at the time of trial was a professor at the University of Louisville – the same city where Petitioner's trial counsel's office was located – testified that he could have testified to all the following at Petitioner's trial:

- The investigating law enforcement officers "mishand[led] the digital forensics evidence that they collected in Petitioner's case and failed to comply with applicable standards as to the best practices for collecting sensitive computer evidence.

As a result, over 3,600 files reflected time stamps indicative of activity after the law enforcement officers seized those computers. Included among those thousands of files were the actual-child-pornography video files that were introduced at trial as the Government's Exhibits 1A, 1B, 1C, and 1D.

- The data from the eMule download-history files, which the Government presented as a rebuttal exhibit at trial and that Investigator Baker told the jury contradicted Petitioner's trial testimony about how he downloaded files in batches, was actually consistent with Petitioner's trial testimony.
- Although he was unable to directly review images of all the relevant hard drives seized from Petitioner's apartment because the Kentucky Attorney General's Office had discarded the ones without contraband before he had an opportunity to view them, the investigators' own forensic report and its supporting documentation flatly contradicted the Government's repeated assertions, in both testimony and when addressing the jury, that eMule was only installed on the one Sony Vaio laptop computer (Comp2) that the Government claimed Petitioner used to used to download contraband pornography. The supporting documentation accompanying that report also showed that eMule had been installed on a third of Petitioner's computers, as well. As such, the Government presented evidence for its "deception" trial theme that "was not correct."
- Investigator Baker's sworn trial testimony that the existence of a .lnk ("link" or "shortcut") file means that a user has opened a file was inaccurate and

"erroneous" because .lnk files can be created in other ways and can be transferred from one computer to another as part of a compressed file such as a .zip file.

- Investigator Baker's testimony at trial that a .jpg file and an .avi file had been viewed and opened on Petitioner's computer was unsound – both because it was based on an erroneous assumption about how files became part of the Internet Explorer history and because of the particular registry settings on Petitioner's computer(s).

Pet. App. 100a-112a.

Petitioner's trial counsel, who did not possess significant personal knowledge of computer-forensics issues when he was retained to represent Petitioner acknowledged that he was aware – including, without limitation, from the Government's expert disclosures – that the Government intended to introduce evidence that Petitioner had interacted with child-pornography files on his computers. Although Petitioner's trial counsel testified regarding his limited recollection of the details of his defense of Petitioner, he acknowledged that, at the time of trial, he did not have any witness prepared to testify to any of the matters to which Dr. Cobb would have testified.

Petitioner himself testified that he was cognizant "[f]rom the second [he] read the search warrant" that digital-forensics evidence would "be the key issue" in this case and repeatedly emphasized that point to his trial counsel and worked extensively prior to trial to prepare demonstrative video exhibits that would have illustrated his batch-downloading process so that the jury could see it and both understand and believe his

contention that "[a]s far as [he] knew, everything that [he] was getting was legal." *See* Pet App. 76a.

Petitioner's appellate counsel testified that the allegation of error regarding the trial court's admission of a "grooming video" was Petitioner's best shot at obtaining a new trial on appeal and further believed that the chances of success hinged, in large part, on how compelling the panel viewed the Government's evidence against Petitioner. Pet App. 150a.

The Government's only witness was a Forensic Examiner/Detective with the Kentucky Attorney General's Office's Cyber Crimes Unit, who was not involved with this particular investigation or prosecution, but opined that the computer files reflecting post-seizure time stamps appeared to be result of the employment of triage software called OS Triage that the Cyber Crimes Unit uses under particular circumstances. Pet. App. 104a-106a.

