

United States Court of Appeals
For the Eighth Circuit

No. 12-3960

United States of America,

Plaintiff - Appellee,

v.

Jeremy Robert Stevenson,

Defendant - Appellant.

Appeal from United States District Court
for the Southern District of Iowa - Davenport

Submitted: June 12, 2013

Filed: August 15, 2013

Before COLLTON, GRUENDER, and BENTON, Circuit Judges.

COLLTON, Circuit Judge.

Jeremy Stevenson entered a conditional guilty plea to two counts of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). The district court¹

¹The Honorable Robert W. Pratt, United States District Judge for the Southern District of Iowa.

denied Stevenson's motion to suppress evidence without a hearing, and quashed a subpoena that Stevenson had served on AOL, Inc. Stevenson appeals, and we affirm.

I.

AOL is an Internet service provider. In the course of operating its business, the company identifies certain files that may damage its network with "hash values." A hash value is an algorithmic calculation that yields an alphanumeric value for a file. Among the files to which AOL assigns hash values are those containing child pornography.

AOL scans files sent through its network with a tool that it calls the Image Detection and Filtering Process. When the filtering process detects a hash value that corresponds to a file containing child pornography, it automatically forwards a report to the National Center for Missing and Exploited Children ("National Center").

In September 2010, the filtering process detected that one of AOL's users had e-mailed images depicting child pornography to a Google e-mail account. The filtering process triggered an alert to the National Center, and the National Center passed the tip along to the Iowa Department of Criminal Investigation. Investigators learned that both the AOL and Google e-mail accounts belonged to Jeremy Stevenson.

In January 2011, law enforcement officers obtained a warrant to search Stevenson's home. After advising Stevenson of his rights under *Miranda v. Arizona*, 384 U.S. 436 (1966), the officers questioned Stevenson. Stevenson said that he lived alone and that he used the computers in his house. When asked whether he had any child pornography on his computers, Stevenson responded, "I hope not." A forensic search of Stevenson's computers and thumb drives yielded four videos and 721 images depicting child pornography.

A grand jury charged Stevenson with two counts of possessing child pornography. Stevenson moved to suppress the images discovered by AOL, the images and videos found in the search of his home, and the statements he made to the officers during the search. Stevenson argued that his rights under the Fourth Amendment were violated when AOL scanned his e-mail for child pornography, and that this violation tainted the subsequent search. Stevenson also served AOL with a subpoena demanding various documents that he hoped would support his motion to suppress, and he requested an evidentiary hearing to present whatever documents he would obtain from AOL.

The district court declined to hold a hearing, denied the motion to suppress, and quashed the subpoena. The court explained that AOL was a private actor, so it was not constrained by the Fourth Amendment, and that Stevenson had failed to raise a contested issue of fact that would require an evidentiary hearing. Stevenson entered a conditional guilty plea, preserving his right to appeal the district court's rulings. On appeal from the denial of a motion to suppress, we review the district court's findings of fact for clear error and its legal conclusions *de novo*. *United States v. Anderson*, 688 F.3d 339, 343 (8th Cir. 2012).

II.

The Fourth Amendment applies only to state action, so it does not constrain private parties unless they act as agents or instruments of the government. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). When a statute or regulation compels a private party to conduct a search, the private party acts as an agent of the government. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614 (1989). Even when a search is not required by law, however, if a statute or regulation so strongly encourages a private party to conduct a search that the search is not "primarily the result of private initiative," then the Fourth Amendment applies. *Id.* at 614-15.

Stevenson argues that two sections of the United States Code demonstrate that AOL acted as a government agent when it scanned his e-mail. Title 18, United States Code Section 2258A(a) requires AOL to report to the National Center any apparent violation of the child pornography laws that AOL discovers while providing electronic communication services. 18 U.S.C. § 2258A(a). Section 2258B(a) immunizes electronic communication service providers from suit in state and federal court for claims “arising from the performance of the reporting . . . responsibilities” imposed by § 2258A. *Id.* at §2258B(a). Although neither provision requires AOL to scan the e-mails of users, Stevenson contends that the sections combine to make AOL an agent of the government.

