CASE NO. 18-1366

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,	)
	)
Plaintiff–Appellee,	)
	)
v.	)
	)
JAMSHID MUHTOROV,	)
	)
Defendant–Appellant.	)

On Appeal from the United States District Court
for the District of Colorado
The Honorable John L. Kane, Senior U.S. District Judge
D.C. Case No. 1:12-cr-00033-JLK-1

APPELLANT'S SUPPLEMENTAL REPLY BRIEF TO THE GOVERNMENT'S CLASSIFIED, EX PARTE BRIEF

PATRICK TOOMEY
ASHLEY GORSKI
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

VIRGINIA L. GRADY
Federal Public Defender

JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002

October 29, 2020

Table of Contents

Table of Authorities

Cases

Statutes

Other Authorities

Rules

Introduction

On August 24, 2020, this Court ordered the government to conduct a declassification review of its classified, ex parte brief and the exhibits thereto. In response, on October 8, 2020, the government publicly filed a partially redacted version of its ex parte brief and addendum, which included several ex parte district court filings. The government's brief and addendum feature declassified facts and legal arguments that Mr. Muhtorov initially sought six years ago, and that the government is only now disclosing (in limited form) for the first time. Mr. Muhtorov submits the following response to the government's belated disclosures.

Argument

I. The Court must consider the government's warrantless "backdoor searches" in evaluating the constitutionality of Section 702 surveillance.

In its ex parte brief, the government asserts that this Court need not address Mr. Muhtorov's arguments concerning "backdoor searches," on the theory that its FISA evidence was not "obtained or derived" from any such queries. Gov't Suppl. Br. 10-11. The government is wrong. For several reasons, this Court's Fourth Amendment analysis must take into account the government's warrantless queries.

First, as Mr. Muhtorov has explained, the government waived this argument by failing to present it below, instead arguing at length that its warrantless backdoor searches were lawful. Def. Reply 11.

Second, the government's effort to carve its backdoor searches out of the case is incompatible with black-letter law. Under the Fourth Amendment, when evaluating the reasonableness of the government's Section 702 surveillance, the Court's analysis must consider the "totality of the circumstances." *Samson v. California*, 547 U.S. 843, 848 (2006). As discussed below, this requires an assessment of the Section 702 procedures that applied to the use of Mr. Muhtorov's private information. Backdoor searches are a key element of those procedures: the FBI is permitted and encouraged to routinely use backdoor searches, and agents conduct such queries in investigations *millions* of times each year. [*Redacted*], 402 F. Supp. 3d 45, 74-75 (FISC 2018). Indeed, the record continues to support the conclusion that FBI agents conducted backdoor searches as part of their investigation of Mr. Muhtorov, as agents do "whenever the FBI opens a new national security investigation or assessment." Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702*, at 59 (2014), https://perma.cc/WD5R-5GKE; Def. Br. 25-26.

The government does not deny that agents conducted backdoor searches of Mr. Muhtorov in the FBI's Section 702 databases as part of their investigation. *See* Gov't Suppl. Br. 2. Instead, it makes a far narrower claim, asserting that any warrantless queries for Mr. Muhtorov's communications did not lead directly to

the Section 702 communications that the government cited in its FISA application. *Id*. at 11. But even if that were true, the government is wrong to argue that these intrusive searches have no bearing on the Court's Fourth Amendment analysis. To the contrary, they are part and parcel of assessing the reasonableness of the surveillance here "under the totality of the circumstances." *Samson*, 547 U.S. at 848.

For electronic surveillance, this test has a well-defined scope: courts consider the breadth of the government's intrusions on privacy, including the strength or weakness of the minimization rules. Def. Reply 6-7 (collecting cases); *see Berger v. New York*, 388 U.S. 41, 58 (1967); *In re Sealed Case*, 310 F.3d 717, 737-41 (FISCR 2002); *United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984) (analyzing "the procedures fashioned in FISA"); [*Redacted*], 402 F. Supp. 3d at 75 (explaining that "the rules for U.S.-person queries are especially important for minimization of Section 702 information").

