No. _____

IN THE
SUPREME COURT OF THE UNITED STATES

ANTHONY ESPINOSA GONZALES,

Petitioner,

v.

UNITED STATES OF AMERICA

Respondent.

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

PETITION FOR A WRIT OF CERTIORARI

JON M. SANDS
Federal Public Defender

* DANIEL L. KAPLAN
Assistant Federal Public Defender
850 West Adams Street, Suite 201
Phoenix, Arizona 85007
(602) 382-2700
* *Counsel of Record*

Date Sent by Federal Express Overnight Delivery: May 7, 2024

QUESTION PRESENTED

Did the court of appeals' ratification of the use of computer-generated evidence to convict petitioner represent a clear departure from the requirements of Federal Rule of Evidence 901(b)(9)?

RULE 14.1(b) STATEMENT

(i) All parties to the proceeding are listed in the caption.

(ii) The petitioner is not a corporation.

(iii) The following are directly related proceedings: *United States v. Gonzales*, No. 17-cr-01311-DGC (D. Ariz.) (judgment entered November 24, 2021); *United States v. Gonzales*, No. 21-10362 (9th Cir.) (judgment entered February 7, 2024).

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes & Rules

Other

Petitioner Anthony Espinosa Gonzales respectfully requests that a writ of certiorari be issued to review the judgment of the United States Court of Appeals for the Ninth Circuit entered on February 7, 2024. App. A.

OPINIONS BELOW

The court of appeals' memorandum is designated Not for Publication, but is available at 2024 WL 466757 and 2024 U.S. App. LEXIS 2822.

JURISDICTION

The United States District Court for the District of Arizona had jurisdiction over the federal criminal charges against Mr. Gonzales pursuant to 18 U.S.C. § 3231. The judgment of the United States Court of Appeals for the Ninth Circuit was entered on February 7, 2024. App. A at 1. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

PERTINENT RULE

Federal Rule of Evidence 901 provides, in pertinent part, as follows:

Rule 901. Authenticating or Identifying Evidence

> **(a) In General.** To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.
>
> **(b) Examples.** The following are examples only—not a complete list—of evidence that satisfies the requirement:
>
> * * *
>
> **(9) Evidence About a Process or System.** Evidence describing a process or system and showing that it produces an accurate result.
>
> * * *

STATEMENT OF THE CASE

At the time of the investigation underlying this case, in late 2016 and early 2017, Petitioner Anthony Espinosa Gonzales was a teenager. He lived with his mother and stepfather in a modest home in Surprise, Arizona, a city northwest of Phoenix. He attended school and worked various minimum-wage jobs. Mr. Gonzales did reasonably well in school, but faced bullying from classmates who considered him a "nerd."

Unbeknownst to Mr. Gonzales, or his mother and stepfather, an FBI computer program called Torrential Downpour was during this period conducting a cyber-investigation that would eventually bring law enforcement to their front door. The investigation took place in the virtual environment of the BitTorrent network—a legal, popular protocol by which computers share files over the internet. The essential purpose underlying the creation of the BitTorrent network was to improve upon the highly inefficient one-to-one method of file-sharing that had been used by earlier services, such as Napster. BitTorrent improved upon this model by allowing files to be shared in pieces, and between multiple computers simultaneously. Through the BitTorrent network, a single computer looking for a file can collect pieces from multiple other members of the network simultaneously, allowing the complete file to be assembled more quickly and reliably.

In the language of the BitTorrent network, a "torrent" is not an actual file, but rather a set of instructions that tell a computer that is part of the network how

to locate all of the pieces of a particular file. The computer then uses the torrent to locate and download the pieces from other computers in the network.

One of the most popular programs used to share files over the BitTorrent network is uTorrent—a widely available program that is free and easy to download and use. The uTorrent program allows a computer on the BitTorrent network to download files, piece by piece, from multiple other computers in the network simultaneously. In addition, the program enables the receiving computer to share the pieces it has received with other computers on the network even as it continues to receive pieces of the file itself, such that the computer is simultaneously collecting and distributing the same content.

