

United States Court of Appeals For the First Circuit

No. 21-1832

UNITED STATES,

Appellee,

v.

SHUREN QIN,

Defendant, Appellant.

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

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

Before
Barron, Chief Judge
Howard and Kayatta, Circuit Judges.

Michael R. Schneider, with whom Good Schneider Cormier & Fried
was on brief, for appellant.

Karen L. Eisenstadt, Assistant United States Attorney, with
whom Rachael S. Rollins, United States Attorney, was on brief, for
appellee.

January 9, 2023

BARRON, Chief Judge. In this appeal, Shuren Qin challenges his federal convictions in the District of Massachusetts for conspiracy to commit export violations, visa fraud, making false statements to federal agents, money laundering, and smuggling. He does so on the ground that the government relied on the fruits of what he contends was an unconstitutional search of his laptop and cellular phone after those devices were seized upon his re-entry to this country after traveling to China. Because we conclude that the search constituted a border search that was supported by reasonable suspicion that Qin was engaged in the ongoing violation of export laws, we affirm.

I.

Qin is a Chinese national who lives part of the year in Massachusetts and part of the year in Qingdao, China. He is President of LinkOcean Technologies, Ltd. ("LinkOcean"), a company based in Qingdao, China that imports and resells marine technology from the United States, Canada, and Europe to customers in China, including Chinese research institutes and the Chinese Navy.

On November 24, 2017, Qin and his wife returned to the United States from a trip to China. Soon after their arrival, two Customs and Border Patrol ("CBP") agents, at the request of agents from other agencies who had been investigating Qin's export

activities for roughly seven months, conducted an interview of Qin in the public baggage claim area in the airport.

The CBP agents asked Qin during the interview about his export activities and to see shipping documents related to his exports. According to one of the CBP agents, Qin answered that he "only" exported items that "attach to buoys."

After Qin indicated that the laptop and phone that he carried with him were used for business, the CBP agents seized those electronic devices for a further search and permitted Qin to leave the airport. Immediately after Qin's devices were seized, the agents who had been conducting the investigation into Qin's export activities brought the devices to the Homeland Security Investigations ("HSI") forensic lab to be imaged and searched.

The laptop contained 776 gigabytes of data, and the phone contained approximately 55 gigabytes of data. The "overwhelming majority" of the content on the devices was in Mandarin, and the language translation tool that the agents conducting the search had downloaded did not provide adequate translations. No local agents could read, write, or translate Mandarin, and the agents searching Qin's devices waited until an agent from New York could travel to the area to assist them. The agents searching Qin's devices sought passwords from Qin to access the encrypted items on his computer, but Qin did not provide them.

During the Mandarin-speaking agent's second trip to Boston, near the end of the 60-day period within which the search took place, the agents searching Qin's devices came across emails that provided evidence that Qin had illegally exported hydrophones to Northwestern Polytechnical University ("NWPU"), a Chinese university with military ties. The agents completed the search of the electronic devices after 60 days. After the search was completed, the agents did not return the electronic devices to Qin. Instead, the agents held the laptop for 11 more days and the phone for 153 more days as the agents applied for and obtained a search warrant, which they used to conduct an additional search.

In October 2018,¹ Qin was indicted based on the evidence of illegal exports of hydrophones to NWPU found during the 60-day warrantless search of his devices. The indictment charged him with conspiring to illegally export parts from the United States to China, 50 U.S.C. § 1705; visa fraud, 18 U.S.C. § 1546(a); conspiring to defraud the United States, 18 U.S.C. § 371; making false statements, 18 U.S.C. § 1001; money laundering, 18 U.S.C. § 1956; and smuggling, 18 U.S.C. § 554.

In September 2019, Qin moved to suppress the fruits of the warrantless search conducted on his laptop and phone. The

¹ Qin was initially served with a three-count indictment on June 26, 2018, before being served with a 14-count superseding indictment on October 30, 2018.