On February 15, 2022, Magistrate Judge Ingram issued a 70-page *Report and Recommendation*, Pet. App. 59a, that, although subsequently described by the reviewing appellate court as "comprehensive," Pet. App. 3a, did not address at all significant aspects of Petitioner's argument(s), including Petitioner's in-the-alternative *Strickland* prejudice claim that trial counsel's constitutionally ineffective assistance created a jaundiced evidentiary record on appeal that made the trial court's reversible error in admitting the "grooming video" appear harmless. Instead, with regard to the trial IAC claims that remain in litigation, Magistrate Judge Ingram primarily grounded his recommendation that Petitioner's § 2255 motion be denied upon his conclusion, after parsing the language of the COA had

granted in *Hentzen II*, that all the Petitioner's trial-related IAC claims were foreclosed and the evidentiary hearing for which the matter had been remanded, that the Government had agreed was required, and that had been held the previous summer was never actually necessary as to those claims. *See* Pet. App. 114a-116a.

In its alternative discussion of Petitioner's IAC claims, the Magistrate Judge's *Recommendation* astonishingly disclaimed any reliance upon Petitioner's trial counsel's evidentiary-hearing testimony. *See* Pet. App. 99a ("Mr. Pence did not remember much about the events leading up to trial, and the Court does not rely on his testimony."). The Magistrate Judge's *Recommendation* nevertheless concluded that none of trial counsel's multiple failures to challenge the Government's false digital-computer-forensics evidence, individually or collectively, amounted to constitutionally ineffective representation or would have changed the jury's verdict. From Magistrate Judge Ingram's perspective, the Government's "most powerful – and most emphasized – evidence[,]" Pet. App. 129a, was the Government's "keyword" proof, and he concluded that, based upon that evidence, "the jury quite understandably disbelieved [Petitioner's] purported ignorance of the child pornography on his devices." Pet. App. 130a. Despite "assum[ing]" that Examiner Baker's rebuttal testimony was erroneous, Pet. App. 127a – not exactly a huge concession given that the Government never introduced any evidence to contradict Dr. Cobb's testimony or otherwise argued that it was, and it is somewhat troubling that the Magistrate Judge pairs that concession with a rationalization that Examiner Baker had "scrambled to

produce" his rebuttal exhibit and testimony "at the last minute," Pet. App. 127a, which, from Petitioner's perspective, falls well short of a compelling excuse for convicting him with false testimony – and also admitting that the issue "packs more of a punch than the others," Magistrate Judge Ingram apparently failed to appreciate that Petitioner's batch-downloading process testimony, the credibility of which would have been undebatable if the jury had been made aware that it was fully consistent with the forensic data (instead of being falsely told that the date contradicted Petitioner's account), would have substantially blunted the impact of the keyword proof that the Magistrate Judge's circular reasoning believed erased any prejudice from trial counsel's failure to challenge the Government's false rebuttal testimony.

Petitioner filed timely objections to Magistrate Judge Ingram's *Recommendation*. The district court overruled those objections,[7] adopted the *Recommendation* in its entirety, *see* Pet. App. 23a, and

---

[7] Although the *Recommendation* had not addressed the alternative-prejudice argument, the district court itself, which had erroneously allowed the Government to introduce the "grooming video" in the first place, did devote a single, conclusory paragraph to the matter. Asserting that, notwithstanding the Sixth Circuit's citation of precedent describing the strength of the evidence of guilt as the principal factor in the harmless-error determination, "the digital-computer-forensic evidence was only a minor factor in the Sixth Circuit's holding that the error was harmless[,]" the district court contended that it was "not reasonably probable that the appellate court would have decided differently had the defense provided an expert to contest the government's digital-computer-evidence." Pet. App. 42a.

contemporaneously entered judgment in favor of the United States. Pet. App. 57a.

