No. _____

In the

Supreme Court of the United States

Christopher Waguespack,

Petitioner,

v.

United States of America,

Respondent.

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

Petition for Writ of Certiorari

Samuel H. Winston
Counsel of Record
Kara A. Larson
The Law Office of Sam Winston
1700 Josephine Street
New Orleans, LA 70113
504-577-2500 (telephone)
504-577-2562 (facsimile)
sam@samwinstonlaw.com

QUESTIONS PRESENTED

I. Whether failing to call the law enforcement agent responsible for generating a computer report in the Government's case-in chief implicates the Sixth Amendment when the defendant is prevented from cross-examining the Government's witness about whether the software was running properly, and what information the agent put into the program.

II. Whether there is sufficient evidence to support convictions for possessing and distributing child pornography when the only illicit files found on a defendant's computer are either deleted or inaccessible.

PARTIES TO THE PROCEEDING

Petitioner is Christopher Waguespack, who was Defendant-Appellant in the court below. Respondent is the United States of America, who was the Plaintiff-Appellee in the court below.

STATEMENT OF RELATED PROCEEDINGS

1. *United States of America v. Christopher Waguespack*, No. 3:16-CR-58-1 in the United States District Court for the Middle District of Louisiana. Mr. Waguespack was convicted on October 19, 2017, and sentenced on June 26, 2018.
2. *United States of America v. Christopher Waguespack*, No. 18-30813 in the United States Court of Appeals for the Fifth Circuit. Judgment was entered on August 15, 2019.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Authorities

PETITION FOR WRIT OF CERTIORARI

Petitioner Christopher Waguespack seeks a writ of certiorari to review the judgment of the United States Court of Appeals for the Fifth Circuit.

OPINIONS BELOW

The opinion of the Court of Appeals is located within the Federal Reporter at *United States v. Waguespack*, 935 F.3d 322 (5th Cir. 2019), and reprinted as Appendix A to this Petition. The district court's judgment and sentence are attached as Appendix B to this Petition.

JURISDICTION

The panel opinion and judgment of the Fifth Circuit were entered on August 15, 2019. This Honorable Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This Petition involves the federal statutes prohibiting the distribution or possession of child pornography, to wit: the Confrontation Clause of the Sixth Amendment; 18 U.S.C. § 2252A(a)(2); and 18 U.S.C. § 2252A(a)(5)(B).

The Confrontation Clause of the Sixth Amendment states:

"In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . ."

U.S. Const. amend. VI.

18 U.S.C. § 2252A(a)(2) provides for the punishment of:

"Any person who knowingly receives or distributes any child pornography using any means or facility of interstate or foreign commerce or that has been mailed,

or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer."

18 U.S.C. § 2252A(a)(2).

Finally, 18 U.S.C. § 2252A(a)(5)(B) provides for the punishment of:

"Any person who knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer."

18 U.S.C. § 2252A(a)(5)(B).

STATEMENT OF THE CASE

Louis Ratcliff, a former investigator with the Louisiana State Police, was terminated after Mr. Waguespack's arrest and before his trial. Mr. Ratcliff was the lead investigator in this case. He authored the search warrant, and he bore responsibility for running and maintaining software called Torrential Downpour. However, Mr. Ratcliff did not testify at Mr. Waguespack's trial.

Reports from Torrential Downpour were crucial for Mr. Waguespack's conviction for distribution of child pornography. The reports from Torrential Downpour purportedly showed logs of file transfers containing child pornography coming from Mr. Waguespack's computer to Mr. Ratcliff's computer from March 29, 2015, and March 30, 2015. There was no other evidence that distribution occurred on these dates. In fact, Government witnesses were subsequently unable locate the files shown in the Torrential Downpour reports on Mr. Waguespack's computer.

A search using Torrential Downpour may be initiated by law enforcement or by automated process. Without the ability to cross-examine Mr. Ratcliff, Mr. Waguespack was unable to ask questions about the methodology of testing, preservation of evidence against him, the version of Torrential Downpour used by Mr. Ratcliff, whether Mr. Ratcliff used Torrential Downpour correctly or incorrectly, or whether Mr. Ratcliff properly maintained, calibrated, or updated his version of Torrential Downpour.

