United States Court of Appeals
For the First Circuit

No. 24-1467

UNITED STATES,

Appellee,

v.

ERIC ROBERT JOHNSON,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Denise J. Casper, U.S. District Judge]

Before

Gelpí, Thompson, and Montecalvo,
Circuit Judges.

Christine DeMaso, Assistant Federal Public Defender, for appellant.

Randall E. Kromm, Assistant United States Attorney, with whom Leah B. Foley, United States Attorney, was on brief, for appellee.

July 7, 2026

THOMPSON, Circuit Judge.

Overview

In the current era of technology, there are myriad ways for people to share content and information with each other. One such way is to participate in peer-to-peer, file-sharing networks, like LimeWire, BitTorrent, or, pertinent to this case, Freenet. These publicly-available, internet-based platforms are a conglomerate of files that users can download from, upload to, and share with each other. Freenet, in particular, advertises as a network that preserves its users' anonymity, thereby providing them a more privatized means to share files. And, as a result, some choose to abuse the platform by circulating illicit content.

Well, in the present case, appellant Eric Robert Johnson's Freenet activity led to his conviction in the District of Massachusetts for possessing child pornography. But since the pretrial phase, Johnson has maintained that the government's bust violated the Fourth Amendment, and he's sought to suppress all evidence derived from the bust. Unable to sway the district court in his favor, however, Johnson decided to plead guilty and rehash the suppression issue before us.

So, we lay out everything in detail below, including our reasons for why the district court is **affirmed**.

I. Background

We pull our facts from the district court's decision and from the evidentiary hearing, "presenting them in the light most compatible with [the district court's] ruling." United States v. McGregor, 650 F.3d 813, 816 (1st Cir. 2011) (citation modified).

a. Freenet

Before getting into what happened in Johnson's case, we need to lay some groundwork about Freenet and its mechanics to understand today's issues. Freenet is an internet-based, peer-to-peer, file-sharing network that focuses on preserving its users' anonymity. The Freenet software is publicly-available and free, and thus it can be downloaded and installed by anyone. Freenet's file sharing operates through a network of linked computers (or "nodes") that break down data into fragments (or "blocks"), encrypts those fragments, and randomly distributes them among its users' nodes for storage.[1] This breakdown process occurs when a user uploads a file onto Freenet. After Freenet distributes the data blocks to a user's nodes for storage, it then generates an index (or "manifest") that lists all the blocks of the file and

[1] Freenet does not store complete files in one place, and, once broken down into blocks, users cannot decrypt the individual blocks to view the content stored on their devices. At most, the users are able to see there is an encrypted block in their data cache.

a "manifest key"[2] that can be used to locate the blocks so it can "reconstruct" the file for download. To reconstruct and download files on Freenet, users share manifest keys through various means, such as email, text, or posting them on online forums.

How does the reconstruction process work? To download a file, a user inputs a manifest key into Freenet and doing so signals the user's node to initiate the hard work. The node first sends out requests to the user's peers -- neighboring nodes -- for the data blocks.[3] As our usage of "requests" (plural) suggests, the Freenet software doesn't contact one sole peer to retrieve the data blocks. The requests are divvied up (in roughly equal parts) and sent out to several of the user's peers. If the receiving-peer's node does not have the respective data block, it will "relay" the request to a group of its peers to help it gather its portion of the requested data blocks (again, with the work divided evenly). Each time a request is sent out is called a "hop," and Freenet will cap a request at no more than 18 hops. We say "no more than" because Freenet attempts to conceal the original requestor's identity by randomizing the maximum number of hops for each download, however, that number never exceeds 18.

---

[2] Each manifest key is made up of a series of letters, numbers, and special characters.

[3] Data blocks are identified by their "hash value[s]" which is, in essence, a unique digital signature for each block.

Freenet is operable in either "Darknet" or "Opennet" mode, based on each user's choice. In the more private and anonymized Darknet mode, a user's computer will connect only to peers selected by that user. But in the less-protected Opennet mode, a user's computer will connect to unknown peers (strangers) on the whole of Freenet's worldwide network (where Freenet is legal, of course). Freenet does not conceal a user's IP address when their node connects to a neighboring node, thus strangers can view an Opennet user's IP address whenever they connect.