Petitioner pursued a timely appeal to the Sixth Circuit, which affirmed the district court's judgment. Pet. App. 22a. Like the Government itself, which did not endorse the Magistrate Judge's law-of-the-case rationale in its brief, the Sixth Circuit panel also ignored that view. Instead, the panel generally parroted the district-court-level conclusions that Petitioner's trial counsel's failure to contest the Government's substantially objectively false, but nonetheless damning digital-computer-forensics evidence was neither deficient nor prejudicial. The panel's resolution of what it described as the "Battle of the Experts" between Dr. Cobb and the Government's witness clearly erred in misconstruing the substance of much of that testimony, including by putting words in Dr. Cobb's mouth that do not appear in the evidentiary-hearing transcript itself. *See* Pet. App. 13a-15a; *id.*, 18a. Ultimately, the circuit court ran off the rails at the same point the district court did: its conclusion that "[t]he weight of properly admitted evidence in this case is overwhelming[,]" Pet. App. 22a, is expressly premised upon a belief that Petitioner:

> intentionally inserted keywords and phrase that he knew related to child pornography into a search box on a peer-to-peer network, directed the program to search for files that matched those known terms, selected the files to download from a screen that revealed the file names, instructed the computer to download those

> files, and eventually removed them from his incoming folder to other locations.

Pet. App. 22a.

The panel had acknowledged several paragraphs earlier, however, that Petitioner "correctly identifies two instances in which Examiner Baker's trial testimony was incorrect[,]" the second of which was his "assertion that [Petitioner] downloaded some files individually or in small batches of a few files at a time," which "was not supported by [Petitioner's] eMule history, which in fact favored [Petitioner's claim that he mostly batch-downloaded his files in bulk." Pet. App. 20a. The panel's single-conclusory sentence that "whether counsel contended that some, most, or all of [Petitioner's] contraband files were downloaded individually or in batches does not render his performance ineffective[,]" *Id.*, is insufficient – particularly when the purported warrant for that argument is that the keyword evidence was powerful. Given the panel's apparent failure even to comprehend the alternative prejudice argument,[8] it should perhaps be unsurprising that it failed to appreciate how much of a game-changer it would have been to expose Examiner Baker's rebuttal testimony as false, which would not only have shredded any credibility he had as an expert with the jury, but would have supercharged Petitioner's defense by verifying that the downloading process he

---

[8] *See* Pet. App. 21a ("Lastly, [Petitioner] claims that, had his counsel been constitutionally adequate, he would have been able to keep out of the trial record an allegedly prejudicial animated 'grooming video' that he claims was erroneously introduced into evidence." (emphasis added)).

described – in the context of an explanation for why the searched-for-sketchy-keywords argument was bunk – was actually supported by the evidence that the Government claimed disproved it.

Petitioner sought a rehearing *en banc*, which was denied. Pet. App. 155a.

Petitioner now seeks a writ of certiorari.

REASONS FOR GRANTING THE WRIT

This Court has long recognized that a criminal defendant's trial counsel who procedurally defaults an appeal the defendant intended to pursue has acted in a professionally unreasonable manner that amounts to constitutionally inadequate assistance of counsel. *See Roe v. Clores-Ortega*, 528 U.S. 470, 477 (2000). In fact, in the failure-to-pursue-appeal-at-all context, where counsel's deficient performance has caused the defendant to procedurally forfeit his right to even pursue an appeal, prejudice is presumed with no requirement of any showing from the defendant that the forfeited appellate allegations had any merit. *See id.*, 528 U.S. at 484; *Garza v. Idaho*, ___ U.S. ___, 139 S.Ct. 738, 203 L.Ed.2d 77 (2018) (holding that the prejudice presumption applies even when the defendant has signed an appeal waiver).

Although Petitioner's trial counsel did not forfeit entirely Petitioner's right to a direct appeal, counsel's deficient performance in failing to contest the Government's digital-computer-forensics evidence accomplished much the same result by producing a warped and distorted evidentiary record on appeal that turned a proverbial silk purse into a sow's ear, *i.e.*, a winning argument for reversal into harmless error.