Stevenson relies primarily on *Skinner*, where the Supreme Court reviewed the regulatory regime that governed breath and urine tests conducted by railroad companies on their employees. 489 U.S. at 614. The regulations required the railroads to conduct tests under certain circumstances, and authorized the companies to conduct tests if other conditions were met. *Id.* at 609-11. As far as the railroad companies were concerned, the authorized tests were optional. *Id.* at 611. The Court held that the Fourth Amendment applied to the optional tests as well as the mandatory tests, because the optional tests were part of a scheme that demonstrated a strong governmental preference for testing. *Id.* at 614-16.

The Court noted three features of the regulations that led it to conclude that the optional tests amounted to state action. First, the regulations “removed all legal barriers” to the testing: they preempted any collective bargaining agreement that did not provide for the specified tests, and they prohibited the railroad companies from negotiating away their right to conduct the tests in the future. *Id.* at 615. Second, the regulations provided for specific consequences if an employee refused to submit to a test that a railroad company chose to conduct. *Id.* When an employee refused, the regulations required the railroads to remove that employee from certain duties. *Id.*

Finally, the regulations authorized the government to obtain the results of the tests. *Id.*

Sections 2258A(a) and 2258B(a) do not resemble the regulations at issue in *Skinner*. Neither section authorizes AOL to scan its users' e-mails. Neither section clears the "legal barriers" to scanning by preempting private contracts that forbid scans, or by prohibiting AOL from contracting away its right to scan. And neither section prescribes consequences for AOL's users should they refuse to submit to AOL's use of the filtering process.

Stevenson points to § 2258B(a)'s grant of immunity, but that section immunizes AOL only for complying with its *reporting* obligations if it discovers a file containing child pornography. Section 2258B(a), like § 2258A(a), is silent regarding whether or how AOL should scan its users' e-mail. The only subsection that bears on scanning makes clear that an electronic communication service provider is not required to monitor any user or communication, and need not affirmatively seek facts or circumstances demonstrating a violation that would trigger the reporting obligation of § 2258A(a). 18 U.S.C. § 2258A(f).

In sum, the only similarity between the statutes that Stevenson cites and the *Skinner* regulations is that both include reporting obligations. A reporting requirement, standing alone, does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography. *Accord United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 366-67 (4th Cir. 2010).

III.

Stevenson next contends that the district court erred by refusing to hold an evidentiary hearing. He argues that even if AOL was not transformed into a

government agent by operation of law, an evidentiary hearing was required to determine whether AOL conducted the particular scan of his e-mail at issue here as an instrument of the government. A district court must hold an evidentiary hearing only when the moving papers are sufficiently definite, specific, and detailed to establish a contested issue of fact. *United States v. Mims*, 812 F.2d 1068, 1073-74 (8th Cir. 1987). We review the district court's denial of Stevenson's request for a hearing for an abuse of discretion. *United States v. Williams*, 669 F.3d 903, 905 (8th Cir. 2012).

Stevenson argues that the government knew of and acquiesced in the search, and that AOL conducted the scan to assist law enforcement, rather than to advance its own objectives. Although those are two of the factors we have examined when evaluating whether a private party acted as a government agent, *see United States v. Smith*, 383 F.3d 700, 705 (8th Cir. 2004), Stevenson offered the district court no reason to believe those factors were present in this case. Stevenson's motion to suppress and his brief in support simply stated, without citation, that AOL acted as a government agent when it scanned his e-mail.

The government, on the other hand, adduced evidence tending to show that AOL was not acting as an instrument of the government. An affidavit submitted by AOL's Director of Investigations and Cyber Security explained that AOL developed its scanning program for its own purposes, without any prompting or input from the government. AOL began using the filtering process for business reasons: to detect files that threaten the operation of AOL's network, like malware and spam, as well as files containing what the affidavit describes as "reputational" threats, like images depicting child pornography. According to the affidavit, AOL operates its file-scanning program independently of any government program designed to identify either sex-offenders or images of child pornography, and the government never asked AOL to scan Stevenson's e-mail. Stevenson responded to the affidavit with more unsupported assertions and did not specifically rebut any of the affidavit's claims.