Torrential Downpour is a version of uTorrent that the government developed for the purpose of conducting cyber-investigations into such matters as the sharing of child porn over the BitTorrent network. The program functions essentially the same as uTorrent, but with some modifications. One such modification is that unlike uTorrent, which is designed to collect pieces of a file from multiple other computers simultaneously, Torrential Downpour is designed to collect pieces of the file from a single device at a time. To accomplish this, the program interacts with a single Internet Protocol (IP) address—a code assigned to identify an internet user at a specific physical address. Another significant difference is that, while uTorrent and Torrential Downpour both include a logging feature, Torrential Downpour's logging function is automatic, mandatory, and designed to keep thorough records of a cyber-investigation for the purpose of being used in a later prosecution. Also

unlike uTorrent, Torrential Downpour does not share the files that it downloads with other computers.

In late 2016 and early 2017, while being used by Special Agent Jimmie Daniels, an agent at the Phoenix FBI Office and member of the Internet Crimes Against Children Task Force, Torrential Downpour reported that it had identified an IP address associated with Mr. Gonzales' home as having been involved in searches for torrents believed to be associated with child pornography. The program went on to produce logs indicating that, on eight dates between December 13, 2016 and January 9, 2017, it had requested and received seventeen video files and eight image files containing child pornography from this IP address.

On February 8, 2017, a group of law enforcement agents executed a search warrant at Mr. Gonzales' home. In Mr. Gonzales' bedroom, under a mattress, they found a Microsoft Surface—a small tablet-style computer. The government later claimed that its forensic examination of the tablet confirmed that Mr. Gonzales had used it to download and distribute child pornography. The government charged Mr. Gonzales with eight counts of distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2), (b)(1), and 2256, and one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2256.

The government's key evidence at trial was generated by computers, rather than by humans. Because Agent Daniels had passed away from complications relating to a training injury shortly before trial, this material was introduced through Robert Erdely, a detective with the Indiana County, Pennsylvania District

Attorney's Office who testified that he had been involved in the development of the Torrential Downpour program, and FBI Special Agent Patrick Cullen, a computer forensic examiner.

Detective Erdely introduced and interpreted the logs that Torrential Downpour had generated in the investigation, telling the jury that they showed child pornography being distributed from an IP address associated with Mr. Gonzales' house to an FBI computer at specified dates and times.

Agent Cullen testified regarding forensic analyses he had conducted of the tablet using several different types of software, some of which he identified and some of which he did not. Agent Cullen testified:

- that he began his analysis by using an unidentified "software" to create a "mirror image" of the contents of the tablet;
- that he then used a process he did not name or describe to "burn[]" the "mirror image" "onto a hard drive," and then proceeded to conduct his analysis on "the copy of the copy" produced by these two processes;
- that screen shots from the copy of the "mirror image" of a hidden file called "AppData" indicated that Mr. Gonzales had downloaded the torrent files underlying Counts 1 through 8;
- that reports generated from the copy of the "mirror image" by a program called "Forensic Tool Kit," as well as a "forensic tool" called "FTK Imager," showed that the files underlying Count 9 were stored in the "Deadpixel" folder on the tablet;

- that a screen shot from the copy of the "mirror image" indicated that Mr. Gonzales had taken measures to hide the Deadpixel folder; and
- that reports generated from the copy of the "mirror image" by a program called "Internet Evidence Finder" confirmed the times and dates shown in Torrential Downpour log reports, purportedly showing the files underlying Counts 1 through 8 being distributed to the FBI—and also showed "jump lists" and "LNK files" indicating that the files underlying most of the distribution counts had been opened around the time they were being distributed to the FBI computer.

During the course of these two witnesses' testimony, as computer-generated evidence was being introduced, Mr. Gonzales' counsel repeatedly objected on the grounds of foundation, hearsay, authentication, and confrontation. The district court summarily overruled virtually all of these objections. The jury convicted Mr. Gonzales on all counts, and the district court sentenced him to 132 months in custody, followed by a lifetime term of supervised release.

Mr. Gonzales appealed his convictions to the United States Court of Appeals for the Ninth Circuit. Mr. Gonzales' lead claim on appeal was that the district court erred in overruling his numerous authentication and foundation objections to the introduction of computer-generated evidence through Detective Erdely and Agent Cullen, because the government failed to produce adequate evidence describing the processes underlying its computer-generated evidence and showing that they produced accurate results. The court of appeals rejected this claim (along with Mr.