Even indulging the Government's and lower courts' Herculean efforts to imagine away the impact that competent counter-force expert testimony about digital-computer-forensics matters would have had at Petitioner's trial, it appears that everyone now agrees and acknowledges that the Government's rebuttal testimony – the last evidence that the jury heard before it began deliberating – was simply and flatly false and incorrect. Contrary to what Examiner Baker swore to in front of the jury, the rebuttal exhibit of eMule download-history files actually supported rather than contradicted Petitioner's explanation about his process of downloading files in batches rather than individually. As such, the Government was relying upon false evidence when the AUSA argued during his closing that the rebuttal exhibit and Examiner Baker's rebuttal testimony showed that Petitioner had been untruthful about his downloading process:

> [P]utting in the search terms is only the first part of the transaction. The second part of the transaction is getting the files you want back. And how do you do that? Select the file, download, select the file, download. Or as the defendant wants you to believe, let me select five, ten, 12 files at a time. But remember from Bill Baker's rebuttal testimony today, he showed you that no, that's not what happened in this case. If he had selected everything on the screen at once, everything would have had the same time stamp. It didn't. That's what the rebuttal evidence was for. Select,

> download, select, download. He was choosing the ones that he wanted.

Pet. App. 128a. The lower courts appear to have overlooked the fact that Petitioner's explanation of his batch-downloading process challenged the Government's foundational assumption that Petitioner would necessarily have been cognizant of CSA-related keywords involved in these searches and downloads. The Government's retort to Petitioner's batch-downloading defense and testimony was to claim that Petitioner was lying about the whole process because, the data showed various downloads had occurred at different times. But, as Dr. Cobb explained, that conclusion is premised upon a methodological flaw and a fundamental misunderstanding of how eMule operates. But, although the Government's evidence on this point was simply wrong and the product of, at-best, its ostensible "expert" witness's ignorance of the subject matter upon which he was opining, the Government got away with it because Petitioner's trial counsel was not prepared to address that testimony.[9]

---

[9] And/or, for reasons Petitioner' trial counsel was unable to explain at the evidentiary hearing, he chose not to follow through with the trial strategy that he and Petitioner had decided upon prior to trial, which involved Petitioner using the demonstrative video exhibits to show the jury how he downloaded material. In fact, although Petitioner's trial counsel testified at the evidentiary hearing that "[t]he whole point was to demonstrate [Petitioner's downloading process] at trial" (emphasis added) and that the "main defense was [Petitioner's] demonstration of how this happened" (emphasis added) and that he was "quite certain" that, at trial, the defense had, in fact, played some of the demonstrative video exhibits that

Contrary to the district court's analysis, this objectively false evidence that the Government introduced without any factual challenge from the defense was a significant part of the exact same evidence that the *Hentzen I* Court referenced as part of what it concluded was "overwhelming" "properly admissible evidence of the defendant's guilt." *Hentzen I*, 638 F. App'x at 435.

It bears mentioning again that whether Petitioner knew that these files downloaded to his computer system contained child pornography was the only element of the charged offenses in dispute at Petitioner's trial. And, notwithstanding the Government's efforts to downplay the significance of the offenses' required culpable mental state with testimony and argument about how the "created date" is "the only date that matters" "when you're talking about a defendant who's charged with receiving child pornography" – which is not only inaccurate, because the data itself is not accessible as of the creation date, but is a notion that turns its back to essentially all of the digital-computer-forensics evidence upon which the Government built its case and which, even more disturbingly, *Hentzen III* appears to have countersigned, *see* Pet. App. at 14a-15a (incredibly

---

Petitioner had prepared, the transcripts reflect that the planned demonstration never took place; none of the video exhibits were played at trial. In fact, unbeknownst to the Petitioner, who only learned that the videos he had spent months preparing would not be utilized when his trial counsel rested at trial, trial counsel had only designated a small portion of those videos pursuant to the trial court's pretrial order and had not even brought a device to trial with which he could review review or play them.

characterizing "the 'created' file dates" as "the only forensic date of importance in a child-pornography case" (emphasis added)) – it is beyond any serious question that, before someone can be found guilty of a child-pornography offense criminalized under 18 U.S.C. § 2252, the defendant must have known that the materials he or she possessed consisted of or contained child pornography. *United States v. X-Citement Video*, 513 U.S. 64, 78 (1994). *See also id.* at 73-74 (observing that "the age of the performers is the crucial element separating legal innocence from wrongful conduct" because, in light of the Court's First Amendment jurisprudence in the obscenity context, "one would reasonably expect to be free from regulation when trafficking in sexually explicit, though not obscene, materials involving adults.").