We agree with the district court that Stevenson did not demonstrate a contested issue of fact that warranted a hearing. Where a defendant offers only conclusory allegations in support of a motion to suppress, and where those allegations are unsupported by any citation to the record, a district court does not abuse its discretion by refusing to hold an evidentiary hearing. *United States v. Allen*, 573 F.3d 42, 52 (1st Cir. 2009); *see Mims*, 812 F.2d at 1073-74.

Finally, Stevenson says the court should not have quashed the subpoena *duces tecum* that he served on AOL. *See* Fed. R. Crim. P. 17(c). The subpoena is not available through the district court's electronic docket, and Stevenson has not furnished a copy to this court, but portions of the subpoena are described in papers that were filed with the district court and are available to us. So far as we can tell, the subpoena sought various agreements between AOL or its subsidiaries and the National Center, the Department of Justice, and a state attorney general. The subpoena suggests that these agreements relate to joint efforts by AOL and governmental actors to limit child pornography on the Internet. The subpoena also sought information regarding the origin of the database of hash values that AOL uses in its filtering process.

Rule 17(c) does not provide a means of discovery from the government in criminal cases. *Nixon v. United States*, 418 U.S. 683, 698-99 (1974). This court has said the same about subpoenas directed to third parties, *United States v. Hang*, 75 F.3d 1275, 1283 (8th Cir. 1996), and Stevenson does not argue for a more permissive standard. *Cf. Nixon*, 418 U.S. at 699 n.12; *United States v. Tomison*, 969 F. Supp. 587, 593 n. 14 (E. D. Cal. 1997). To warrant the issuance of a subpoena under the rule, a party must request a document with adequate specificity and show that the requested document is relevant and admissible. *Hang*, 75 F.3d at 1283; *United States v. Hardy*, 224 F.3d 752, 755 (8th Cir. 2000). The relevance and specificity elements "require more than the title of a document and conjecture as to its contents," and a subpoena should not issue based upon a party's "mere hope" that it will turn up

favorable evidence. *Hang*, 75 F.3d at 1283. We review the district court's decision to quash a subpoena for abuse of discretion. *Id.*

The subpoena to AOL did not meet the *Nixon* standards. Stevenson contends that the requested documents would have supported his motion to suppress, because they would have proved that AOL partnered with law enforcement to combat child pornography. Even assuming such a "partnership" exists, however, AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes. Stevenson does not allege that the agreements sought by the subpoena would reveal the sort of official regulatory features that led the Court in *Skinner*, 489 U.S. at 615, to conclude that searches of railroad employees were not primarily the result of private initiative. AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent. *Smith*, 383 F.3d at 705.

Stevenson speculates that the agreements might show that law enforcement officials asked AOL regularly to conduct certain scans, and argues that such information would be relevant to his Fourth Amendment claim. But Stevenson does not identify a specific agreement that supposedly reveals such requests, and he offers only conjecture about what such a document might contain. Stevenson's request for "[d]ocuments identifying the . . . creator and provider" of AOL's hash value database was similarly vague, suggesting an effort at exploratory discovery. Indeed, Stevenson acknowledged in the district court that he sought "an opportunity to discover . . . evidence with subpoenas" before completing briefing on his motion to suppress. R. Doc. 20-1, at 1. The subpoena requests, therefore, were not sufficiently specific to satisfy the rule, and the district court did not abuse its discretion in granting the motion to quash. See *Hang*, 75 F.3d at 1283; see also *Richardson*, 607 F.3d at 368 (holding that a district court properly quashed a subpoena duces tecum to AOL,

where a defendant sought to use it “as a discovery mechanism to develop his agency claim.”).

* * *

The judgment of the district court is affirmed.