Gonzales' other claims) in an unpublished memorandum, reasoning in conclusory fashion that the testimony of Detective Erdely and Agent Cullen "adequately explained the reliability" of the processes underlying this evidence. App. A at 2.

REASON FOR GRANTING THE WRIT

The court of appeals' ratification of the government's use of computer-generated evidence at Mr. Gonzales' trial represented a clear departure from the requirements of Federal Rule of Evidence 901(b)(9).

The court of appeals' conclusion that the government adequately authenticated the computer-generated evidence that it employed to convict Mr. Gonzales represents a clear departure from the authentication requirement set forth in Federal Rule of Evidence 901(b)(9), which requires that evidence generated by a process or system be authenticated by evidence "describing" the process or system and "showing that it produces an accurate result."

The investigation that led to Mr. Gonzales' prosecution was carried out largely by computers. Torrential Downpour identified an IP address associated with Mr. Gonzales' home as possibly having been involved in distributing child pornography, and generated reports appearing to show that the child porn underlying the first eight counts in the indictment was distributed from that IP address to an FBI computer. Other programs produced reports purporting to show that the tablet found under Mr. Gonzales' mattress had distributed the files underlying the distribution counts, that he had opened (most of) those files before or during their distribution, and that the tablet contained the child porn files underlying the possession count. Most of the trial was taken up with government

witnesses Patrick Cullen and Robert Erdely laying the foundation for the admission of these reports and interpreting their incriminating implications—over Mr. Gonzales' repeated authentication and foundation objections.

The district court erred in overruling those objections.

Objections citing authentication and foundation implicate Federal Rule of Evidence 901, which requires the proponent of evidence to "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). Subpart (b)(9) of Rule 901 specifies that evidence about a process or system may be authenticated by evidence "describing" the process or system "and showing that it produces an accurate result." Subpart (b)(9) "typically is employed to authenticate evidence generated by a mechanism rather than a witness." 31 Victor J. Gold, *Federal Practice & Procedure* (FPP) § 7114 (West, Westlaw through April 2023 Update); *see also United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1110 (9th Cir. 2015) ("when faced with an authentication objection, the proponent of Google–Earth–generated evidence would have to establish Google Earth's reliability and accuracy") (*citing*, *inter alia*, Rule 901(b)(9)).

The extent of the foundation required to authenticate computer-generated evidence depends on, among other factors, "the complexity of the computer processing" involved. 5 *Weinstein's Federal Evidence* § 900.06[3] (Matthew Bender & Co., Inc. 2024) (Weinstein). "[W]hen a computer is tasked with a complex job, for example, creating a simulation or complicated model, a more elaborate foundation is needed to show its reliability." *Id.* Thus, the foundation required to authenticate

computer output that transforms or evaluates data "must both describe the process or system in question and circumstances demonstrating why the result of that process or system is accurate." FPP § 7114. "[T]his foundation may include proof that (1) the type of device in question is accepted as reliable and as suitable for generating the sort of data offered in evidence, (2) the specific device in question was in good working order at the time it generated the data at issue, and (3) the individual that operated the device was competent to do so." *Id.* (footnotes omitted).

Although there is no per se rule that a computer programmer or other expert witness must testify in order to authenticate computer-generated evidence, *U-Haul Int'l Inc. v. Lumbermens Mut. Cas.*, 576 F.3d 1040, 1045 (9th Cir. 2009), the authenticating witness must be competent to establish the system's reliability and accuracy. *Lizarraga-Tirado*, 789 F.3d at 1110; *In re Vee Vinhee*, 336 B.R. 437, 448 (9th Cir. B.A.P. 2005). The authenticating witness cannot establish that competence by merely testifying that he regularly uses the system, without also identifying the basis for his conclusion that it is reliable and accurate. *See*, *e.g.*, *Zayre Corp. v. S.M. & R. Co.*, 882 F.2d 1145, 1149 (7th Cir. 1989) (expressing doubt that affidavit of witness who was identified as company's controller, but was not shown to be familiar with computer system that produced reports of payments to employees, was adequate to authenticate reports); *Lyngaas v. Curaden AG*, No. 17-10910, 2019 WL 6210690, at *11–*12 (E.D. Mich. Nov. 21, 2019), *judgment entered*, 436 F. Supp. 3d 1019 (E.D. Mich. 2020), *aff'd*, 992 F.3d 412 (6th Cir. 2021) (testimony of witness who routinely relied on fax machine summary report logs, but was not shown to

have personal knowledge of process or accuracy of logs, held inadequate to authenticate logs). Thus, although it is not a hard and fast requirement, "[b]ecause Rule 901(b)(9) evidence commonly is the product of some sophisticated machine or process, this foundation often is established through expert testimony." FPP § 7114.