X-Citement Video understandably focused on construing what Congress meant by its employment of the term "knowingly" in 18 U.S.C. § 2252 to "reflect [its] aim of separating culpable offenders from inadvertent recipients of child pornography." *Child Pornography, The Internet, and the Challenge of Updating Statutory Terms*, 122 Harv. L.R. 2206, 2209 (2009) (hereinafter "*Child Pornography*"). And the circuit courts have accurately construed existing precedent to frame the line of demarcation in cases like this one as that "a person who seeks out only adult pornography, but without his knowledge is sent a mix of adult and child pornography, would not have violated [§ 2252(a)(2)'s prohibition on receipt of child pornography]." *United States v. Myers*, 355 F.3d 1040, 1042 (7th Cir. 2004).

Because technology often evolves more quickly than Congress can respond, however, responsibility for

determining the kind(s) and extent of proof sufficient to infer that a particular defendant had the requisite knowledge falls to the federal courts, which thereby "serve as a backstop protecting innocent defendants in . . . cases where receipt of child pornography was truly inadvertent." *Child Pornography* at 2227. But, in making those determinations, the circuit courts have, on occasion, reached divergent conclusions in evaluating sufficiency-of-the-evidence disputes with regard to evidence and inferences from digital-computer-forensics evidence. *Compare, e.g., United States v. Figueroa-Lugo*, 793 F.3d 179 (1st Cir. 2015) (holding that the trial record adequately supported the jury's rejection of the defendant's "inadvertent download" defense because, from the expert testimony, "a rational jury could have found that, in order to retrieve files with names such as 'porn pthc 9yo Vicki stripping and sucking (kiddie pedo illegal underage preteen)' . . . Figueroa used search terms associated with child pornography [and] then intentionally downloaded the files that the LimeWire network had shared with him in response to those search requests[.]") *with United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011) (reversing the defendant's conviction for knowingly receiving child pornography notwithstanding forensic-analysis evidence that "indicated both that Mr. Dobbs had typed in multiple search terms reflecting the pursuit of child pornography, and that Mr. Dobbs had visited websites consistent with such pornography" because the circuit court found it dispositive "that there was no evidence that Mr. Dobbs actually viewed the charged images, much less clicked on, enlarged, or otherwise exercised

actual control over any of them.")*. See also* Note, Katie Gant, *Crying Over the Cache: Why Technology Has Compromised the Uniform Application of Child Pornography Laws*, 81 Fordham L.R. 319, 322 (2012) (observing that questions about the meaning of "knowing" receipt and/or possession "have divided federal circuit courts, and raise an even greater questions: what does 'knowingly' mean in a technologically advanced day and age?").

In current procedural posture, of course, Petitioner's case is no longer a sufficiency-of-the-evidence matter. And despite the lower courts' repeated attempts to cast or shoehorn Petitioner's alternative-prejudice argument as an attempt to re-litigate a sufficiency challenge, Petitioner's § 2255 motion itself clearly contended exactly what Petitioner has argued at every point of his post-conviction proceedings:

> Absent the above-described ineffective assistance of counsel, the proof at trial would have been reasonably unlikely to persuade a jury to find Mr. Hentzen guilty beyond a reasonable doubt or, alternatively, on appeal the Sixth Circuit Court of Appeals would have been reasonably likely to reverse any conviction because of the erroneous introduction of the non-probative and prejudicial "grooming video," which would not have been found to be harmless error in the face of a properly developed factual record untainted by the ineffective assistance of counsel, which the Court would not have

found to be "overwhelming." (emphasis added).

