In the

United States Court of Appeals

For the Seventh Circuit

No. 23-1010

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DENY MITROVICH,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 1:18-cr-00789-1 — **Gary Feinerman**, *Judge*.

ARGUED NOVEMBER 29, 2023 — DECIDED MARCH 12, 2024

Before RIPPLE, SCUDDER, and JACKSON-AKIWUMI, *Circuit Judges*.

SCUDDER, *Circuit Judge*. A sprawling multinational investigation resulted in the indictment of Deny Mitrovich, a Chicago native, for possessing child pornography. To mount a defense, Mitrovich sought technical information about the software program that Australia and New Zealand had used to identify his computer. The United States did not have that information and, despite repeated efforts, was not able to

obtain it. Even so, Mitrovich asserts that the government was duty bound to produce the requested information under Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure and the Due Process Clause of the Fifth Amendment. The district court disagreed. So do we. Because Rule 16 does not impose an obligation to produce documents held exclusively by foreign authorities and because Mitrovich has failed to prove either suppression or prejudice under *Brady v. Maryland*, 373 U.S. 83 (1963), we affirm.

I

A

In 2014 the Federal Bureau of Investigation began investigating a child-pornography website called The Love Zone. It existed on the dark web, a collection of unindexed pages that cannot be accessed through traditional search engines. To visit the site, a user needed a particular software program called a TOR browser that conceals their IP address—a digital identifier of the accessing device and local network. By routing encrypted data through multiple servers, TOR browsers enable users to navigate the internet without disclosing their identity or location. Or so Deny Mitrovich thought.

A few months into its investigation, the FBI learned that someone in Australia was administering The Love Zone using physical servers in the Netherlands. The Bureau alerted Australian and Dutch authorities, who seized the server and arrested the administrator. Australia and New Zealand then secured the administrator's cooperation, which allowed them to infiltrate and run the website themselves.

Over the summer of 2014, the two Oceanian authorities worked alongside international counterparts to identify and

arrest Love Zone users. U.S. agents provided assistance by extracting data from copies of the server, compiling databases, sharing leads, and issuing subpoenas at the request of foreign allies.

By November 2014, Australia and New Zealand developed a technique to pierce the anonymity provided by TOR browsers. Impersonating the administrator of The Love Zone, they posted a message advertising a new child pornography video. The message contained a hyperlink. When users clicked on it, the link prompted them to stream a file from an external website on Windows Media Player. Anyone who did so unknowingly revealed their IP address.

Australia and New Zealand forwarded the FBI any IP addresses belonging to networks in the United States. The Bureau then traced them to physical addresses. One belonged to the defendant Deny Mitrovich. Law enforcement obtained a warrant to search Mitrovich's home, which yielded hard drives containing troves of child pornography.

B

In November 2018, a grand jury indicted Mitrovich for possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).

From the start, Mitrovich's defense options were limited. Authorities had caught him in the act of streaming child pornography and had uncovered hundreds of unlawful images in his home. To avoid conviction, he needed to suppress this damning evidence.

But Mitrovich had a problem. To exclude evidence obtained from his hard drives, he needed to prove that the unmasking technique that had led to their discovery was an

unconstitutional search. Yet the Fourth Amendment generally does not prohibit unreasonable searches conducted entirely by foreign governments. See *United States v. Stokes*, 726 F.3d 880, 890 (7th Cir. 2013). And New Zealand and Australia had deployed the unmasking technique without U.S. involvement.

To overcome this hurdle, Mitrovich had to show that the Oceanian countries had launched the unmasking technique as part of a joint investigation with the United States. That way the Fourth Amendment would apply to their conduct. See *id.* at 890–91 (holding that the Fourth Amendment applies to a foreign government's extraterritorial search of a U.S. citizen when conducted pursuant to a joint operation with U.S. agents).

Mitrovich also had to show that the unmasking technique amounted to a "search" within the meaning of the Fourth Amendment. This required demonstrating that the Oceanian authorities had violated his reasonably held expectation of privacy. See *Katz v. United States*, 389 U.S. 347, 351 (1967). Without knowing how the unmasking technique worked, that was a tall order. It was made taller by our precedent, which has established that a person has no reasonable expectation of privacy in their IP address because they voluntarily share it with third parties while browsing the internet. See *United States v. Caira*, 833 F.3d 803, 809 (7th Cir. 2016).

Mitrovich insisted that he never voluntarily shared his IP address, even when he clicked on the baited hyperlink. He claimed that, once clicked, the hyperlink operated to install malware that forced his computer to broadcast its IP address without Mitrovich making any decision to do so. But all along

the Oceanian governments consistently denied using malware.