The testimony of Detective Erdely and Agent Cullen regarding Torrential Downpour, the "mirror image" and copying process applied to the tablet, Forensic Tool Kit, and Internet Evidence Finder, does not meet this standard. It is clear that these programs undertook "complex" and "sophisticated" operations to generate the evidence that appeared to confirm Mr. Gonzales' distribution and possession of the charged files. *Weinstein* § 900.06[3]; FPP § 7114. But the closest the record comes to providing a foundation for the conclusion that these programs operated reliably and accurately in this investigation is a handful of largely conclusory opinions to that effect by Detective Erdely and Agent Cullen—proffered with little or no explanation of their methodology or basis. *See* Ct. App. Excerpts of Record at 575–76 (Erdely testifying that he and "students" conducted unidentified "different various validation testing" of Torrential Downpour "at the conclusion of our classes"); *id*. at 576–77 (Erdely testifying that he had no information of "any issues" with Torrential Downpour, and that it was "functioning properly," in the investigation—in which he did not participate); *id*. at 577–78 (Erdely testifying that the Torrential Downpour log files were "formatted" appropriately, "looked correct," and included nothing "unusual"); *id*. at 804 (Cullen testifying that he knew Forensic Tool Kit to be reliable and accurate, and that its presence on the "approved tool list" indicated

that it passed through unidentified testing and validation at FBI headquarters); *id.* at 813 (Cullen testifying that he knew Forensic Tool Kit to be reliable and accurate); *id.* at 823 (same); *id.* at 846–47 (Cullen testifying that he "kn[e]w" Internet Evidence Finder "to be accurate").

These conclusory opinions are inadequate to satisfy Rule 901. *See Zayre Corp.*, 882 F.2d at 1149; *Lyngaas*, 2019 WL 6210690, at *11–*12; *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 545–46 (D. Md. 2007) (authenticating witness for electronically stored information must provide more than "boilerplate, conclusory statements"); *Vee Vinhee*, 336 B.R. at 447 & n.9 (records custodian's "vague" and "conclusory" attestation that computer system that generated monthly credit card statements was "highly accurate" held inadequate to authenticate statements); *compare United States v. Espinal-Almeida*, 699 F.3d 588, 610–13 (1st Cir. 2012) (foundation for GPS-generated maps could have been "better" but was not "obvious error," where authenticating witness was forensic scientist who had been specially trained with respect to GPS devices and who provided detailed explanation of how device worked and how he had verified its accuracy).

The inadequacy of these attestations is especially apparent in light of the fact that the government neither had these witnesses qualified as experts, nor disclosed their opinions and the bases for them prior to trial under Federal Rule of Criminal Procedure 16. Given the complexity of the computer operations in question, the opinions expressed by Detective Erdely and Agent Cullen effectively amount to lay opinions on matters requiring "scientific, technical, or other specialized

knowledge"—which is prohibited by Federal Rule of Evidence 701. Fed. R. Evid. 701(c); *see United States v. Figueroa-Lopez*, 125 F.3d 1241, 1244–46 (9th Cir. 1997) (district court violated Rule 701 by permitting government to elicit lay opinion testimony that defendant's conduct conformed to methods and techniques of experienced drug dealers).

In short, the court of appeals' ratification of the use of computer-generated evidence to convict Mr. Gonzales represented a clear departure from the requirements of Rule 901(b)(9).

CONCLUSION

For the reasons set forth above, the Court should grant the petition for a writ of certiorari and reverse the judgment of the court of appeals.

Respectfully submitted on May 7, 2024.

JON M. SANDS
Federal Public Defender

s/*Daniel L. Kaplan*
*DANIEL L. KAPLAN
Assistant Federal Public Defender
850 West Adams Street, Suite 201
Phoenix, Arizona 85007
(602) 382-2700
* *Counsel of Record*