Petitioner acknowledges that the higher-order thinking that *Strickland*'s prejudice analysis demands can be difficult. And that analysis is especially complex in a context of a case like this one, where conceptualizing what this trial and the evidentiary record would have looked like in a hypothetical world where Petitioner's trial counsel was actually prepared to contest the Government's "expert" testimony[10] instead of what actually transpired, which amounted to showing up to a knife fight not just unarmed, but functionally waiving a white flag. But, even if one concludes that the jury would have returned a guilty verdict even if Petitioner had received constitutionally adequate representation vis-à-vis the digital-computer-forensics evidence,[11] it is plain as day that, on direct

---

[10] *See Hinton v. Alabama*, 571 U.S. 263, 276 (2014) ("[W]e have recognized the threat to fair criminal trials posed by the potential for incompetent or fraudulent prosecution forensics experts. . . . This threat is minimized when the defense retains a competent expert to counter the testimony of the prosecution's expert witnesses.").

[11] To be perfectly clear, Petitioner vehemently disagrees with the lower courts' suggestion that the jury's verdict would not likely have changed if the trial defense had actually confronted the Government's digital-computer-forensics proof. Where not purely tautological and/or conclusory, those rationalizations rest on fundamental misunderstandings of how the evidence interacted. For example, the trumpeting of the significance of the Government's child-sexual-abuse "keyword" proof only supercharges the significance of the rebuttal-testimony fiasco, which, if the jury had heard the truth instead of the falsehoods that

appeal the case would have reached the Sixth Circuit in a radically different form that it historically did. To put

---

the Government fed them, would have substantially challenged if not entirely broken the link between Petitioner and those keywords because that linkage boiled down to an inaccurate assumption that Petitioner individually entered those keywords as search terms. Moreover, the lower courts' no-blood-no-foul apologia fails to appreciate or account for the fatal credibility blows the Government and its witnesses would have taken when the keystone to their "deception" trial theme – that eMule was installed only on what the AUSA characterized in his closing argument as "the deception laptop" – was shown to be categorically untrue as it was abundantly clear from the face of the report prepared by the witness who was testifying otherwise. The prosecution obtained the verdict it did in large part because it was able to leverage an appearance of expertism on the part of its witnesses, who would have been exposed as gold bricks if the jury had learned not only that their evidence-collection procedures were a dumpster fire, but also that that the various opinions expressed by those witnesses about features of the Windows XP OS ranged from indefensibly wrong to at-best incomplete. Stated otherwise, by being unprepared to challenge the Government's witnesses' testimony, the defense allowed them to appear that they knew what they were talking about when they were really just shooting from the hip. The paved pathway to a prejudice determination principally urged in this Petition, however, is simply cleaner because the evidentiary threshold at which the erroneous introduction of prejudicial evidence ceases to be harmless should be well below the point at which courts are willing to accept that an entirely different trial might very well have resulted in a different verdict. As it stands, of course, the question of how the June 2014 jury would have evaluated a properly developed and contextualized evidentiary record as to the digital-computer-forensics proof is one that can never be answered with certainty. And a trial court's preponderance-of-the-evidence prediction is an inferior simulacrum for a jury's own reasonable-doubt determination. *Cf. United States v. Haymond*, ___ U.S. ___, 139 S.Ct. 2369, 204 L.Ed.2d. 897 (2019) (plurality op.).

it simply, the evidentiary record before the reviewing panel would not have contained unchallenged digital-computer-forensics evidence that Petitioner had been intentionally "searching for the names of child pornography studios" or that he had "viewed" "two still images[12] of child pornography" child-pornography files on his computer. *See Hentzen I*, 638 F. App'x at 432. Instead, the circuit court would have been evaluating in the context of a far weaker and more balanced factual record whether the admission of the "grooming video" (and prejudice associated with its implicit but clear suggestion that it reflected pedophiliac inclinations on Petitioner's part) constituted reversible error.