Needing evidence to support his theory, Mitrovich asked the government in discovery to produce all documents related to the unmasking technique. The government declined to make any production, explaining that the technique at issue has been deployed by foreign governments operating in an undercover capacity.

Mitrovich then moved to compel the production of all "information regarding the software used to unlawfully seize [his] IP address" and "any and all communications between the government and [the Oceanian agencies]." He maintained that the information was essential for him to succeed on his motion to suppress and, by extension, to develop a defense to the child pornography charges.

The district court granted the motion. It observed that Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure requires the government to produce documents after only a preliminary "showing that the requested items are material to [the] defense." See *United States v. Thompson*, 944 F.2d 1331, 1341 (7th Cir. 1991). The district court found it at least "plausible" that a joint investigation had existed between the United States and Oceanian governments and that the latter had installed malware on Mitrovich's computer. Because the district court "could not reject outright the possibility that the exclusionary rule would require suppression of evidence," it ordered the government to produce all responsive discovery "subject to any targeted objections to the production of specific material."

The government responded by producing hundreds of additional documents, including email communications about the unmasking technique between FBI and Oceanian agents, screenshots showing the technique in action, and a five-page "Technique Overview" created by New Zealand law enforcement.

The government also sought more specific details about the software program. But Australian and New Zealand officials refused to provide additional information. One former Australian law enforcement agent shared little more than "some vagaries" about the program. And a New Zealand official stated that domestic law prohibited him from disclosing any information at all.

Unsatisfied, Mitrovich filed a motion for discovery sanctions. He argued that by not disclosing more detailed information about the unmasking technique, the government had violated its disclosure obligations under Rule 16(a)(1)(E) and the Supreme Court's decision in *Brady v. Maryland*. More specifically, Mitrovich contended that the newly produced documents left unanswered whether the unmasking technique had deployed malware onto his computer, attaching an affidavit from a computer forensics expert in support. In his sanctions motion, Mitrovich also claimed for the first time that malware might have permitted a third party to download child pornography onto his hard drives—effectively setting him up.

To be sure, Mitrovich acknowledged that the U.S. government lacked access to the technical information he sought. Still, he insisted that the government be held responsible for its failure to produce because it necessarily had *constructive*

possession over the requested information by participating in a joint international investigation.

The district court declined to issue sanctions. Because the COVID-19 pandemic prevented a full evidentiary hearing on the matter, the court assumed without explicitly finding that Oceanian authorities had deployed the unmasking technique pursuant to a joint investigation with the United States. Even so, it determined that the government's failure to disclose the requested information violated neither Rule 16 nor *Brady*. Indeed, the district court found that the prosecution had already produced all responsive documents in its possession and concluded that it had "no obligation to turn over materials that it [did] not have and [could not] obtain through good faith, diligent efforts."

Mitrovich now appeals the denial of his sanctions motion, alleging independent violations of Rule 16 and *Brady*.

II

A

Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure requires the government to disclose documents within its "possession, custody, or control" that are "material to preparing the defense." District courts may enforce this rule through any "order that is just under the circumstances." See Fed. R. Crim. P. 16(d)(2)(D). We review a district court's decision whether to impose sanctions for abuse of discretion, reversing only if it was unreasonable. See *Collins v. Illinois*, 554 F.3d 693, 696 (7th Cir. 2009). In doing so, we embrace the factual findings supporting the district court's decision unless they are clearly erroneous. See *United States v. Carmack*, 100 F.3d 1271, 1276 (7th Cir. 1996) ("Clear error review means that

the district court's decision will not be reversed unless after reviewing the entire record we are left with a definite and firm conviction that a mistake has been committed.").

With admirable candor, Mitrovich again concedes that the U.S. government does not actually possess the technical information he seeks. The district court went further, finding that the prosecution was unable to access the information. That conclusion finds firm support in the record.

The government did not succeed in obtaining the technical information sought by Mitrovich. But not for lack of trying. In early 2014 FBI agents expressed unfamiliarity with the unmasking protocol, requesting a more thorough explanation for how it worked. They repeated their requests in December 2014, asking Oceanian officials for details on the technique several times without receiving an answer. U.S. officials made another unsuccessful entreaty during a visit to New Zealand in March 2016. Four years later, the United States renewed its overtures again but received little more than a high-level summary of how the unmasking technique worked.