Mr. Ratcliff bore responsibility for running and maintaining Torrential Downpour and authoring the search warrant in this case, but the jury never heard

from Mr. Ratcliff. Instead, the Government used the testimony of another law enforcement agent, who had no first-hand knowledge of Mr. Ratcliff's use of Torrential Downpour in this investigation, to introduce reports from Torrential Downpour. This other law enforcement agent was used to lay the foundation for the Torrential Downpour reports and certify the results as accurate—despite finding no corroborating evidence of distribution on the dates in the reports on Mr. Waguespack's computer.

Moreover, the only files containing child pornography used as evidence against Mr. Waguespack at his trial were either deleted, cached, or both cached and deleted. No user-accessible files containing child pornography were ever found on Mr. Waguespack's computer. Mr. Waguespack's convictions rested on: (1) file pathways indicative of child pornography; (2) evidence tending to show an interest in child pornography; and (3) assumptions about an encrypted portion of a hard drive that was never opened before or after trial. There was also evidence that Mr. Waguespack knew how to use a computer and possessed more computer knowledge than his mother, but the Government did not establish that Mr. Waguespack was a computer expert. Although no child pornography was found that Mr. Waguespack could access, Mr. Waguespack was convicted of both knowing distribution and knowing possession of child pornography.

Mr. Waguespack appealed his convictions and sentences to the Fifth Circuit Court of Appeals for the United States, which had jurisdiction under 28 U.S.C. § 1291.

The Fifth Circuit affirmed Mr. Waguespack's convictions and sentences on August 15, 2019.

REASONS TO GRANT THIS PETITION

I. This Honorable Court should clarify the contours of the Sixth Amendment for reports that are produced by a combination of machine and human input.

"Perhaps the final frontier in law's reliance on machine conveyances of information is the full automation of the act of witnessing."[1]

The Sixth Amendment guarantees the right to all accused to confront the accusers against them. U.S. Const. amend. VI. Previously, indicia of reliability was sufficient to render an out-of-court statement admissible. *See Ohio v. Roberts*, 448 U.S. 56, 66 (1980). However, this Court subsequently recognized that the true exercise of one's right to confront the accusers against them requires that evidence be tested in "the crucible of cross-examination." *Crawford v. Washington*, 541 U.S. 36, 61 (2004). The reach of *Crawford* was expanded to exclude test results when there is a certification by an analyst that the test was accurately performed. *Bullcoming v. New Mexico*, 564 U.S. 647, 659-62 (2011).

Unfortunately, the holdings of *Crawford* and *Bullcoming* left open one increasingly prevalent method of shielding evidence from the requirements of the Sixth Amendment: reliance on so-called "machine-generated evidence." *See id.* at 673-74 (Sotomayor, J., concurring in part). Implicit in sanctioning this shield is the notion that machines and programs cannot and should not be subject to cross-examination

[1] Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 2021 (2017).

because they are inherently more reliable than humans. Roth, *supra* at 1989, ("Some courts and scholars assume that 'machines . . . fall outside the scope of hearsay because the hearsay problems of perception, memory, sincerity and ambiguity have either been addressed or eliminated.'") (internal quotation marks, footnotes, and citations omitted). In the same way that a fingerprint cannot be cross-examined, a machine-generated report cannot be cross-examined. This logic implies that a report either establishes a fact or it does not.

However, this position misrepresents the reliability of machine-generated data. There are a number of issues that must be examined before certifying a result as reliable. *See* Roth, *supra* at 1990-2000. Was the machine designed properly? Was there proper maintenance of the machine? Did the machine run properly? What level of input did the operator have on the machine? Was the operator able to confirm that the machine's results were accurate?

For example, breathalyzer machines, which are widely used and accepted as reliable, are not so reliable after all. *See* Stacy Cowley & Jessica Silver-Greenberg, *These Machines Can Put You in Jail. Don't Trust Them*, NY Times (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html (improper calibration of breathalyzer machines led to results "that were at times 40 percent too high"). If an accused is prevented from cross-examining the operator of a machine, then there is no way to test whether the machine's report is sufficiently reliable. This does not lead to increased confidence in or the efficiency of the criminal justice system; in fact, it leads to just the opposite. *See Cowley*, *supra* (reporting that

42,000 convictions are at risk in Massachusetts and New Jersey because of issues with breathalyzer machines).