Had Petitioner's trial counsel done the job the Sixth Amendment required him to do, the evidentiary record before the circuit court on direct appeal would have permitted a jury to infer only that Petitioner (a) might have interacted with and/or opened deleted files that might have contained child pornography – because the presence of a "keyword" that law enforcement associates with child sexual abuse in those no-longer-available files is by no means definitive as to its actual content,[13] and (b) utilized such keywords in searches,

---

[12] The fact that the panel referred to a .jpg file and an .avi file (the latter of which is, by definition, a video file) as "two still images" is another object lesson in the extent to which the evidence in this record was never properly contextualized for anyone – jury or jurist.

[13] The Government had, in fact, judicially admitted during the evidentiary hearing that "[f]ile names do not equal content." And the Government's expert witness at the evidentiary hearing similarly acknowledged that "just because a file is named

but not in the individual, "select, download, select, download" manner that the Government claimed. Even though Petitioner's trial counsel unilaterally called an audible that resulted in the jury not seeing the demonstrative videos that would have illustrated Petitioner's downloading process and buttressed his contention that process did not involve his scrutiny of

---

something . . . doesn't necessarily mean that's the content" and that, while "hash value" matching can result in being "pretty certain" about the content, confirming that a file is "in fact, child pornography" will often involve actually viewing it. Unfortunately, Petitioner's trial counsel doubled down on allowing the Government to skew the record by not making sure that the jury was aware of the very inferential nature of the keyword evidence – or that the terms that the Government's witnesses described as "keywords commonly associated with child pornography" also appear in entirely legal, non-contraband contexts, including adult pornography. For example, Petitioner had developed evidence that the Government-identified CSA-affiliated keyword "Lolita," which dates back to the infamous 1950s novel, was and is commonly used in the adult-entertainment industry to market legal pornography depicting young-presenting adult women – and, in fact, actually appeared in the title of an adult-pornography movie, Lolita from Interstellar Space, that aired on an HBO channel in 2013, shortly after the defense received the Forensic Report in discovery. This resulted in a false impression, on the part of the reviewing appellate panel, and no doubt on the less-savvy jury members, as well, that the large file numbers bandied about, including the unconfirmable-content files with which the Government claimed Petitioner interacted in some manner, actually were child pornography instead of merely suspected child pornography. *See, e.g., Hentzen I*, 638 F. App'x at 428 ("The investigators found 6,536 child pornography videos and 554 child pornography images on the various devices, including those files that had been deleted." (emphasis added)). The distinction should have been critical to the jury's reasonable-doubt determination as to Petitioner's knowledge of the content of the files downloaded to his computer system.

search terms or file titles in the manner that the Government's circumstantial proof assumed he did, the Government had no evidence that contradicted Petitioner's account.

Moreover, although the lower courts jumped on OS Triage as a convenient, Mr. Clean Magic Eraser excuse for the post-seizure time stamps, Dr. Cobb stood firmly behind his opinion that "having time stamps an hour and a half after equipment is seized is not handling it properly." (emphasis added). Had Petitioner's trial counsel developed comparable evidence to challenge the evidence-collection procedures, it would have ignited a firestorm at trial that, at a minimum, would have placed in dispute all the Government's digital computer forensics evidence that, in reality, went untouched at trial. The lower courts' hasty generalization(s) that this criticism would have been marginalized by the Government's OS Triage explanation ignores – literally, given that none of the lower courts ever addressed it – the fact that the story about seeing downloading activity on the laptop screen, which was the purported justification for employing OS Triage, was based on testimony flatly contradicted by photographs taken during the search warrant's execution. And cross-examination of the Government's convenient OS Triage excuse would have further chipped away at the Government's witnesses thin-at-best veneer of expertism not only because "triage" is only coherent when decisions are being made about which devices to seize (which was not a question here because they seized them all, and were always going to seize the laptop on which they ran OS Triage) but also by exposing other breaches of evidence-collection protocol,

including turning on devices that had been powered down, which the Government's evidentiary-hearing expert acknowledged was always a no-no, and judging from the fact that one of Petitioner's seized laptops was never forfeited and the Cyber Crimes Unit has offered no explanation for where it ended up, apparently at-best "misplacing" some of the evidence they seized.