Because reasonableness depends on the nature and degree of the privacy invasion, a court must consider whether the rules that apply to the surveillance as a whole are sufficiently protective—from acquisition, to retention, to *use*. Contrary to the government's claim, this is not a piecemeal exercise that depends on tracing each defect in the surveillance to the government's evidence at trial. Def. Reply 6-7. For example, in *Berger*, 388 U.S. at 55, the Supreme Court observed that the

petitioner "clearly ha[d] standing to challenge" the wiretap statute at issue, because he was "indisputably affected by it." Having reached that conclusion, the Court proceeded to examine numerous defects in the statutory wiretap procedures, without regard to whether those particular defects bore directly on the government's trial evidence. *See id.* at 55, 58-60.[1]

In fact, the Supreme Court has expressly held that, when evaluating broad electronic searches, a court must consider even those aspects of the intrusion that do not lead to evidence at trial. In *Scott v. United States*, 436 U.S. 128, 142-43 (1978), the Supreme Court weighed, as part of its Fourth Amendment analysis, the government's interception of seven phone calls between the defendant and her mother—even though "none of these conversations turned out to be material to the investigation at hand." *See also, e.g.*, *United States v. Hyde*, 574 F.2d 856, 870 (5th Cir. 1978) (analyzing interception of privileged communications that did not produce evidence of conspiracy). Courts take this approach because electronic searches are often expansive, enabling the government to seize large amounts of private information that is unrelated to the government's investigation. *See United*

[1] The government's argument that it ultimately obtained Mr. Muhtorov's communications using FISA, independent of any backdoor searches, fails for similar reasons. Gov't Suppl. Br. 11 (citing *Murray v. United States*, 487 U.S. 533, 542 (1988)). It is undisputed that the government's FISA application relied on its Section 702 surveillance of Mr. Muhtorov's communications. The reasonableness of that surveillance depends on the safeguards as a whole—including those that allowed agents to freely query Americans' communications.

States v. Ganias, 824 F.3d 199, 217-18 (2d Cir. 2016) (en banc). If the Fourth Amendment analysis turned solely on what the government found useful at trial, courts would not consider intrusions into innocent or irrelevant communications.

Third, even if the government's narrow claim about its FISA application were relevant, this Court cannot credit it, because Supreme Court precedent requires that the "fruit of the poisonous tree" question be litigated in an informed adversarial context, not ex parte. *Alderman v. United States*, 394 U.S. 165, 168, 182-85 (1969). If this Court concludes that its legal analysis turns on the government's claim, then the due process principles in *Alderman* entitle Mr. Muhtorov to the disclosure of materials concerning the government's backdoor searches, and an opportunity to cross-examine the government's witnesses. Def. Reply 12, 36, 42-43.

Adversarial process is essential in this context. The government has provided little factual information to support its backdoor search argument, and the defense lacks access to nearly all of those facts. Moreover, even if the government's claim were accurate, it is far too narrow to resolve the "fruit of the poisonous tree" question. For example, even if a backdoor search of Mr. Muhtorov did not directly lead to the Section 702 communications cited in the FISA application, such a search could have led to *other* evidence cited in that application. Similarly, the government fails to address how backdoor searches of

Mr. Muhtorov may have informed investigative efforts beyond its FISA application—such as Rule 41 warrants, Stored Communication Act warrants, and the use of informants.

Finally, there is good reason to doubt the government's version of events. Most significantly, the government does not appear to know when and how agents queried the FBI's Section 702 databases using identifiers associated with Mr. Muhtorov. *See* Gov't Suppl. Br. 2 ("even assuming *arguendo* that any such queries occurred). How can the government be so confident that its backdoor searches did not taint any aspect of its investigation if it cannot say when it queried Mr. Muhtorov's communications, what those queries produced, and how agents used the results? The Court should not credit the government's unilateral claims. As just one example, the defense should have the opportunity to compare the timing of the queries involving Mr. Muhtorov with the timing of the investigative steps that the government now claims led to the Section 702 communications in its FISA application. And critically, even that information would not resolve whether the queries associated with Mr. Muhtorov led to other information in the FISA application or other investigative efforts.