District Court issued a memorandum and order denying the suppression motion. The District Court ruled that the search was a "non-routine border search" and that the search was lawful because the agents who searched Qin's devices had reasonable suspicion at the time of the search that Qin's devices contained evidence of "export violations."²

After the District Court's ruling, Qin entered into a plea agreement with the government that "reserv[ed] [his] right to appeal the denial of his Motion to Suppress Evidence obtained from his laptop computer and Apple iPhone." Qin timely appealed for review of the District Court's decision to deny his motion to suppress. "In reviewing motions to suppress, we review [the District Court's] legal determinations de novo" and its "factual findings for clear error." United States v. Bater, 594 F.3d 51, 55 (1st Cir. 2010).

II.

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. It

² The District Court stated that the agents who searched Qin's devices had reasonable suspicion "that the electronic devices, which Qin identified as devices he used for work, would contain evidence of export violations, including but not limited to causing the filing of false EEI, visa fraud . . . , and, after his statements to CBP agents about the limits of his exports (which the investigating agents reasonably believed to be false), false statements to federal agents."

further provides that "no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Id.

Border searches -- which the Supreme Court has described as searches of travelers and "belongings" "crossing an international boundary" of the United States, Carroll v. United States, 267 U.S. 132, 154 (1925) -- have long constituted an exception to the Fourth Amendment's warrant requirement. See United States v. Ramsey, 431 U.S. 606, 621 (1977). The exception derives from a recognition of the government's "inherent authority to protect, and a paramount interest in protecting, its territorial integrity." United States v. Flores-Montano, 541 U.S. 149, 153 (2004).

We have distinguished between "routine" and "non-routine" border searches. The former type of search may be conducted not only without a warrant upon probable cause but also without the government having any reasonable basis for suspecting that it will turn up "contraband, evidence of contraband, or . . . evidence of activity in violation of the laws enforced or administered by CBP or ICE." Alasaad v. Mayorkas, 988 F.3d 8, 19-21 (1st Cir. 2021). The latter type of search, though it also may be conducted without a warrant upon probable cause, must be

supported by reasonable suspicion that the search will turn up contraband or evidence of the sort just described.³ Id. at 18.

The required reasonable suspicion must be "objective" and based on "specific and articulable facts . . . taken together with rational inferences from those facts." Terry v. Ohio, 392 U.S. 1, 21 (1968). The evidence needed to support reasonable suspicion is less than that needed to support probable cause and "considerably" less than that needed for "proof of wrongdoing by a preponderance of the evidence." United States v. Sokolow, 490 U.S. 1, 7 (1989).

III.

We begin with Qin's contention that insofar as the District Court was right to rule both that the search at issue was a border search and that it was "non-routine,"⁴ the search still violated the Fourth Amendment because the District Court erred in

³ Whether a search is "'routine' or 'not routine' often depends on the 'degree of invasiveness or intrusiveness associated with' the search." United States v. Molina-Gómez, 781 F.3d 13, 19 (1st Cir. 2015) (quoting United States v. Braks, 842 F.2d 509, 511-12 (1st Cir. 1988)). "[N]on-routine" border searches involve a greater "degree of invasiveness or intrusiveness" than "routine" searches. Id. In assessing whether searches of electronic devices are routine or non-routine, this court has considered factors including whether the searches were conducted manually so as to limit the amount of content reviewed; whether the data reviewed was "resident on the device;" and whether "deleted or encrypted files" were viewed. See Alasaad, 988 F.3d at 18-19.

⁴ The government does not dispute on appeal the District Court's ruling that the type of border search that was conducted here was a non-routine one.

finding that the government had demonstrated that the agents who searched Qin's devices had the required reasonable suspicion. Qin understands the ruling to rest on the ground that the record supportably shows that the agents who searched his electronic devices had reasonable suspicion that the devices would contain evidence of Qin's ongoing efforts to export controlled marine instruments to China without proper licensure in violation of U.S. export laws. But, Qin contends, the record simply does not show as much. We disagree.

Well before the CBP agents interviewed Qin at the airport about his export activities concerning China, federal agents from a number of agencies had been investigating those activities. And from that investigation, those agents had already generated evidence of the following kinds.

First, the agents who had been investigating Qin's export activities had gathered evidence that reasonably led them to conclude that Qin had shown a past interest in flouting U.S. export laws while conducting his business with clients in China. This evidence included Qin's expression of interest in using a common practice to evade U.S. export laws, namely the establishment of a front company based in the United States. In Qin's case, the front company that he expressed interest in creating would purchase autonomous underwater vehicles ("AUVs") without a U.S. export license and then unlawfully export the unlicensed AUVs to China.