Upon the download and installation of Freenet, users are warned explicitly before choosing an operation mode that, in low security Opennet mode, "an attacker with moderate resources may be able to trace [the user's] activity on Freenet back to [the user]."[4] It further warns (on another screen) that in low security mode, "[i]t may be quite easy for others to discover [the user's] identity." Freenet also reminds users throughout the file downloading process that they are operating in low security mode

[4] One more caveat is worth noting. Opennet mode can operate in either "low security" or "normal security" mode. By choosing low security mode, the user agrees that they "do not care about monitoring and want [Freenet's] maximum performance." By choosing normal security mode, the user agrees that they "live in a relatively free country, but [they] would like to make it more difficult for others to monitor [their] communications." Also, when selecting normal mode, Freenet warns that it "will be reasonably careful to protect [the user's] anonymity, at some performance cost. [The user] should add friends running Freenet and upgrade to [Darknet mode] when [they] are able."

and to "[b]e careful" when opening a newly-downloaded file because "it might cause your web browser or other software to breach your anonymity[] [or] give away your IP address."

b. Freenet Roundup

Freenet's anonymity features make it alluring to those who want to share and retrieve illicit materials, such as child sexual abuse material ("CSAM"), online. To combat this problem, Dr. Brian Levine -- a professor at the University of Massachusetts -- created "Freenet Roundup," a law enforcement tool that can identify and trace CSAM file-sharing on Freenet. Freenet Roundup is a modification of Freenet that operates in Opennet mode and is available only to law enforcement officers. When using Freenet Roundup, an officer's node operates as would a normal peer in the Freenet network. Thus, the officer's node receives and relays strangers' requests for data blocks like a typical Freenet user. The difference with Freenet Roundup is that it logs requests it receives and filters them through a two-step process.

At the first step, the law enforcement node looks at the "Hops to Live" counter for the request -- which shows the remaining number of hops out of the possible 18-hop maximum -- to determine whether it has 16 or more hops remaining.[5] If at least 16 hops do remain, the request proceeds to step two of filtering. At step

[5] Requests with less than 16 hops are not of interest because they are highly unlikely to have come from an original requestor.

two, the flagged requests are sent to a server managed by Pennsylvania's Internet Crimes Against Children Task Force ("ICAC") to determine whether the requests were made for a known CSAM file. The ICAC has a library of data blocks identified as CSAM and compares their hash values with the blocks in the flagged requests. If there's no match, there's no further processing of that request. If there is a match, though, the request information is entered into a spreadsheet that employs a formula to determine whether its sender was the original requestor or merely a relayer of another user's request.[6] The request information includes the timestamp (date and time) of when it was made, the number of remaining hops, the number of peers in the node's network, and the node's IP address.[7] The information is then sent to the appropriate jurisdiction for further investigation based on the geolocation for the respective IP address.

c. The Arrest

Eric Robert Johnson was one of the Freenet users caught in the web of Freenet Roundup. An investigation ensued after Federal Bureau of Investigations ("FBI") Special Agent Bryce

[6] Dr. Levine stated in his testimony that his report revealed the false positive rate for identifying these matches as requestors or relayers has been no more than 2.3 percent.

[7] The node's number of peers, IP address, and the request's remaining number of hops are all transmitted when using the Freenet software in the normal course.

Montoya was tipped off that Freenet Roundup identified a user (with an IP address that was later determined to be Johnson's) sent out three different requests for CSAM data blocks between May 29 and June 8, 2021.[8] In February of 2022, Agent Montoya successfully applied for a search warrant for Johnson's residence in Billerica, Massachusetts, aiming to find evidence of his possession and receipt of child pornography.[9] FBI agents executed the search, and it yielded positive results. They found two laptops (at least one of which that had the Freenet software downloaded), a tablet, and multiple external hard drives (at least one of which that had contained CSAM).

So, naturally (as they say), he caught a case, and we now move on to recall the juridical play-by-play.