Moreover, as the FISC has held, the FBI's recordkeeping with respect to backdoor searches has been nothing short of abysmal. [*Redacted*], 402 F. Supp. 3d at 67-68, 73-91. For years, the FBI did not even require agents to write down their

reasons for targeting an American with a backdoor search, nor did the agency document the volume of U.S.-person queries of its Section 702 databases. *Id.* at 52-53, 68, 79, 88-91. By all indications, these problems beset the FBI's searches during the period relevant here. *See id.* at 68-73 (describing limitations of FBI systems). Indeed, even after Congress required the FBI to record the number of its U.S.-person queries in 2018, the agency failed to do so. *Id.* If the Court deems the government's "fruit of the poisonous tree" claim relevant in any way, the FBI's failures to implement basic recordkeeping requirements related to backdoor searches are yet another reason to require disclosure and adversarial testing of its assertion.[2]

* * *

The present record supports the conclusion that the government's Section 702 surveillance of Mr. Muhtorov violated his Fourth Amendment rights. Def. Reply 2-28. The Court should not permit the government to introduce new claims, that rely on secret facts, at this late stage of the case and after nearly a decade of litigation. But if the court were to consider the government's "fruit of the poisonous tree" claim, a remand would be necessary to develop the factual record.

[2] In addition, the government has a track record of making unduly narrow claims about whether its evidence is "derived from" a particular form of surveillance, including in this case. It improperly withheld notice of Section 702 surveillance from Mr. Muhtorov for nearly two years after his arrest, based on its unilateral (and incorrect) "derived from" determination. *See* V3 at 116.

At a minimum, both Mr. Muhtorov and the district court should have the opportunity to examine how agents used the fruit of their backdoor searches in the investigation, and how those investigative steps related to the evidence the government presented at trial. *See United States v. Hasbajrami*, 945 F.3d 641, 676-77 (2d Cir. 2019).

II. Mr. Muhtorov's concerns about the government's use of novel surveillance tools are justified.

Beyond Section 702 and FISA, Mr. Muhtorov is entitled to notice of other novel surveillance tools used in the government's investigations, based on the Constitution, statutory law, and the Federal Rules of Criminal Procedure. Def. Br. 69-80; Def. Reply 33-42. Without notice, he is unable to meaningfully challenge the legality of this surveillance. While the government's ex parte brief purports to address some of Mr. Muhtorov's arguments for notice, it fails to address the core question: which novel surveillance techniques did the government actually use in its investigation? Def. Br. 72-75 (discussing, for example, the use of location tracking and collection of communications metadata).[3]

The Constitution requires notice of those techniques, as the Ninth Circuit's recent decision in *United States v. Moalin*, 973 F.3d 977, 997-1001 (9th Cir. 2020),

[3] Although the government provides a purported chronology of its investigation, it is unlikely that those few pages identify each of the surveillance tools FBI agents used in their years-long investigation of Mr. Muhtorov. Gov't Suppl. Br. A36.

confirms. In *Moalin*, the defendants argued that the Fourth Amendment required the government to provide notice of its collection and use of Mr. Moalin's telephone metadata under Section 215, as well as other forms of foreign intelligence surveillance. The court agreed with the defendants' constitutional argument, concluding that "the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use or disclose information obtained or derived from surveillance of that defendant conducted pursuant to the government's foreign intelligence surveillance authorities." *Id.* at 1000.[4] So too, here. Under the Constitution, Mr. Muhtorov is entitled to notice and the opportunity to challenge the surveillance tools that the government used in its investigation.