An AUV is a type of unmanned underwater vehicle ("UUV") that can "operate without being 'tethered' to another vehicle." The evidence of Qin's past interest in flouting U.S. export laws that the agents investigating his export activities had gathered also included his request to an undercover agent posing as a U.S. seller of AUVs not to disclose to a U.S. manufacturer of AUVs -- who bears responsibility for acquiring an export license when a product is sold for export to China -- that the end users for the AUVs that Qin was seeking were in China.

Second, the agents investigating Qin's export activities had gathered evidence that the clients of Qin's company, LinkOcean, included entities to which the United States restricted or prohibited certain kinds of exports. These clients included Chinese research institutes⁵ and the PLA Navy, which is the naval warfare branch of the Chinese Army that oversees the development and operation of surface warships, submarines, and unmanned submersible vehicles.

Third, the agents investigating Qin had gathered evidence that Qin had expressed interest in exporting products to

⁵ Although the research institutes that the agents knew to be clients of LinkOcean were not on the "Entity List," which identifies entities that are believed to be involved in "activities contrary to the national security or foreign policy interests of the United States" and requires additional licensing requirements, see 15 C.F.R. § 744.16, certain products require a license if they are shipped to any client in China, including the research institutes that the agents were aware were Qin's clients.

China through LinkOcean that require export licenses, including AUVs. And, relatedly, the agents knew at the time of the search that Qin had expressed an interest in exporting to China products that are on the U.S. Munitions List and cannot be exported from the United States to China under the U.S. Arms Embargo against China -- namely, sonobuoys, which are defense articles used in anti-submarine warfare.

Finally, the agents investigating Qin had gathered evidence concerning Qin's willingness to conceal the nature of his export activities from authorities. This evidence included documents filed with the U.S. government concerning approximately 31 of LinkOcean's transactions involving exports that listed LinkOcean as the "ultimate consignee," even though the company was a reseller of the exported products and was often or always aware of the identity of the end users of those exported products. The evidence also included Qin's having asked a U.S. seller not to disclose the end user for a product when the seller filled out the export documents to provide to the U.S. government.

Thus, all that evidence had already been gathered in the course of the investigation into Qin when the CBP agents questioned him at the airport as he was returning from China about the nature of his exports to China. And so, after Qin answered during that

questioning that he exported "only" items that "attach to buoys,"⁶ as the District Court found that he did, we conclude that at least at that point, the agents who then conducted the search of Qin's electronic devices had reasonable suspicion that Qin was engaging in the kind of unlawful export activities that he contends the record fails to show that the agents had reason to suspect. For, at least as of that point, the agents who conducted the search of Qin's electronic devices not only had all the information gathered throughout the investigation into his export activities that we have described above. Those agents as of that point also had been informed of what the CBP agents had interpreted as Qin's lie to them about the nature of his export activities to China. See United States v. Favreau, 886 F.3d 27, 30 (1st Cir. 2018) (finding that a "patent lie" to agents can, along with other evidence, support a reasonable suspicion that someone is "in fear of revealing evidence of wrongdoing"); United States v. Wright, 582 F.3d 199, 213 (1st Cir. 2009) (finding that "reasonable suspicion arises not just from the combination of facts, but from their progression"); Sokolow, 490 U.S. at 8-9 (finding that reasonable suspicion requires reviewing the "totality of the circumstances"); United States v. Ruidíaz, 529 F.3d 25, 30 (1st Cir. 2008)

⁶ The agents had evidence that Qin exported remotely operated side scan sonar systems, UUVs, unmanned surface vehicles, and hydrophones, which do not attach to buoys.

(explaining that "individual facts, taken in the aggregate [may be] sufficient to trigger a reasonable suspicion that some criminal activity was afoot -- and that the defendant was involved").

Moreover, Qin does not dispute that, if the agents who conducted the search were armed with the requisite suspicion concerning his ongoing violations, then they would have had reason to suspect that evidence of the suspected export violations would be contained on Qin's electronic devices. Accordingly, we conclude that the record shows that the agents possessed the requisite reasonable suspicion to search those devices.