The software used in this case—Torrential Downpour—is not immune from questions about its reliability. Jack Gillum, *Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned*, ProPublica (Apr. 3, 2019), https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned. In addition to Mr. Waguespack's case, there are at least two other cases in which the child pornography purportedly identified by Torrential Downpour was not found on the accused's computer. *Id.*

In this case, Mr. Waguespack was prevented from learning whether the Torrential Downpour report was the result of an automated process or Mr. Ratcliff's actions. Mr. Waguespack was unable to ask Mr. Ratcliff whether Torrential Downpour was properly calibrated and maintained; he was unable to learn which version of software Mr. Ratcliff used. Moreover, Mr. Ratcliff was terminated from his employment after Mr. Waguespack's arrest. And the Government had to change the dates in the indictment after realizing that Mr. Ratcliff listed the wrong dates in his report and affidavit in support of a search warrant. These would otherwise be fertile grounds for cross-examination.

Instead, caselaw currently suggests that evidence need only be run through a computer to avoid the necessity of cross-examination. This is an increasingly digital world. It is not hard to imagine that as more and more investigative processes are automated that the need for live testimony will be largely dispensed with unless this

Court takes action on this important issue. Therefore, Mr. Waguespack respectfully requests that this Honorable Court grant this Petition for review of the Fifth Circuit's decision affirming his convictions and sentences.

II. This Honorable Court should resolve the circuit split over how to establish intent in a child pornography case in which all of the illicit files are cached or deleted.

This Honorable Court should grant certiorari to resolve the circuit split over how to satisfy the element of intent in a prosecution involving child pornography when the only illicit files found are all inaccessible or deleted. R. 10. Currently, the same evidence, which results in a conviction in one circuit, would be insufficient to support a conviction in a different circuit.

The Fifth Circuit previously acknowledged the difficulty in determining whether and how to impute knowledge when illicit files are inaccessible. *United States v. Winkler*, 639 F.3d 692, 696 (5th Cir. 2011) (citing *United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011); *United States v. Bass*, 411 F.3d 1198 (10th Cir. 2005); *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002); *United States v. Pruitt*, 638 F.3d 763 (11th Cir. 2011); *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006); *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006); *United States v. Stulock*, 308 F.3d 922 (8th Cir. 2002)). This difficulty has led to divergent opinions about how best to establish the intent element when all of the illicit files found are inaccessible.

The Third Circuit uses a four-factor test to determine whether there is sufficient evidence to establish the intent element when no images are found in a

user-accessible portion of a computer: (1) whether the images were found on the defendant's computer, (2) the number of images of child pornography found, (3) whether the content of the images was evidence from their file names, and (4) the defendant's knowledge of and ability to access the storage area for images. *United States v. Miller*, 527 F.3d 54, 67 (3d Cir. 2008) (citing *United States v. Irving*, 452 F.3d 110, 122 (2d Cir. 2006); *United States v. Payne*, 341 F.3d 393, 403 (5th Cir. 2003); *United States v. Romm*, 455 F.3d 990, 997-1001 (9th Cir. 2006); *United States v. Kuchinski*, 469 F.3d 853, 861-63 (9th Cir. 2006)).

The Fourth Circuit has yet to officially weigh in, but in an unpublished, per curiam decision, the Fourth Circuit indicated that intent could be established if there was evidence that the defendant attempted to delete a computer's temporary files and browsing history. *United States v. Myers*, 560 Fed.Appx. 184, 186 (4th Cir. 2014) (unpublished) (per curiam).

In *United States v. Stulock*, the Eighth Circuit noted without opining that "The district court explained that one cannot be guilty of possession for simply having viewed an image on a web site, thereby causing the image to be automatically stored in the browser's cache, without having purposely saved or downloaded the image." *United States v. Stulock*, 308 F.3d 922, 925 (8th Cir. 2002).