II. Procedural History

Johnson was charged with one count of possession of child pornography in violation of 18 U.S.C. § 2252(a)(5)(B), (b)(2). During the pretrial phase, Johnson moved the court to suppress all

[8] To trace the IP address back to its owner, law enforcement first determined that Verizon serviced the IP address. Thereafter, the FBI subpoenaed Verizon for the subscriber information, which was registered under Johnson's name and Billerica address.

[9] In the affidavit, Agent Montoya explained the operations of both Freenet and Freenet Roundup, and, from the evidence the FBI had gathered and reviewed, that he believed a user with an IP address registered to Johnson had sent out three different requests for CSAM files. Agent Montoya also described the content of the sought-after files.

the evidence derived from law enforcement's use of Freenet Roundup. He kicked off his motion by arguing that the FBI's use of its tool to monitor Freenet and track his activity constituted a Fourth Amendment search and that he had an expectation of privacy in the requests he sent out on the platform.

To strengthen his challenge, Johnson said the government's conduct was in contradiction to Kyllo v. United States, 533 U.S. 27 (2001), being that it was only able to obtain the at-issue evidence by using "sophisticated technology that is not in general public use," which made the purported search "presumptively unreasonable without a warrant." He also compared law enforcement's warrantless use of Freenet Roundup with its warrantless procurement of cell phone site information which the Supreme Court deemed unconstitutional in Carpenter v. United States, 585 U.S. 296 (2018).

In harmony with the Fourth Amendment framework for answering these types of questions (fret not, we'll break this down in more detail below), the remainder of Johnson's suppression arguments can be placed in two categories: subjective and objective expectations of privacy. We'll start with the former, the subjective variant.

For this prong of his argument, Johnson explained that a Freenet user relies on the software to provide anonymity, and the limited data revealed through transmissions are a "dint of its

operation," id. at 315, that allows Freenet to perform its functions. A single node, Johnson said, cannot determine "the overall structure of the network and identify individual users." Thus, a user's subjective expectation of privacy in their Freenet transmissions is violated when the government deploys its Freenet Roundup tool to track activity "on the network, assemble the data, and analyze it using special law enforcement-only software."

As to his claim of having an objective expectation of privacy, Johnson focused on the process law enforcement undertook to distinguish requestor nodes from relayer nodes (explained above). He argued the "requirements and resources necessary to de-anonymize Freenet users" make it "out-of-reach to all but state actors." He supported his claim with a forensic report prepared by Michael Miglianti,[10] who described the "significant research and validation resources" the government used to create Freenet Roundup and explained how such techniques "are vastly different than the resources associated with a typical Freenet user."[11]

[10] Miglianti is an expert witness with "years of experience in the digital forensics and cyber-security fields" who Johnson called upon to testify at trial.

[11] Miglianti stated (in his report) that the Freenet "software is freely available," "easily downloaded from the website," and "requires minimal user time and effort." He contrasted this near-burdenless process with Freenet Roundup for which "significant resources have been expended" to develop.

In its opposition to the suppression motion, the government argued Johnson failed to establish a subjective and objective expectation of privacy in his Freenet transmissions. It challenged Johnson's contention that his "mere use of Freenet, as a file sharing platform specifically aimed at anonymizing its users, alone[,] manifests a reasonable expectation of privacy[.]" The government said Johnson lacked a reasonable expectation of privacy when he "voluntarily shared requests for child pornography files with an unknown collection of strangers on Freenet," homing in on the rule that a person does not have a reasonable expectation of privacy in information voluntarily disclosed to third parties. And it further emphasized that Johnson chose to use Freenet in Opennet mode, which warned him that his IP address "would be shared with many virtual strangers."

Additionally, the government pointed to a breadth of cases that held a person does "not have an expectation of privacy with their peer-to-peer activity on the Internet." And it ultimately sought to align Johnson's case with United States v. Pobre, No. 8:19-CR-348-PX, 2022 WL 1136891 (D. Md. Apr. 15, 2022), which determined the government's use of Freenet Roundup didn't violate the Fourth Amendment because a Freenet user operating in Opennet mode lacks an expectation of privacy in their activity on the software.

