RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 17a0105p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

MICHAEL MANCIL BROWN,

Defendant-Appellant.

No. 16-6291

Appeal from the United States District Court
for the Middle District of Tennessee at Nashville.
No. 3:13-cr-00118-1—Billy Roy Wilson, District Judge.

Argued: May 3, 2017

Decided and Filed: May 15, 2017

Before: COLE, Chief Judge; SUTTON and KETHLEDGE, Circuit Judges.

COUNSEL

ARGUED: J. Alex Little, BONE MCALLESTER NORTON PLLC, Nashville, Tennessee, for Appellant. Byron M. Jones, UNITED STATES ATTORNEY'S OFFICE, Nashville, Tennessee, for Appellee. **ON BRIEF:** J. Alex Little, BONE MCALLESTER NORTON PLLC, Nashville, Tennessee, for Appellant. Byron M. Jones, UNITED STATES ATTORNEY'S OFFICE, Nashville, Tennessee, Anthony V. Teelucksingh, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee.

OPINION

SUTTON, Circuit Judge. When criminal-law cases imitate art, they do not always choose its highest form. In *Austin Powers*: *International Man of Mystery*, Dr. Evil develops a

plan to steal a nuclear warhead and to hold the world hostage for $1 million. This was not, Dr. Evil's deputy pointed out, all that much money for a 1990s global criminal enterprise. But it was enough for an anonymous extortionist in today's case, who apparently was familiar with the movie and who chose some features of it as signatures of his 2012 crime. Assuming the nom de guerre "Dr. Evil," the individual demanded $1 million in Bitcoin in exchange for an encryption key to Mitt Romney's unreleased tax returns. The extortionist claimed to have stolen Romney's returns from PricewaterhouseCoopers, and he posted a taunting, digitally altered image of Mike Myers's Dr. Evil, wearing a Secret Service badge, in the lobby of the accounting firm's offices in Franklin, Tennessee.

A trail of digital breadcrumbs led law enforcement to Tennessean Michael Brown. It turned out that Brown never stole Romney's returns. And his attempt to extort PricewaterhouseCoopers, the Democratic and Republican parties, and the public earned Brown twelve convictions for wire fraud and extortion, a four year prison sentence, and an order to pay over $200,000 in restitution. Brown appeals his convictions on the grounds that the Secret Service's search warrant lacked probable cause and that he was prejudiced by the trial judge's decision to allow questions from the jury. Brown also appeals the obstruction of justice enhancement in the district court's calculation of his sentence. We affirm Brown's convictions but vacate his sentence.

I.

On August 28, 2012, a padded envelope arrived at the Franklin, Tennessee office of PricewaterhouseCoopers, an accounting and professional services firm. The envelope contained a flash drive and a letter, which explained that the anonymous sender had gained access to the firm's network and stolen the unreleased tax documents of Republican presidential nominee Mitt Romney and his wife Ann. To "Stop Release" of those tax records, all PricewaterhouseCoopers had to do was deposit one million dollars in Bitcoin—a virtual, sovereign-free currency—into a specified account. App. R. 34 at 4. The encrypted tax files on the thumb drive would go to every major media outlet, the sender said, and the encryption key would become public if no one paid him before September 28. At "the same time," the letter stated, "other interested parties

will be allowed to compete" for the returns and guarantee immediate release of them by depositing a million dollars in a separate, "Promote Full Release" Bitcoin account. *Id.*

Within three days, similar envelopes with similar letters and flash drives arrived at the offices of the Williamson County Republican and Democratic parties. And within a week after that, a series of posts appeared on Pastebin.com, a website that permits anonymous publication, describing the stolen documents and the information in the letters. The third of these Pastebin posts—signed "Dr. Evil" and accompanied by an image of Dr. Evil superimposed on the lobby of PricewaterhouseCoopers' Franklin office—directed users to a downloadable, encrypted file named "Romney1040-Collection.7z," which had been uploaded to another site by timyenmor28@live.com (that's "Romney" and "Mit" spelled backwards). *Id.* at 34, 39, 41.

Meanwhile, the Secret Service opened an investigation, as did PricewaterhouseCoopers. The PricewaterhouseCoopers security team concluded that no one had breached its network or compromised the Romney tax records. That left the Secret Service to catch the schemer. Records obtained from Pastebin showed that the three posts had been made using the TOR network, which routes online communications through anonymizing proxy computers to hide the user's IP address. And the Secret Service took possession of the envelopes, letters, and flash drives. All three flash drives contained a file named "Romney1040-Collection.7z." R. 177 at 33, 53–54. The unallocated space on the drives also held text strings and two photos of cats. The PricewaterhouseCoopers flash drive held the text string, "5276 dolphin kathryn." *Id.* at 35. The Democratic Party drive had the string "4154 dolphin KnightMB." *Id.* at 55, 57; App. R. 34 at 22.