Qin challenges this conclusion in part by arguing that the agents who searched his devices could not have reasonably believed that he lied to CBP agents at the airport about whether he exported "only" items that attach to buoys. In particular, he argues that the agents who searched his devices had evidence that he was not very fluent in English and that he said that things that "attach to buoys" are "the types of things" that he exported to China rather than the "only" things. But, given the evidence in the record that Qin spoke "excellent" English and the CBP agents' reports about Qin's responses to their questions, the District Court did not clearly err in finding that the agents reasonably believed that Qin lied to them about the types of products that he exported. See United States v. Espinoza, 490 F.3d 41, 46 (1st Cir. 2007) ("[W]hen two or more legitimate

interpretations of the evidence exist, the factfinder's choice between them cannot be deemed clearly erroneous.").⁷

Qin separately argues that there were innocent explanations for the conduct that the government contends supported the reasonable suspicion of the agents who searched Qin's devices and that the agents who searched those devices were aware of such explanations when they conducted the search. In particular, Qin argues that the record shows that the agents who searched his devices were aware that some of the technologies that he sought were used for academic in addition to military purposes; that he had financial incentives to conceal the end users of the

⁷ We note as well that our conclusion is not undermined even if we accept Qin's contention that the diagrams Qin showed to the CBP agents during the interview portrayed technologies that Qin exported that do not necessarily attach to buoys, given that Qin does not contend that the technologies depicted cannot attach to buoys. We also note that there is no merit to Qin's contention that the agents who searched Qin's devices could not have had reasonable suspicion at the time of the search in November simply because they conceded they did not have such suspicion in October and nothing happened between October and November. In addition to the fact that the agents who searched Qin's devices obtained evidence that Qin had lied to CBP agents at the airport in November, the agents' subjective experience is not the relevant inquiry. See United States v. Arvizu, 534 U.S. 266, 273 (2002). Rather, the relevant inquiry is an objective one based on all "the cumulative information available to [the agents]" at the time of the search. Id. And, because the inquiry is an objective one, we also reject Qin's contention that the agents who searched his devices could not have relied on the lie as a predicate for determining that they had reasonable suspicion because the agents had decided to conduct the search weeks before the lie. See id.

products he exported on some occasions; and that "some of the components of the sonobuoys [that Qin was interested in] may have been made in Canada" and may therefore not be barred for export by U.S. export controls. Qin relatedly argues that the evidence that the export documents associated with his transactions did not disclose who his end users were could not have reasonably generated suspicion, because disclosure of end users is not legally required under U.S. export regulations. He further contends that even if such disclosure was legally required, it was U.S. sellers -- rather than buyers like Qin -- who were responsible for submitting the information to the U.S. government and thus for any omissions in the information submitted.

But, in pressing these specific points, Qin does not dispute that the agents had evidence of Qin's past expression of a willingness to violate export laws, the nature of the clients of his company in China, the products that he was interested in exporting to China, and his misleading answer to the agents at the airport about his export activities with China. Nor does Qin dispute that the agents possessed evidence that the export documents associated with approximately 31 of his export transactions did not disclose the end users of the items exported in those transactions or that Qin asked one seller not to disclose the end user for a product when the seller filled out the export documents to provide to the U.S. government. Thus, Qin's focus on

the favorable inferences that could be drawn from the evidence that the agents who searched his devices had is ultimately a contention that those agents knew from that evidence that there existed "the possibility of innocent conduct." Wright, 582 F.3d at 205 (quoting Arvizu, 534 U.S. 266, 277 (2002)). But, the agents need not have ruled out that possibility to have reasonably suspected that the conduct was not innocent, id., and, for the reasons explained above, the unique "factual mosaic" that the collection of evidence in this case created, see United States v. Pontoo, 666 F.3d 20, 28 (1st Cir. 2011), gave rise to the required reasonable suspicion of ongoing export violations.