All things considered, the district court ultimately agreed with the government and denied Johnson's motion to suppress, reasoning that he lacked a reasonable expectation of privacy in his Freenet activity. Despite Johnson's choice "to participate in a peer-to-peer network designed to allow censorship-resistant communication and with measures to protect anonymity," the court said, Freenet "warned any user that [their] identification could be discovered and that the choice of Opennet will allow connections with strangers (which could or could not be law enforcement)." The court distinguished "the wholesale cataloguing and disclosure of cell site location information in Carpenter" from Freenet Roundup, "which essentially logs the block requests that are likely to contain suspected CSAM." Though law enforcement employed a modified version of Freenet, as the court explained, it operated "in a forum where Johnson already ha[d] no reasonable expectation of privacy." Accordingly, Freenet Roundup allowed agents to "act[] like an undercover officer crashing a public meeting." Pobre, 2022 WL 1136891, at *6. Lastly, the court acknowledged that it was persuaded by "cases rejecting similar challenges to traditional peer-to-peer networks[,]" and it found Pobre to be on point with Johnson's case.

Following the district court's order and some additional trial preparation, Johnson opted for a conditional guilty plea that preserved his right to appeal the court's suppression ruling.

Thereafter, the court sentenced him to 120 months' imprisonment and five years' supervised release. He timely appealed, and here we are.

III. Standard of Review

We embark on a bifurcated review for appeals of a district court's denial of a suppression motion. See United States v. Tiru-Plaza, 766 F.3d 111, 114 (1st Cir. 2014). Factual and credibility determinations are assessed for clear error, and for such determinations, "we grant significant deference to the district court, overturning its finding only if, after a full review of the record, we possess 'a definite and firm conviction' that a mistake was made." Id. at 114-15 (quoting McGregor, 650 F.3d at 820). The district court's legal conclusions, however, garner de novo review. United States v. Camacho, 661 F.3d 718, 724 (1st Cir. 2011). The "ultimate decision to grant or deny [a] motion to suppress" qualifies as a legal conclusion subject to de novo review. United States v. Centeno-González, 989 F.3d 36, 44 (1st Cir. 2021) (citation modified).

IV. Discussion

Johnson's claims of error closely track his arguments below. But before diving in, we'll tease out the relevant legal rules of the Fourth Amendment.

a. The Fourth Amendment's Shield

Our exposé begins with the bedrock principle that the Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. At bottom, this Amendment is intended "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Carpenter, 585 U.S. at 303 (quoting Camara v. Mun. Ct. of City & Cnty. of S.F., 387 U.S. 523, 528 (1967)). A government actor searching one's home is "presumptively unreasonable" in the absence of a warrant supported by probable cause. See United States v. Karo, 468 U.S. 705, 714-15 (1984).

A Fourth Amendment search occurs when the government violates a person's reasonable expectation of privacy. Kyllo, 533 U.S. at 33. The Amendment's protection therefore hinges on whether the person trying to invoke it can demonstrate they had a reasonable expectation of privacy in the area searched or item seized by a government actor. See Carpenter, 585 U.S. at 304. As we alluded to above, the "reasonable-expectation-of-privacy" inquiry, commonly referred to as the Katz inquiry, see Katz v. United States, 389 U.S. 347 (1967), has both a subjective and objective component. Harper v. Werfel, 118 F.4th 100, 107 (1st Cir. 2024) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979) (citation modified)). A subjective expectation of privacy exists

where a person, "by [their] conduct," demonstrates that "[they] seek[] to preserve something as private." Smith, 442 U.S. at 740. The objective counterpart of the test is satisfied if the person's "subjective expectation of privacy is one that society is prepared to recognize as reasonable." Id. (citation modified). If they fail to meet either component of the Katz inquiry, the warrantless-search challenge becomes futile, and our review will come to a halt.[12] See Centeno-González, 989 F.3d at 47 ("There can only be a Fourth Amendment violation where the complainant had an expectation of privacy in the item that was searched.").

