NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 16-3365

UNITED STATES OF AMERICA

v.

JAVIER PEREZ,
Appellant

On Appeal from the United States District Court
for the Eastern District of Pennsylvania
(D.C. No. 2-14-cr-00611-001)
District Judge: Honorable Jan E. DuBois

Argued May 10, 2017

Before: AMBRO, RESTREPO, and COWEN, *Circuit Judges*.

(Filed: October 18, 2017)

Keith M. Donoghue, Esquire (Argued)
Brett G. Sweitzer
Leigh M. Skipper
Federal Community Defender Office
For the Eastern District of Pennsylvania
Suite 540 West – Curtis Center
601 Walnut Street
Philadelphia, PA 19106

Counsel for Appellant

Louis D. Lappen, Esquire
Robert A. Zauzmer
Albert S. Glenn (Argued)
Office of the United States Attorney
615 Chestnut Street, Suite 1250
Philadelphia, PA 19106

Counsel for Appellee

OPINION*

RESTREPO, *Circuit Judge.*

Javier Perez appeals from his conviction of possession of child pornography, arguing that the initial motion to suppress evidence recovered in a general search of his computer was denied in error, and that the Government's presentation of child pornography evidence at trial—although Perez offered to stipulate to every element except identity—unduly prejudiced the jury. For the reasons that follow, we will affirm.

I

Because we write for the benefit of the parties, we set out only the facts necessary for the discussion that follows. In October 2013, an FBI agent discovered a user of a common peer-to-peer file-sharing network sharing a video of child pornography. The FBI subsequently subpoenaed the user's internet service provider for the account information corresponding to the internet protocol ("IP") address in question, and discovered that the account belonged to Perez, located at a residence in Philadelphia.

* This disposition is not an opinion of the full Court and, pursuant to I.O.P. 5.7, does not constitute binding precedent.

Using the child pornography that the agent had discovered being shared by a user at that IP address, the FBI obtained a warrant authorizing a search and seizure of all computer equipment at that physical address.

In executing the warrant, the FBI discovered that five people lived in the residence, including an individual who repaired computers out of the home. Among the five residents and the computer repair business, the home contained 130 computers and digital storage items, all of which the FBI seized. The only items ultimately found to contain child pornography came from the basement in which Perez resided.

To guide the subsequent human-conducted search of the desktop computer recovered from Perez's basement space, a forensic team duplicated the computer's hard drive, then ran software that scanned the entire drive and catalogued all of its contents by file type. The scan checked for mismatches of file extensions and file contents—e.g., assessing whether an image file had been saved in a .doc format to obscure its true content—and also checked images against databases of known child pornography. Agents used the results of the forensic scan to guide a human search of web browsing history, email, photos and videos, and files specifically identified as pertaining to missing and exploited children. The human search involved some limits; with respect to emails, for example, agents looked at metadata first and subsequently looked at message content if the metadata prompted additional questions. With respect to pictures and videos, agents looked at thumbnails first and then viewed expanded versions if the thumbnail seemed to involve responsive material. The human search, however, included an

inspection of the entire web history, including browsing, search queries, bookmarks, and social media usage.

Having discovered a number of images and videos of child pornography, as well as internet browsing and search history that indicated the user of the computer had sought out such images, the Government charged Perez with numerous offenses. In advance of trial, he indicated that he planned to dispute only the identity of the person who had engaged in the conduct at issue—noting that, because the basement did not even have a door, anyone could have accessed the computer—and offered to stipulate to all non-identity elements of the crimes, including that the media files were sexually explicit and contained minor children. The Government declined the stipulation, and presented child pornography to the jury after the District Court overruled Perez's objections on the basis of undue prejudice. The jury ultimately convicted Perez of possession, but not distribution.

II[1]

The Fourth Amendment prohibits "[g]eneral warrants" that would allow "exploratory rummaging in a person's belongings." *Andresen v. Maryland*, 427 U.S. 463, 479 (1976) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). To guard against such general warrants, courts require "particularity," which "prevents the seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927). Particularity has three components: "First, a warrant must identify

[1] We have jurisdiction under 28 U.S.C. § 1291.

the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Third, the warrant must specify the items to be seized by their relation to designated crimes." *United States v. Galpin*, 720 F.3d 436, 445-46 (2d Cir. 2013) (citations omitted). Ultimately, the particularity requirement intends that "nothing is left to the discretion of the officer executing the warrant." *Marron*, 192 U.S. at 196.

Courts—including our own—have struggled to adapt Fourth Amendment search doctrines designed for physical spaces to digital contexts. *Riley v. California*, 134 S.Ct. 2473, 2493 (2014). Adapting the particularity requirement to searches of digitally stored information presents one example of that problem. For one thing, the place to be searched encompasses much more information in a search of digital storage than in one of physical space, which appears to allow the plain view exception to undercut the warrant requirement. Putting all information on a digital storage device that can hold data "roughly equal to 16 billion thick books," *United States v. Ganias*, 824 F.3d 199, 218 (2d Cir. 2016), in plain view whenever law enforcement officers have a valid warrant to search for something that may exist in the storage substantially expands the aggregate quantity of material encompassed by the exception. Conversely, because of individuals' ability to "hide, mislabel, or manipulate files," *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011), "there may be no practical substitute for actually looking in many (perhaps all)" files and locations during a search of digital storage. *Id*. at 239.