These diligent but failed efforts permit only one conclusion: the U.S. government lacked the capacity to obtain the requested information by any reasonable means. On this record, we cannot conclude that the information fell within the government's "possession, custody, or control," as required by Rule 16.

Mitrovich presses a contrary position. In the context of a joint international investigation, he contends that it is not enough to simply find that one member did not hold a document. We should also ask whether the partners they closely collaborated with had possession.

Aligned with the district court, we assume without deciding that the United States, New Zealand, and Australia participated in a joint international investigation. We also assume—again simply for the sake of resolving this appeal—that the Oceanian countries deployed the IP-unmasking technique as part of that investigation. Mitrovich's Rule 16 claim fails nonetheless.

Like our sister circuits, we have declined to extend prosecutors' Rule 16 disclosure obligations to information outside the possession of the federal government. See *United States v. Hamilton*, 107 F.3d 499, 509 n.5 (7th Cir. 1997), *cert. denied*, 521 U.S. 1127 (1997) (explaining that "Rule 16(a)(1)(C) imposes upon the federal government no duty to obtain documents that are controlled by the state government or police, even if the prosecution is aware of the items"); see also *United States v. Marshall*, 132 F.3d 63, 68 (D.C. Cir. 1998) (holding the same for local law enforcement); *United States v. Brazel*, 102 F.3d 1120, 1150 (11th Cir. 1997), *cert. denied*, 522 U.S. 822 (same); *Thor v. United States*, 574 F.2d 215, 220–21 (5th Cir. 1978) (same). We reaffirm today that the duty of production imposed by Rule 16(a)(1)(E) extends to all qualifying documents within the "possession, custody, or control" of any component of the U.S. federal government—but not beyond.

A contrary ruling would impose an unrealistic burden. Requiring U.S. prosecutors to produce all material and responsive documents held by foreign partners would expand their duty to produce beyond their capacity to obtain. To comply with Rule 16, prosecutors would be compelled to produce documents that they do not possess, cannot acquire, have not confirmed exist, and—because Rule 16 is triggered by merely a preliminary showing of materiality—may not even matter

to the defendant's case. See *Thompson*, 944 F.2d at 1341. Rule 16 imposes no such duty.

B

Mitrovich next renews his separate constitutional challenge, claiming the government's nondisclosure violated the Due Process Clause of the Fifth Amendment. In *Brady v. Maryland*, the Supreme Court held that due process prohibits the suppression of material evidence favorable to the accused. 373 U.S. 83, 87 (1963); see also *Kyles v. Whitley*, 514 U.S. 419, 432–34 (1995). To establish a *Brady* violation a defendant must demonstrate that the government suppressed evidence, that the evidence was either exculpatory or impeaching, and that prejudice resulted. See *United States v. O'Hara*, 301 F.3d 563, 569 (7th Cir. 2002); see also *Giglio v. United States*, 405 U.S. 150, 154 (1972).

As a general rule, prosecutors cannot suppress evidence they do not possess. See *United States v. Romo*, 914 F.2d 889, 898–99 (7th Cir. 1990). But, in contrast with applications of Rule 16, we have recognized a constructive-possession doctrine in the *Brady* context. The government cannot "get around *Brady* by keeping itself in ignorance, or compartmentalizing information about different aspects of the case." *Carey v. Duckworth*, 738 F.2d 875, 878 (7th Cir. 1984). To the contrary, "the individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case." *Kyles*, 514 U.S. at 437. This duty to disclose favorable evidence, we have explained, "extends beyond evidence in [the prosecution's] immediate possession to evidence in the possession of other actors assisting the government in its investigation." *United States v. Walker*, 746 F.3d 300, 306 (7th Cir. 2014) (citing *Fields v. Wharrie*, 672 F.3d 505,

513 (7th Cir. 2012)). That includes any state and municipal agencies that are part of the "'prosecutorial team' broadly understood." See *United States v. Gray*, 648 F.3d 562, 566 (7th Cir. 2011) (citations omitted).

Our case law has not addressed whether the principle of constructive possession under *Brady* extends to co-participants in a joint international investigation. In *United States v. Stokes*, we established that the Fourth Amendment applies to searches conducted by foreign governments so long as "U.S. agents substantially participate[d] in [the] extraterritorial search of a U.S. citizen and the foreign officials were essentially acting as agents for their American counterparts or the search amounted to a joint operation between American and foreign authorities." 726 F.3d at 890. But we have not decided whether the due process protections articulated in *Brady* have a similar international reach. Nor have we had occasion to determine what degree of U.S.-foreign cooperation—if any—would be sufficient to give rise to an assumption of constructive possession.