At this point, the reader might be wondering how our standard of review impacts the Katz inquiry. Wonder not, though, for we shall explain. The existence of a person's subjective expectation of privacy "is a question of fact subject to review for clear error." United States v. Guzman, 149 F.4th 1132, 1140-41 (10th Cir. 2025) (quoting United States v. Wells, 739 F.3d 511, 522 (10th Cir. 2014)). The question of a person's objective expectation of privacy lies in the realm of law and is therefore

[12] The question of whether a defendant can successfully demonstrate a reasonable expectation of privacy in the area searched or item seized has been framed as a question of standing. See United States v. Rheault, 561 F.3d 55, 58 n.8 (1st Cir. 2009). Put plainly, a defendant who fails to sufficiently prove their expectation of privacy will lack "standing to claim that an illegal search or seizure occurred." United States v. Vilches-Navarrete, 523 F.3d 1, 13 (1st Cir. 2008) (quoting United States v. Mancini, 8 F.3d 104, 107 (1st Cir. 1993)).

subject to de novo review. See id.; United States v. Rheault, 561 F.3d 55, 59 n.9 (1st Cir. 2009). Because this threshold "standing" question is make-or-break for Johnson's appeal, we'll start (and, as you'll see below, end) here. Let's get into it.

b. Johnson's Reasonable Expectation of Privacy in His Freenet Activity

Johnson puts forth a number of arguments to justify his claim of subjective privacy in his Freenet activity. But the government's response doesn't necessarily oppose Johnson on this point; it states tersely that the question is, "at best, debatable." The government urges us (throughout its brief) not to dwell on the subjective piece but to instead focus on whether Johnson has proven his claim of objective privacy. Because this is the most expeditious route to resolving Johnson's Fourth Amendment claims, we oblige and assume without deciding that Johnson has satisfied the subjective inquiry of the Katz test. So the pièce de résistance of our discussion will be determining whether Johnson adequately justifies his claim of objective privacy in his Freenet activity.

Of first import is this: It is well established that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." United States v. Morel, 922 F.3d 1, 10 (1st Cir. 2019) (quoting Katz, 389 U.S. at 351). But what a person "seeks to preserve as

private, even in an area accessible to the public, may be constitutionally protected." Id. To make our determination, we look at factors such as "ownership, possession and/or control; historical use of the property searched or the thing seized; ability to regulate access; the totality of the surrounding circumstances; . . . and the objective reasonableness of such an expectancy under the facts of a given case." Id. (quoting United States v. Stokes, 829 F.3d 47, 53 (1st Cir. 2016)).

To reiterate, Freenet is a peer-to-peer, file-sharing network that is available at no cost to anyone, anywhere (where legally permitted) with internet access. This court and all of our sister circuits that have considered this question hold that a defendant lacks a reasonable expectation of privacy in content uploaded to publicly-available, peer-to-peer networks. See Morel, 922 F.3d at 10; United States v. Shipton, 5 F.4th 933, 936 (8th Cir. 2021) (stating that "a defendant has no objectively reasonable expectation of privacy in files [they] share[] over a peer-to-peer network, including those shared anonymously with law enforcement officers"); United States v. Ewing, 140 F.4th 1339, 1348 (11th Cir. 2025); United States v. Weast, 811 F.3d 743, 748 (5th Cir. 2016); United States v. Conner, 521 F. App'x 493, 497 (6th Cir. 2013); United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008).

But Johnson sees things differently. Despite Freenet being a publicly-accessible, file-sharing network, still, he feels his claim of an objective expectation of privacy passes muster. His position goes like this: Because the world is becoming ever so digital, his "online movements," much like his physical movements, are likely to reveal his "familial, political, professional, religious, and sexual associations." Carpenter, 585 U.S. at 311. Therefore, he asserts, the Fourth Amendment should prohibit law enforcement from warrantlessly surveilling his online activity. Unfortunately for Johnson, we must stop him in his tracks. With this argument, he is misconstruing the scope of the government's conduct at issue. And as he himself acknowledges, when performing the Katz inquiry, we must pinpoint "the nature of the state activity [being] challenged." Smith, 442 U.S. at 741.

The government contends it did not surveil Johnson's online activity, and, at most, Freenet Roundup captures a user's activity only at the moment the requestor's solicitation is transmitted to the government's node. We agree. The government didn't use Freenet Roundup to surveil the entirety of Johnson's online movements -- in fact, it didn't necessarily surveil *any* of Johnson's online activity. Through Freenet Roundup, the government functioned like an ordinary Opennet-Freenet user -- by using its node to receive others' voluntary requests and retrieve

data blocks -- and by dint of luck (or unluck), some ended up being Johnson's.