To the extent that some courts have tried to address this tension, results have been mixed. In 2009, the Ninth Circuit issued an en banc opinion with five principles to guide

Magistrate Judges in issuing or approving warrants for digital storage spaces. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc) ("*CDT II*"). Notably, the Ninth Circuit reissued the opinion about a year later as a per curiam opinion, which differed little except that it moved the guidance protocols to a (non-binding) concurrence. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam) ("*CDT III*"); *id.* at 1179-80 (Kozinski, C.J., concurring). As a result, subsequent Ninth Circuit panels have upheld broad warrants authorizing searches of all of a target's digital storage devices and media despite the "absence of precautionary search protocols." *United States v. Schesso*, 730 F.3d 1040, 1043 (9th Cir. 2013).

Rejecting an attempt to jettison the plain view exception in the digital storage context, the Seventh Circuit "simply counsel[s] officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described." *United States v. Mann*, 592 F.3d 779, 786 (7th Cir. 2010). The Sixth Circuit has described computer searches as a "unique problem," but it has declined to impose "a specific search protocol," instead applying "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis." *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011). The Tenth Circuit has suppressed incriminating digital evidence of child pornography discovered by an agent searching a computer for evidence of drug sales, declining to apply the plain view exception to the contents of digital files (as opposed to the files themselves). *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999).

Two years later, however, the same Court declined to suppress child pornography discovered by an agent who "proceeded to rummage through the hard drive for more images of child pornography despite the fact that he did not possess a warrant to conduct such a search," because it was "persuaded the search was reasonable." *United States v. Walser*, 275 F.3d 981, 987 (10th Cir. 2001).

Factual circumstances often complicate the problem. Often, as here, the initial search is undertaken by a computer program rather than a human. Searches of digitally stored data often implicate the rights of other individuals not included in the warrant—which happens more often and to more people with the increased prevalence of cloud storage. Leaving aside the intermingling of responsive and non-responsive data of a named individual, cloud storage often intermingles the data of an individual named in the warrant with the data of an individual not even under suspicion. *See CDT III*, 621 F.3d at 1166; *see also Richards*, 629 F.3d at 552 (6th Cir. 2011) (Nelson Moore, J., concurring in the judgment); *see also Schesso*, 730 F.3d at 1049.

Federal courts have yet to strike a tenable doctrinal balance between protecting the constitutional rights of criminal suspects whose digital storage law enforcement agents intend to investigate and the practical challenges facing those same agents seeking specific information in the proverbial digital haystack. Neither has Congress struck a statutory balance nor the Executive branch via regulation. We do not attempt to do so today.

* * *

We "review[] the District Court's denial of a motion to suppress for clear error as to the underlying factual findings and exercise[] plenary review of the District Court's application of the law to those facts." *United States v. Perez*, 280 F.3d 318, 336 (3d Cir. 2002). In the absence of statutes and doctrine that better address rapidly evolving technology, the manner of searching digital storage is circumscribed by objective reasonableness rather than specific search protocols. *Stabile*, 633 F.3d at 239.

Here, Perez did not argue that the law enforcement agents exceeded the scope of the warrant, nor could he have. Unlike cases of agents exceeding the scope of a warrant authorizing a search for evidence of one type of criminal activity by rummaging for evidence of other types of activities, the warrant here specifically described the target of the search. Perez did not argue even that the initial computer scan—by which law enforcement agents preliminarily scanned the entire contents of the hard drive—was unreasonable. Instead, he merely argued overbreadth as to the execution of the warrant, and would have preferred that the agents searched the digital storage in a particular order. As the agents stayed within the scope of the warrant and employed a search protocol guided by an initial scan whose propriety Perez does not dispute, the District Court did not err in denying the motion to suppress.

III

Perez, as noted, also disputes the District Court's decision to allow the Government to present graphic evidence of child pornography to the jury. We review a District Court's determination after engaging in a Rule 403 balancing for abuse of discretion. *United States v. Sampson*, 980 F.2d 883, 886 (3d Cir. 1992). Perez argues

that, because he disputed only identity, the Government's refusal to accept his stipulation and presentation of child pornography amounted to undue prejudice. Recent precedent forecloses this line of argument. "The government is entitled to prove its case free from a defendant's preference to stipulate the evidence away." *United States v. Finley*, 726 F.3d 483, 492 (3d Cir. 2013). *Finley* arose in the same factual circumstances as here—a defendant in a child pornography case offered to stipulate to all elements except identity—and is binding on subsequent panels. Perez himself recognizes this, allowing that "precedent of this Court is presently to the contrary," Appellant's Br. at 18, and merely asks to preserve the issue for certiorari or collateral review. Perez may consider the issue preserved, and we affirm the District Court.

IV

For the foregoing reasons, we will affirm the District Court's denial of Perez's motion to suppress and its decision to allow the Government to present evidence of child pornography at trial.