This case presents no such occasion. Again, we accept the district court's assumption that Mitrovich's arrest stemmed from a joint U.S.-Oceanian investigation. But even if that investigation—and the level of cooperation it involved—sufficed to trigger a presumption of constructive possession in theory, the circumstances before us rebut any such presumption in fact. Where, as here, the United States has made diligent, good-faith efforts to obtain information from a foreign authority and the failure of those efforts establishes that the United States lacks the capacity to access or acquire that information through reasonable means, any presumption that the

government constructively possessed the information as a member of a joint investigation dissipates.

The district court's finding on this fact was clear and precise: "[T]he Government has turned over everything in its possession relating to the technical details of how the Oceanian authorities identified Mitrovich's IP address [and] has been unable to obtain the software and/or source code" that Mitrovich seeks. This finding that the prosecution lacked the capacity to obtain requested discovery materials is fatal to any presumption of constructive possession that might have otherwise applied.

The doctrine of constructive possession developed on the premise that prosecutors have the means to obtain documents held by fellow members of an investigatory team because of the close working relationship they share. When first extending *Brady* to documents possessed by federal enforcement agencies, the Supreme Court in *Kyles* reasoned that there is no "serious doubt" that "the prosecutor has the means to discharge the government's *Brady* responsibility" by establishing "procedures and regulations" to ensure the free flow of information between investigative entities. See 514 U.S. at 438.

Our case law echoes *Kyles*'s emphasis on access as an underlying assumption behind constructive possession. See, *e.g.*, *Crivens v. Roth*, 172 F.3d 991, 997 (7th Cir. 1999) (finding that the government had suppressed information within the meaning of *Brady* precisely because "the state in this case had the information at its disposal"). In keeping with that emphasis, we have never held that a prosecutor constructively possessed *Brady* material that she was unable to obtain. To the contrary, we have declined to find constructive possession in situations where prosecutors lack the capacity to access the

documents at issue. See, *e.g.*, *Walker*, 746 F.3d at 307 (finding that federal prosecutors did not constructively possess documents held by a municipal police department because the prosecution had no "access to or knowledge of the suppressed evidence"). A definitive showing that prosecutors cannot obtain discovery materials by any reasonable means destroys any presumption of constructive possession arising from their relationship with other investigating parties. This makes sound sense. The view that the government constructively possesses a document cannot coexist with a finding that it lacks, and has always lacked, the capacity to access it.

Mitrovich's *Brady* claim also fails for another reason. Without knowledge of what the requested technical information would have showed, he cannot demonstrate prejudice. To establish a *Brady* violation, "the cumulative effect of all such evidence suppressed by the government" must "raise[] a reasonable probability that its disclosure would have produced a different result." *Kyles*, 514 U.S. at 421–22. That is a hard standard to meet without any knowledge of the content of the information in question. See *Gray*, 648 F.3d at 567 (cautioning that "[t]he *Brady* rule is not a rule of pretrial discovery"); *Romo*, 914 F.2d at 889 (explaining that the rule "assumes the discovery, after trial, of favorable, material information" (internal quotation marks and citation omitted)).

Mitrovich's attempt to establish prejudice amounts to little more than speculation. His forensic examiner explained that without more information, it would be "impossible to prove exactly how th[e] code" behind the unmasking technique "was utilized" or "what is specifically transferred to a user's computer when their browser follows th[e] link." Accordingly, all the expert was able to say was that the use of

malware was "conceivable." This showing does not suffice to establish prejudice. Under *Brady*, Mitrovich bears the burden of demonstrating that the missing documents are not only necessary but sufficient to establish a "reasonable probability" of a different outcome—in this case the suppression of evidence. *Kyles*, 514 U.S. at 421–22.

Prejudice cannot be established through guesswork. Our review of the record provides no reason to infer that the missing technical information would have supported Mitrovich's defense theory. "Mere speculation that a government file may contain *Brady* material is not sufficient." *United States v. Morris*, 957 F.2d 1391, 1403 (7th Cir. 1992) (internal quotation marks and citation omitted).

III

Because the government's discovery obligations under Rule 16 do not extend to documents held exclusively by foreign members of a joint investigation, because the prosecution cannot "suppress" documents held by a foreign government that it cannot access through reasonable means, and because Mitrovich cannot establish that the government's nondisclosures resulted in prejudice, we AFFIRM the district court's denial of Mitrovich's motion for discovery sanctions.