True, Freenet Roundup did deviate from the ordinary Freenet software in two material ways. Upon receiving a user's file request, it used the Hops to Live counter to determine whether at least 16 hops out of the 18-Hop-maximum remained and, for those that did, it logged the information transmitted along with the request.[13] The government took additional steps outside the Freenet-verse to ascertain whether the request was for potentially illicit content -- and those steps were: (1) comparing the data blocks' hash values with those in the ICAC's CSAM database, (2) applying a formula to determine whether the request was from the originator, and (3) figuring out the subscriber information for the IP address -- but even taking a conglomerate view of these steps (as Johnson urges us to do thematically throughout his briefs), the government's conduct is far short of surveilling Johnson's online movements. The post-Freenet steps taken by the government are based solely on the timestamped information that Johnson transmitted voluntarily when he initiated his requests, and nothing indicates that the government went beyond that

[13] While testifying at the suppression hearing, Dr. Levine agreed that "if [one] were to break up what the law enforcement node does into two components, one being operation and one being logging, the logging is what makes the law enforcement node unique[,] but the operation is the same as any other user."

information to access any other local files on his private devices. See Ewing, 140 F.4th at 1347. The scope of the government's challenged conduct is therefore limited to its participation on Freenet as an Opennet user (through its Roundup variant) and its use of the information that accompanied Johnson's voluntary requests.

Adamant in his position that his case is on point with Carpenter, Johnson persists. He says (in essence) that much like a cell phone, "almost all of daily life involves the internet" so much so that there's no easy way to avoid using it. And because the internet is made of "a global network of linked computing devices," there's no real means to completely privatize one's use of it (again, his view). Johnson supports his claims by citing portions of Dr. Levine's hearing testimony wherein he explained the difficulty of achieving anonymity on the internet. And where he stated, "[b]y virtue of using the internet, if you expect a reply, which you always do on the internet [i.e., as Johnson expected a reply to his CSAM solicitations], just like a letter in the post office, you have to include your IP address in order to get a response." Given the reality and necessity of operating in such a realm, Johnson contends he should maintain a reasonable expectation of privacy in his internet activity because the mechanics of its operation make it impossible for him to avoid some type of identifiable disclosure.

We beg to differ for this reason. Johnson argues too broadly and fails to direct his challenge towards his voluntary Freenet-specific conduct, as opposed to what he might do or might have done elsewhere on the internet. Indeed, to argue his claim, the specific question he must address (as our precedent instructs) is whether Freenet is so integrated with members of society's, or even its users', everyday lives that it could provide the government with an intimate window into their private details. See, e.g., Harper, 118 F.4th at 109 (assessing whether Coinbase digital currency exchanges are an indispensable part of daily life).

In Carpenter, the Supreme Court explained that a person maintains "a reasonable expectation of privacy in the whole of their physical movements," which prohibits the government from warrantlessly collecting one's cell phone location records to discover their whereabouts. 585 U.S. at 310-11. In making its narrow decision, the Court reasoned that a cell phone is "almost a 'feature of human anatomy,'" id. at 311 (quoting Riley v. California, 573 U.S. 373, 385 (2014)), that "logs a cell-site record *by dint of its operation*," id. at 315 (emphasis added). And "[a]part from disconnecting the phone from the network," said the Court, "there is no way to avoid leaving behind a trail of location data." Id. But, in our view, cell phones and their

stockpile of location data are patently different from the technology involved in this case, and here's why.

Unlike cell phones, Freenet is not so intertwined with its users' lives that it could reveal the "whole of their physical movements." Id. at 310; see also Pobre, 2022 WL 1136891, at *5 (stating that Freenet "is not a ubiquitous part of everyday life as is a cell phone"). Far from it. Instead, it is a rarefied, file-sharing software with limited information on its users' personal lives (insofar as a user chooses to upload personal details onto the platform). Freenet does not "follow[] its [users] beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," Carpenter, 585 U.S. at 311; cf. id. ("[I]ndividuals . . . compulsively carry cell phones with them all the time."), allowing it to "amass a trail of location data," Pobre, 2022 WL 1136891, at *5 (citation modified). Additionally, Freenet Roundup, as described, is unable to "achieve[] near perfect surveillance" of a person's physical movements, thereby categorically excluding it from the "species of technology" that demands more rigid constitutional scrutiny as did the cell phone technology involved in Carpenter. 585 U.S. at 318. The law enforcement tool here simply takes note of bits of information attached to a user's request -- which is shared and visible to users on the normal version of Freenet -- and additional