In any event, the record contains not a shred of evidence to support even the suggestion that there might have been some "opportunity cost" to challenging the evidence-collection procedures at trial that might have constituted reasonable strategy underlying Petitioner's trial counsel's unexplained decision not to challenge the digital-computer-forensics evidence. Even if the jury was for some reason ultimately skeptical of the challenge to the Government's evidence-collection procedures, presenting the evidence to them would have been fully consistent with whatever the defense actually presented was supposed to be, which Petitioner's trial counsel was unable to explain and/or seemed to believe was something far different from what actually happened in the Lexington courtroom in June 2014. Conspicuously absent from any of the decisions below is any articulation as to how it could ever have been reasonable trial strategy in this case to show up at the courthouse unprepared to contest the prosecution's expert testimony as to how the data on the Petitioner's computers proves he is guilty. Petitioner easily clears *Strickland*'s requirement of showing a reasonable probability of a different result. Juxtaposing the erroneous introduction of the "grooming video" with an evidentiary record that might be sufficient to get past a sufficiency challenge at the motion-for-judgment-

of-acquittal stage, but cannot, in any intellectually honest universe be described as "overwhelming" substantially forecloses the harmless-error labeling it received when the record on direct appeal inaccurately portrayed the strength of the Government's case against Petitioner.

The evidentiary record developed below during the post-conviction proceedings conclusively shows that Petitioner's trial counsel did nothing to prepare to defend Petitioner against the Government's digital-computer-forensics evidence that he knew the Government would introduce. Despite acknowledging the relevant goalposts, *see, e.g.*, App. Pet. 13a; *id.*, 70a, none of the lower courts has ever even attempted to articulate how trial counsel's performance satisfied foundational "well-defined norms" of practice as reflected in the American Bar Association standards, which, quite simply, should and do demand more than occurred here. *See, e.g. Padilla v. Kentucky*, 559 U.S. 356, 366-67 (2010). Merely observing that *Strickland*'s deficient-performance standard is rigorous and that hindsight should be avoided and fast-forwarding to a not-good-enough conclusion is not enough to drag Petitioner's trial counsel's non-performance over the constitutional bar. The Sixth Amendment's guarantee would be meaningless if a cursory investigation and doing less-than nothing[14] at trial to defend against the

[14] Petitioner describes it as "less-than nothing" because Petitioner's trial counsel not only failed to prepare a defense to the Government's digital-computer-forensics evidence – apparently deciding instead to simply ignore that evidence existed. He also

Government's principal evidence on the only element in dispute can be declared constitutionally adequate.

Certiorari in this case would not only permit this Court to examine the "knowingly" culpable mental state it correctly found applicable to child-pornography in *X-Citement Video* in the new light of technologies that have replaced the dominant pornography mediums in the decades since Congress criminalized the receipt and possession of child pornography in order to provide some clarity and direction for law enforcement as to the type and quantity of evidence necessary to show a proper inferential link between a defendant and files found on a computer network. Moreover, given the procedural posture of Petitioner's case – where a circuit court previously found an evidentiary-introduction error on direct appeal, but found that error to be harmless in the context of the evidentiary record before it, which record was the product of a constitutionally ineffective representation of trial, this case would also serve as a perfect vehicle for the Court to speak to what appears to be a first-impression context of *Strickland's* prejudice prong novel enough that the lower courts substantially side-stepped it.

CONCLUSION

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

---

figuratively chucked Petitioner's own preparatory work out the window when he unilaterally, and without any advance warning, jettisoned the plans to demonstrate Petitioner's process and innocence to the jury.

Respectfully submitted,

Trevor W. Wells
Counsel of Record
REMINGER CO., L.P.A.
707 E. 80th Place, Suite 103
Merrillville, IN 46410
(219) 663-3011
twells@reminger.com

Counsel for Petitioner

May 1, 2024.