Qin does also highlight evidence in the record that he contends shows that the agents who searched his devices knew of his past honesty and lawfulness in some contexts concerning his export activities, as if that evidence suffices to establish that the agents did not have reason to suspect his ongoing violation of export laws. For example, Qin notes that he listed the Chinese Navy as one of LinkOcean's clients on the LinkOcean website; he was "very open" with some prospective business partners about who his clients were; he "repeatedly asked" a U.S. seller and an undercover agent to submit the paperwork required to obtain export licenses; and he decided not to purchase sonobuoys because he believed that sonobuoys "require[d] an exporting license or permit."

But, this evidence at most shows that the agents who searched Qin's devices knew that Qin sometimes revealed who his clients were and sometimes chose to abide by the law. Such evidence does not show -- indeed, does not even purport to show -- that the agents lacked all the evidence that the record supportably shows they also had, which included evidence of his past expression of interest in violating the export laws, the nature of his clients, the products he was interested in exporting, his lie to the agents at the airport, and the concealment of his end users.

Thus, here, too, Qin is necessarily equating evidence that might support a conclusion that his conduct was innocent with evidence that could refute other evidence that, based on a "broad-based consideration of all the attendant circumstances," United States v. Brown, 500 F.3d 48, 54 (1st Cir. 2007), including "objective observations" coupled with "consideration of the modes or patterns of operation of certain kinds of lawbreakers," United States v. Cortez, 449 U.S. 411, 418 (1981), supports a reasonable suspicion that the conduct is not innocent. But, evidence that can support the possibility of innocent conduct is not evidence that, on its own, suffices to show that there was no evidence of the required reasonable suspicion.

We thus find that, given the specific facts of this case, taken all together, the agents conducting the search of Qin's

devices had reasonable suspicion that Qin was exporting controlled marine instruments to China without proper licensure, in violation of U.S. export laws. And, Qin does not dispute that, insofar as the agents had such suspicion, they also had a reasonable basis to suspect that evidence of this unlawful activity was contained on the electronic devices searched by the agents. Accordingly, we reject Qin's contention that the record shows that the agents who conducted the search of Qin's electronic devices did not possess the requisite reasonable suspicion needed to justify a non-routine border search of those devices.

IV.

Qin next argues that, even if we were to assume that the agents who conducted the search of his electronic devices had the reasonable suspicion required for a non-routine border search, the search of those devices did not constitute a border search at all. Qin is right that if the search at issue was not a border search at all, then it would require both a warrant and probable cause, rather than merely reasonable suspicion that the electronic devices would contain evidence of his ongoing export violations. See Riley v. California, 573 U.S. 373, 382 (2014). The District Court rejected the arguments that Qin makes to us as to why the search did not constitute a border search, however, and we do so as well.

Qin rests his argument that the search at issue did not constitute a border search in part on its "duration," which he contends was so long that the search became disconnected from efforts to regulate the border and prevent border-related crime and therefore no longer fell into the border search exception. Qin notes that the search of his devices lasted 60 days and so fell beyond the 22-day search of a laptop that was upheld in Molina-Gómez as "not unreasonable" but that "seem[ed] lengthy."⁸ United States v. Molina-Gómez, 781 F.3d 13, 21 (1st Cir. 2015). The search was also longer, Qin points out, than the 14-day search that at least one other court found not to be a border search given its length and scope, see United States v. Kim, 103 F. Supp. 3d 32, 57-58 (D.D.C. 2015), as well as the "presumptive" 30 days allotted for a search under HSI policy.

The search at issue in this case certainly pushes the bounds of what may reasonably fall into the border search exception, and we by no means hold categorically that a search that lasts sixty days and otherwise qualifies as a border search falls within the border search exception. The inquiry is context

⁸ To the extent Qin did not waive the argument that, after the 60-day search concluded, the government impermissibly detained his computer for an additional eleven days and his phone for an additional 153 days while seeking a warrant, we do not see how that argument bears on the only issue before us in this appeal, namely whether the District Court erred in denying Qin's motion to suppress the evidence gathered during the preceding 60 days.

specific and fact dependent. We hold only that, on this record, the duration of the search did not in and of itself render it so disconnected from the purpose of the border search exception that it falls outside the scope of that exception, given the District Court's findings that the length of the search was justified by the amount of data that the electronic devices contained, as well as the language barriers and encrypted files that impeded access to that data.