A series of Google searches using "KnightMB" revealed an email address, knightmb@knightmb.dyns.org, and that a 33 year-old Tennessean named Michael Brown made online posts connected to that address. The Tennessee Department of Motor Vehicles confirmed that Michael Mancil Brown lived in Franklin and had a spouse named Kathryn. AT&T's subscriber records for Brown's home listed his email address as knightmb@knightmb.dyns.org. Brown's Comcast subscriber records led to knightmb@timekoin.org. YouTube videos posted by "KnightMB" had Brown in them. And another online post by "KnightMB" had bragged about encrypting a file using 7-Zip, the program denoted by the ".7z" file extension in "Romney1040-

Collection.7z." The Secret Service obtained a trap-and-trace order, *see* 18 U.S.C. § 3123(a)(1), to monitor internet traffic in and out of Brown's house. On September 11, 2012, an IP address associated with Brown connected to TOR—the anonymizing proxy network that "Dr. Evil" and "timyenmor" had used—and accessed the same German IP address that one of the Pastebin posts had come from.

The Secret Service obtained a search warrant for Brown's home, and forensic examination of Brown's computer identified more incriminating evidence. The key conclusions were (1) that the extortionist's flash drives had connected to Brown's computer less than a week before they arrived at PricewaterhouseCoopers and the Democratic and Republican parties, (2) that Brown's computer had stored the Romney1040-Collection.7z file, (3) that Brown's internet browser had bookmarked the Bitcoin addresses in the extortion letters two days before the first extortion letter arrived at PricewaterhouseCoopers and had accessed those addresses on the morning of the search, (4) that his computer had used TOR to connect to the IP address linked to one of the Pastebin posts ten minutes before that post appeared, (5) that the computer used the KnightMB email address around the time it had Googled directions to the PricewaterhouseCoopers office in Franklin, one week before the letter arrived there, and (6) that the computer had stored the images of Dr. Evil and the PricewaterhouseCoopers lobby, the "timyenmor" email address, and the text of the "Dr. Evil" post—all before any of those items appeared on Pastebin—as well as numerous filenames related to Romney's taxes. Brown's neighbors said that he went to their house to print some files (the extortion letters), where he had also gotten padded envelopes like the ones the letters and thumb drives arrived in. Brown's spouse and daughter resolved one last mystery: The anonymous cats pictured on the Democratic Party thumb drive belonged, they said, to a neighbor, Janine Bolin. Ms. Bolin corroborated that those were her cats, Tripper and Valentine, and that Brown had once helped her with some computer problems.

When confronted with this evidence, Brown denied any involvement. He told the Secret Service that someone else must have been in his house and manipulated his computer to do all of those incriminating things. He couldn't say who, but he did say he had seen two unknown black men sitting at his computer at different times. In fact, he added, strangers often came to his

house, and any one of them, or any one of the eight people on a list of visitors that Brown provided to the Secret Service, could have been the extortionist.

The government did not buy these explanations, and a grand jury indicted Brown. A jury convicted him on all twelve counts—six for wire fraud, six for extortion. That led to a 48-month sentence and $201,836 in restitution to PricewaterhouseCoopers for the cost of its investigation.

II.

Motion to suppress. Brown argues that the district court erred when it denied him a hearing under *Franks v. Delaware* as part of his motion to suppress evidence from the search of his home. 438 U.S. 154, 155–56 (1978). If a defendant shows that the police used "false statements" to obtain a warrant, *Franks* gives the defendant the right to obtain an evidentiary hearing to challenge its validity. *United States v. Fowler*, 535 F.3d 408, 415 (6th Cir. 2008). No hearing is needed if the affidavit supports probable cause after setting aside any false statements. *Franks*, 438 U.S. at 171–72.

Here are the alleged falsities. The affidavit details the Secret Service's prior investigation of Brown for an unrelated incident involving data stolen from an insurance company. That investigation started in 2009 and ended in 2010, after Brown took a polygraph exam. The affidavit repeatedly refers to this as the "2009 investigation," but misstates the date of the polygraph exam as "January 13, 2012," when it occurred on January 13, 2010. R. 4 at 47–48. The affidavit also fails to state that Brown passed the polygraph. This error and this omission, says Brown, created the false impression that the investigation concluded more recently than it had and that the Secret Service had caught him lying before. He also says the affidavit unfairly omitted (1) that many presumably innocent people use TOR, (2) that the cats pictured on the thumb drives did not appear to be at his house, (3) that Brown runs an internet business, which means many users besides Brown use his IP addresses, (4) that the Secret Service did not know when or how the text strings got on the extortionist's thumb drives, and (5) that Brown sometimes spelled "advice" correctly, even though he had misspelled it (as "advise") during the insurance company incident in the same way the "Dr. Evil" letter misspelled it.