The Ninth Circuit does not allow mere assumptions to be used to establish the intent element. *See United States v. Kuchinski*, 469 F.3d 853, 861 (9th Cir. 2006). Instead, the intent element may be established by (1) evidence that the defendant is a sophisticated computer user; and (2) evidence that (a) the defendant tried to access

cached files, or (b) the defendant actually knew that the illicit images were in the cache. *Id.*

The Tenth Circuit's requirements resemble those found in the Ninth Circuit. *See United States v. Dobbs*, 629 F.3d 1199, 1204 (10th Cir. 2011). The Tenth Circuit has held that intent is not established unless there is evidence of either (1) access to images in the cached portion of the hard drive, or (2) the defendant's knowledge of the computer's automatic caching function. *Id.*

In contrast to the test established by the Ninth Circuit, a conviction based on assumptions is allowed in the Eleventh Circuit. *See United States v. Pruitt*, 638 F.3d 763, 766 (11th Cir. 2011). If a defendant is in a district court in the Eleventh Circuit, then the intent element may be established in the case against him or her through evidence that the defendant sought out child pornography and that the computer contains child pornography—no matter where the child pornography is located on the computer. *Id.* at 766-67. Therefore, less evidence is required for a conviction in the Eleventh Circuit as compared to the Third, Fourth, Eighth, Ninth, or Tenth circuits. *Compare Pruitt*, 638 F.3d at 766-67 *with Miller*, 527 F.3d at 67; *Myers*, 560 Fed.Appx. at 186; *Stulock*, 308 F.3d at 925; *Kuchinski*, 469 F.3d at 861; *Dobbs*, 629 F.3d at 1204.

Using a hypothetical will help demonstrate the difference in the circuit tests. Take a case in which the Government's evidence solely consists of inaccessible files containing child pornography and search history indicative of an interest in child

pornography. Under the test used in the Ninth Circuit,[2] the accused would be acquitted because there is no evidence showing that the accused is a sophisticated computer user or knew that the inaccessible files were on the computer. *See Kuchinski*, 469 F.3d at 861. However, if the same evidence is presented during a trial at a district court in the Eleventh Circuit, the accused would be convicted because the evidence shows that the accused sought out child pornography and the computer contains child pornography. *See Pruitt*, 638 F.3d at 766-67. The accused may or may not be convicted in the Eighth Circuit, which appears to condone a conviction regardless of an accused's knowledge of automatic caching as long as the accused purposefully sought out child pornography. *See Stulock*, 308 F.3d at 925.

The Fifth Circuit affirmed Mr. Waguespack's conviction on the basis that Mr. Waguespack used a peer-to-peer file sharing software that notified users when file-sharing was occurring, that the computer was under Mr. Waguespack's exclusive use and control, that Mr. Waguespack had an interest in child pornography, that Mr. Ratcliff downloaded child pornography from Mr. Waguespack's computer,[3] that Mr. Waguespack had advanced technological proficiency, and that there were 2,800 images found on the seized computer.[4] Instead of addressing whether Mr. Waguespack had specific knowledge of the deleted and inaccessible images—which

[2] A similar result is obtained in the Third, Fourth, and Tenth circuits.
[3] Of course, Mr. Ratcliff was not called to testify in the Government's case-in-chief. *See* Section I, *supra*.
[4] As noted, all of the images found were cached, deleted, or cached and deleted.

all of the images were—the Fifth Circuit determined that the evidence was sufficient for a finding of dominion and control.

The application of the test for sufficient evidence of intent in this instance seems more analogous to the tests of the Eighth or Eleventh Circuits than the Third, Fourth, Ninth, or Tenth circuits. *See, supra*, for discussion of the different tests and elements thereof. There was no finding that Mr. Waguespack possessed particular knowledge of or access to the cached and deleted files as would be required in the majority of the other circuit courts that have considered the issue. There was no finding that Mr. Waguespack was home to witness notifications from the file-sharing program that files were being shared on the dates alleged in the indictment. Instead, the Fifth Circuit relied on assumptions about Mr. Waguespack's computer usage and interest in child pornography to sustain his conviction.

These disparate results based on the same evidence necessitate this Court's intervention. R. 10. This Honorable Court should exercise its discretionary jurisdiction to resolve the important question of what evidence is necessary to establish the intent element of a prosecution involving child pornography. If discretionary jurisdiction is not exercised, then similarly situated defendants in different district courts will continue to face incongruous results.

CONCLUSION

Petitioner respectfully submits that this Court should grant *certiorari* to review the judgment of the United States Court of Appeals for the Fifth Circuit.

Respectfully submitted this13th day of November, 2019.

/s/ Samuel H. Winston
Samuel H. Winston
Counsel of Record
Kara A. Larson
The Law Office of Sam Winston
1700 Josephine Street
New Orleans, LA 70113
504-577-2500 (telephone)
504-577-2562 (facsimile)
sam@samwinstonlaw.com