investigatory steps (explained above) are required to unveil the location of the user's node when the request was sent out. This conduct is in stark contrast to warrantlessly collecting "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years" through a person's cell phone location records. See id. at 315.

Resisting that logic, Johnson argues that we should not deem his expectation of privacy unreasonable solely because researchers have created software and come up with a mathematical formula that allows the government to bypass Freenet's anonymity and privacy protections. He directs us (once more) to Dr. Levine's suppression hearing testimony, wherein he stated that his interest in developing Freenet Roundup was "because law enforcement . . . found it difficult to conduct investigations" on that platform. In other words, says Johnson, routine law enforcement tools would not have allowed the disclosure of his identity. Continuing, Johnson says in light of Freenet's assurances that it was better at protecting anonymity than similar products, notwithstanding Freenet's cautionary warnings about the risks of being identified when using the platform, it was reasonable for him to believe that no ordinary Freenet user would be capable of or even interested in "developing a mathematical formula, modifying Freenet, and collecting the data necessary" to reveal the contents of his requested files or of the requestor's

origin. And, as Johnson urges, the Fourth Amendment must evolve to account for these ever-emerging advancements in technology. Put differently, his claim is that Freenet Roundup amounts to law enforcement's use of advanced technology to gather information akin to that which would normally require physically invading a constitutionally protected area.

Color us unpersuaded. Freenet Roundup does not amount to exclusive, enhanced technology that provides the government with a backdoor into a person's private life. Cf. Kyllo, 533 U.S. at 40 (prohibiting the government from using technology "that is not in general public use" to learn the private details of a person's home). Freenet Roundup works only to "facilitate[] [the government's] membership into Freenet and record[] the file requests that the [government node] receives." Pobre, 2022 WL 1136891, at *6. Aside from logging and filtering information that accompanies each request voluntarily sent to other Freenet users, as we've discussed, Freenet Roundup otherwise operates like a normal user on the platform. These actions therefore could not fairly be viewed as conduct involving technology that "is not in general public use." Kyllo, 533 U.S. at 34; see Ewing, 140 F.4th at 1349 (stating law enforcement used "Torrential Downpour" to "merely scan[] publicly available information . . . not shrink the realm of guaranteed privacy by exposing information that was not already broadcast to the public" (citation modified)).

Johnson's mention of the government's purportedly sophisticated hash value cataloguing and application of its mathematical formula does not change our minds. Dr. Levine testified that he used "standard techniques" and that he "didn't invent some crazy math to" design the formula. And as described, it uses only the information transmitted as part of the user's request -- such as the number of immediate peers a Freenet user has and the remaining number of Hops for each request it logs -- to calculate the likelihood that the request came from the originator. Nothing on the record suggests to us that this conduct is so advanced and out of reach, especially when Freenet itself warned that users with "moderate resources" could ascertain similar information. Further, once Johnson voluntarily sent out his request, he could neither reasonably expect the information to remain private nor control how strangers would use the information, which applies equally when the government lawfully obtains potentially incriminating information. Compare Boroian v. Mueller, 616 F.3d 60, 67 (1st Cir. 2010) (noting that courts have held "the government's matching of a lawfully obtained identification record against other records in its lawful possession does not infringe on an individual's legitimate expectation of privacy"), with Carpenter, 585 U.S. at 314 (stating that, under the third-party doctrine, "an individual has a reduced expectation of privacy in information knowingly shared with

another"). Thus, the government's use of information Johnson voluntarily disseminated on Freenet does not alter our conclusion. See United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information.").