Even if we edit the affidavit in the way Brown requests, probable cause still exists. All that's needed for probable cause "is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Miller*, 314 F.3d 265, 268 (6th Cir. 2002) (quotation omitted). That is a "practical, common-sense decision," *Illinois v. Gates*, 462 U.S. 213, 238 (1983), based on "the totality of the circumstances, not line-by-line scrutiny" of the affidavit, *United States v. Thomas*, 605 F.3d 300, 307 (6th Cir. 2010).

The revised affidavit offers "a fair probability" that Brown's home would contain evidence of the crime. Start with the text strings on the flash drives. One of them featured "KnightMB," which was associated with several of Brown's email addresses, online usernames, his Bitcoin-like business (called TimeKoin), and the utility companies that serviced his house in Franklin. Searches related to "KnightMB" also showed that Brown lived in Franklin, where all three extortion letters arrived, and that he was married to someone named Kathryn. One of the *other* flash drives had the name Kathryn, spelled the same way, in its unallocated space. Even accounting for the fact that the Secret Service did not know how those text strings landed on the flash drives, these facts alone established probable cause to search Brown's house.

But that's not the last of it. The supposed Romney tax files were encrypted with 7-Zip, and someone going by "knightmb" (Brown's frequent username) had posted online about successfully using 7-Zip. The Pastebin poster had used TOR (a common mechanism for anonymizing internet use) to connect to a specific IP address in Germany; the Secret Service then observed someone in Brown's house using TOR to connect to the same German IP address. Looking at all of these circumstances and without mentioning the insurance company incident, these facts establish a fair probability that the Secret Service would find evidence of a crime in Brown's house. *See Thomas*, 605 F.3d at 307.

Once you add the insurance company incident, that probability gets higher. After properly accounting for the fact that Brown passed his polygraph and that the investigation concluded almost three years before, the 2009 insurance company investigation still showed that Brown was a sophisticated computer user who had gained access to private information inside a secure network. It also revealed that he misspelled "advice" as "advise" at least once (but not always). "Dr. Evil" made the same mistake. R. 4 at 34, 48. All in all, probable cause existed.

Brown responds that TOR is so common that it renders his home's connection to it "meaningless." Appellant's Br. 31. But his home didn't merely connect to TOR; it used TOR to connect to the same German IP address that the Pastebin poster used.

Saying "advise" instead of "advice," he adds, is meaningless given that he sometimes used "advice" correctly. He's right that this was not the Rosetta Stone to the investigation. But it still had *some* probative value and supported all of the other arrows pointing in his direction.

Same with the insurance company incident. Brown argues for the first time on appeal that we should redact the *entire* insurance company incident from the affidavit. *See* Appellant's Br. 31–33. That's quite a change of heart. He first wants to challenge the omissions from this part of the affidavit, then claims the incident told the magistrate too much. But law enforcement need not omit facts from an affidavit just because they came to light in an earlier investigation. It's usually a good idea for affidavits to include as much potentially relevant information as possible, not least because it avoids reckless omissions under *Franks*. The 2009 investigation explains what the Secret Service already knew about Brown, including his facility with computers and his experience in taking protected data from a private company. The Secret Service agent fairly included it in the affidavit.

Juror questions. Brown challenges the trial judge's decision to permit jurors to propose questions during the trial. Because he declined to raise this objection before or during trial, we review it for plain error. Fed. R. Crim. P. 52(b); *United States v. Henry*, 797 F.3d 371, 374 (6th Cir. 2015). That means we may correct the error only if it was obvious, prejudiced the defendant, and seriously affected the integrity of the proceeding. *Molina-Martinez v. United States*, 136 S. Ct. 1338, 1343 (2016).