The Supreme Court has "consistently rejected hard-and-fast time limits" on border searches and has instructed that, "[i]nstead, 'common sense and ordinary human experience must govern over rigid criteria.'" United States v. Montoya de Hernandez, 473 U.S. 531, 543 (1985) (quoting United States v. Sharpe, 470 U.S. 675, 685 (1985)). And, while the search did exceed the 30 days that HSI policy identifies as presumptively reasonable for a border search, it did not exceed the 60 days that HSI policy itself has identified as permissible when, as in this case, extensions beyond 30 days are merited by the fact-specific challenges that the search being conducted poses.

Qin contends in response that the justifications the government puts forth for the length of the search do not in fact justify the length. On this score, he first contends that much of the content on the laptop was in English and thus did not require translation. But, he does not contest that much of the content on

the laptop was also in Chinese. And, searching this content required a Mandarin-speaking agent who could not assist with the search for several weeks.

Qin also argues that the agents' contention that they needed to detain his devices while waiting for Qin to provide them with passwords is undermined by the fact that the advanced encryption mechanisms that the agents were most concerned about, including PGP, Keychain, and Bitlocker, were not used on the laptop. Qin does not suggest, however, that the laptop did not contain any relevant encrypted items for which a password was needed, so his argument does little to call into doubt the District Court's finding that the encrypted items -- and the wait for the passwords -- helped justify the length of the search.

Qin separately argues that, independent of the length of the search, it was sufficiently intrusive to be not a border search but rather "a general exploratory search in the hope that evidence of a crime might be found." See Go-Bart Importing Co. v. United States, 282 U.S. 344, 356-58 (1931). Qin argues in this connection that the government used keyword searches to look for a broad array of business records, financial documents, and technical documents and schematics.⁹

⁹ We note that Qin acknowledges that, under Alasaad, border searches can include searches not only for "contraband or evidence of contraband," but also for evidence of border-related crime, see

But the fact that the agents used keywords to search for such records, documents, and schematics does not, on its own, show that the search fell outside the scope of a border search, given the nature of the suspected criminal activities concerning the conduct of Qin's business. After all, such records, documents, and schematics can contain "contraband, evidence of such contraband, or . . . evidence of activity in violation of the laws enforced or administered by CBP or ICE," all of which can be searched for during a border search. Alasaad, 988 F.3d at 21. Moreover, Qin does not point to any specific keywords that, he says, were used for the purpose of a general exploration rather than a search for information about the ongoing export violations of which the agents were suspicious. Thus, we do not see how Qin's assertion about the keywords used by the agents turns this search into a general exploratory search.

Qin does also advance the related contention -- in arguing that the search was too intrusive to constitute a border search -- that, while searching his laptop, the government looked "broadly for evidence of past and future crime," not "ongoing or imminent" criminal conduct. To support this contention, Qin points

988 F.3d at 21, and that Alasaad governs our decision in this case. And while Qin argues that we should revisit Alasaad en banc and hold that border-related searches should not include evidence of border-related crime, that contention has no bearing on how we must rule as a panel.

out that the agents continued to search for evidence even after they saw that the last email on the laptop was from May 2017.

But, the record shows that the laptop did contain evidence created after May 2017, and there is nothing in the record to indicate that the agents were not searching this later evidence. Moreover, old emails can shed light on future actions, so the agents could have reasonably believed that the old emails were relevant to their search for ongoing conduct. Thus, we do not see how Qin's contention about the date of the last email on the laptop supports a finding that the agents only searched for past criminal conduct.

Accordingly, we conclude that neither the length nor scope of the search at issue placed it outside the scope of a border search and thus that neither probable cause nor a warrant was required for the search to be lawful under the challenges posed and the Fourth Amendment. And that is so in this case, even taking into consideration both how long the search lasted and how comprehensive it was, given the suspicion that the agents who searched Qin's electronic devices reasonably had that a search of those devices would turn up evidence of his ongoing export violations.¹⁰

¹⁰ Because we conclude that the agents in this case had reasonable suspicion to conduct the search at issue, we need not address Qin's argument that, if the agents' search was not

v.

For the foregoing reasons, the judgment of the District Court is **affirmed**.

supported by reasonable suspicion, the fruits of their search should be suppressed because the agents did not act in good faith.