The government posits that by using Freenet Roundup to receive requests Johnson voluntarily sent to strangers on Freenet, its actions are more akin to that of an undercover officer invited to participate in an illicit transaction. See Lewis v. United States, 385 U.S. 206, 210-11 (1966). But Johnson pushes back on such a comparison and says it is inapt. He suggests that, unlike being chatty with an undercover, he "relied on the privacy-protection" afforded by Freenet, "not on his confidence in other Freenet users." Johnson argues that he didn't announce to anyone on Freenet (or otherwise) that he sought to download CSAM, and, normally, the users receiving his requests have no idea of the contents of any particular block or file. Thus, society should see his expectation of privacy as reasonable.

We remain unconvinced by Johnson's argument and instead, our view tracks that of the government's. Similar to inviting an "undercover agent to [their] home for the specific purpose of executing a felonious sale of narcotics," id. at 210, Johnson voluntarily connected his computer to strangers on Freenet to

retrieve files. Even when warned throughout his time on the platform, Johnson never opted to toggle on Freenet's more-privatized Darknet mode.[14] And the government never targeted Johnson specifically, nor did it ever solicit his Freenet requests. What law enforcement did do was go on Freenet as an Opennet-user (something Johnson does not argue was improper governmental conduct in and of itself), and that is what caused it to receive peers' requests, including the illicit ones Johnson initiated. See Pobre, 2022 WL 1136891, at *6 ("From this, the [c]ourt cannot conclude that the technology did anything more than receive that which Pobre and others willingly shared in Freenet."). Such conduct does not violate the Fourth Amendment.

Johnson won't budge. He says Freenet's warnings don't defeat his privacy claims because they signal only that a user's identity could be discovered, not that they could be made out as the original requestor of a file or that the contents of a requested file could be revealed. He's wrong. Freenet warned Johnson -- like all users operating in Opennet mode -- that his IP address was vulnerable to identification, that "an attacker with moderate resources may be able to trace [his] activity on Freenet back to [him,]" and that "[i]t may be quite easy for others to

[14] To be clear, we are not saying that a Freenet user operating in Darknet mode would have a reasonable expectation of privacy in their activity on the platform. We leave that question for another day.

discover [his] identity." He was therefore adequately warned that he was opening his Freenet transmissions to the world, including the world of the government. See Ganoe, 538 F.3d at 1127. And despite any purported ambiguity in the warnings, Johnson was *at least* on notice that his activity could be traced back to him. What's more, by continuing to use Freenet in Opennet mode after the warnings were displayed, Johnson failed to take any "affirmative steps to protect the [files]" by switching to Darknet mode. Morel, 922 F.3d at 10. He presents to us no case, and we are aware of none, that suggests society would deem his expectation of privacy reasonable because he believed only some aspects of his identity were discoverable.

Finally, Johnson asserts that Freenet is materially different from other peer-to-peer networks, and therefore, any cases involving those other platforms are inapplicable. As opposed to traditional networks in which users open their computers and files to the public, he contends that Freenet's users can only access encrypted data blocks that are unidentifiable without a manifest key. Johnson says these files are not made public in a way that would call into question a Freenet user's expectation of privacy.

Again, we disagree. Despite his many claims that he used Freenet to anonymize his file-sharing activity to the furthest extent possible, (to repeat) Johnson voluntarily operated on

Freenet in low security Opennet mode when transmitting his requests after being explicitly warned of that mode's shortcomings. Because of his personal choice to connect with total strangers on Freenet, we see no meaningful difference between Freenet and other peer-to-peer, file-sharing networks. Once he chose to connect openly in the Freenet-verse, "his expectation of privacy ha[d] already been frustrated." Ewing, 140 F.4th at 1348 (citation modified). And "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information." Id. (alteration in original) (quoting Jacobsen, 466 U.S. at 117).

Against all of this, Johnson has failed to prove a reasonable expectation of privacy in his Freenet activity, and we needn't inquire any further. See United States v. Mayendía-Blanco, 905 F.3d 26, 37 (1st Cir. 2018) (stating that "[t]he simplest way to decide a case is often the best" (alteration in original) (quoting Stor/Gard, Inc. v. Strathmore Ins., 717 F.3d 242, 248 (1st Cir. 2013))).

V. Conclusion

Johnson's challenge to the district court's denial of his suppression motion is unsuccessful. The matter is thus **affirmed**.