Brown's claim does not get out of the gate. There was no error, plain or otherwise, in the choice to allow juror questions. Trial judges have discretion to permit juror questions if they take precautionary measures. *United States v. Collins*, 226 F.3d 457, 462–65 (6th Cir. 2000); *see also United States v. Rawlings*, 522 F.3d 403, 407 (D.C. Cir. 2008) (noting unanimity among ten circuits). Juror questioning, we have explained, "should be a rare practice," but "the balance of risks to benefits is more likely to weigh in favor of juror questions in complex cases." *Collins*,

226 F.3d at 463. When a district court decides to permit juror questions, (1) counsel should be alerted as early as practicable; (2) the jury should be instructed that questions should be reserved for important points, that the rules of evidence may prevent certain questions from being asked, and that jurors should not draw any inferences from the court's choice not to ask a question; (3) the court should give a prophylactic instruction in its final charge to the jury; and (4) "a screening mechanism should be set in place, such as having the jurors write down their questions and pass them to a judge, followed by a sidebar at which the judge would rule on attorneys' objections." *Id.*

No abuse of discretion occurred. Understanding the evidence required the jury to grasp the Secret Service's forensic analysis of thumb drives, online posts, and Brown's computers, as well as the TOR network, Bitcoin, fingerprint matching, and digital photo manipulation. That's enough complexity for a district court to believe that permitting questions might aid jurors in their search for truth. And the precautionary measures taken by the trial judge ensured that the jury would retain its proper role and that the parties would not be prejudiced.

As in *Collins*, the district court announced its intention to permit juror questions on the first day of trial. *See id.* As in *Collins*, the court created a screening procedure and instructed jurors that, after the lawyers were finished, they could ask questions they "consider[ed] important of [that] witness [by] writ[ing] it out [and] pass[ing] it down" so that the judge and lawyers could consider whether to ask it. R. 176 at 34–35; *Collins*, 226 F.3d at 464. The court further instructed the jury, as *Collins* recommends, that a juror should not "become a detective. Don't ask too many questions." R. 176 at 34. And "don't get your feelings hurt" if your question doesn't get asked, because it may have "been ruled on earlier" or may be addressed by another witness later. *Id.*; *see Collins*, 226 F.3d at 463. Although the district court did not repeat those instructions in its final charge, it reminded the jury that its prior instructions still applied. No error occurred.

Obstruction of justice. Brown claims that the district court improperly increased his offense level based on obstruction of justice. In assessing an obstruction of justice enhancement, we give clear error review to the district court's factual determinations and fresh review to its legal conclusions. *United States v. Bazazpour*, 690 F.3d 796, 805 (6th Cir. 2012).

The Sentencing Guidelines add two levels to the offense level if "the defendant willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the investigation, prosecution, or sentencing of the instant offense of conviction." U.S.S.G. § 3C1.1. The Application Notes provide non-exhaustive lists of covered and non-covered conduct. *Id.* at n.4, n.5. Note 4(G) provides that "a materially false statement to a law enforcement officer that significantly obstructed or impeded the official investigation or prosecution" generally merits an enhancement. And Note 5(B) provides that "making false statements, not under oath, to law enforcement officers" generally does not merit an enhancement "unless Application Note 4(G) above applies." The upshot is that a lie to an investigator by itself does not usually warrant an enhancement unless it substantially interferes with the government's investigation. *United States v. Carter*, 510 F.3d 593, 598 (6th Cir. 2007).

The district court found one obstructive act: that Brown "ran a rabbit across the trail" by telling investigators that other people had "access" to his computer and thus may have committed the crimes. R. 175 at 16. There is some dispute over whether the two unnamed black men Brown mentioned during the proffer were included in the list of eight people with access to Brown's computer that his lawyer later emailed to investigators. But Brown cannot be subject to an obstruction enhancement either way. If the two men were not included in the list, the government has not shown, and the district court did not find, that this statement caused any obstruction, significant or otherwise, to the government's investigation.

And even if the list of eight included the two men mentioned during the proffer, Brown's statements do not establish obstruction of justice for two reasons. The first is that Brown did not lie. The emailed list of eight names, supplied by his lawyer to investigators, responded to a question posed by investigators and came with the caveat that it was "not furnished as being exculpatory." App. R. 34 at 209. The trial established that six of the eight people had indeed been to Brown's house and thus had "access" to Brown's computer. As for the two individuals on the list who had never been to Brown's house, they were added to the list by Brown's wife, not Brown.

The second reason is that the email did not "hurt or retard [the] investigation." *United States v. Williams*, 952 F.2d 1504, 1516 (6th Cir. 1991). Brown's defense was that he didn't do

it and that these eight people had access to his computer and thus may have committed the crime. All the investigators had to do in response was investigate the eight people on the list. The investigators interviewed each one. They called each one at trial. And when each of the persons on this discrete list denied using Brown's computer, that helped the government, as it undermined Brown's credibility, bolstered the government's case, and eliminated one of the few remaining ways in which this crime could have been committed. Brown's statements to prosecutors thus did not "significantly obstruct[] or impede[] the government's investigation" and thus cannot suffice for an obstruction of justice enhancement. *Carter*, 510 F.3d at 598; *see* U.S.S.G. § 3C1.1 n.4,

For these reasons, we affirm Brown's convictions, vacate his sentence, and remand for resentencing consistent with this opinion.