[4] Although the *Moalin* court concluded, on the basis of the classified record, that any lack of notice was not prejudicial to the defendants, its Fourth Amendment holding supports Mr. Muhtorov's arguments for notice. *Id.* at 1001. The court's decision not to remand the case to the district court for *Alderman* disclosures and a suppression hearing was based on "the particular circumstances of [that] case," in which the defense sought information about the government's collection of telephone metadata, but had already "fully" obtained access to conversations overheard pursuant to FISA. *Id.* at 993 n.6. As the court recognized, "in a different case," disclosure under *Alderman* may be required in order for the defense to "intelligently litigate" a challenge to unlawful surveillance—including the government's collection of metadata. *Id.*

A. The government appears to have misused CIPA to improperly conceal its novel surveillance techniques.

As Mr. Muhtorov has explained, the government appears to have misused CIPA to conceal its use of novel surveillance techniques from the defense, in violation of *Alderman* and due process. Def. Br. 69-88; Def. Reply 42-45; Def. 28(j) Letter, Sept. 18, 2020. The government contends that these concerns are "unfounded," Gov't Suppl. Br. 13-14, but its ex parte brief in fact provides further support for Mr. Muhtorov's argument.

First, the government's brief strongly suggests that one of the subjects of the CIPA proceedings pertained to "novel surveillance techniques." *Id.* at 13-14. The government claims that the proceedings "focused on" several topics—apparently four categories of information. *Id.*[5] Although three categories do not relate to novel surveillance techniques, the plain implication is that the fourth category does. The

[5] Of course, a proceeding may "focus" primarily on certain topics while addressing several others. It is not clear that the government has offered an exhaustive list of the surveillance issues addressed in the district court's numerous CIPA proceedings over six years. This includes, *e.g.*, the hearings at district court doc. nos. 137, 175, 816, 919, 1093, 1223, 1244, 1269, 1276, 1304, 1369, 1466, 1540, 1551, 1552, 1564, 1620, 1621, 1657, 1691, 1854; orders at doc. nos. 175, 1210, 1260, 1288, 1295, 1297, 1565, 1579, 1616, 1686, 1720; protective orders at doc. nos. 1094, 1196; and government filings at doc. nos. 198, 336, 569, 1092, 1171, 1302, 1489, 1534, 1560, 1567, 1590, 1643, 1679, 1681, 1743. The Court should order the government to provide a complete accounting of those issues, rather than accept the government's summary at face value.

use of CIPA to conceal information about these techniques is precisely Mr. Muhtorov's concern. Def. Br. 69-88; Def. Reply 42-45; Def. 28(j) Letter.

Second, the government contends that the only relevant question is whether the information addressed during the CIPA proceedings would have provided a basis for "any *additional* motions to suppress." Gov't Suppl. Br. 14 (emphasis in original). But this is the wrong legal test. The CIPA framework and *Alderman* forbid ex parte litigation over Fourth Amendment suppression issues. Def. Br. 81-88; Def. Reply 42-45. And even if the government were not advancing ex parte arguments about whether evidence was "derived from" a particular surveillance technique, due process would still require disclosure of information relevant and helpful to any argument that evidence was obtained illegally. Def. Br. 63-64, 81-82; Def. Reply 37, 43-44.

* * *

While Mr. Muhtorov's concerns about the government's misuse of CIPA are well-founded, the government also may not have fully identified its surveillance even in those proceedings. Given the government's narrow view of its notice obligations, it may be the case that the government did not describe to the district court during CIPA proceedings each of the novel surveillance techniques that it used in its investigation of Mr. Muhtorov. If so, the government's summary of

those proceedings cannot resolve the core question here: whether the government is unlawfully withholding notice from Mr. Muhtorov.

B. Mr. Muhtorov is entitled to notice of surveillance conducted under Executive Order 12,333.

The government now asserts, for the first time, that its evidence was not "obtained or derived" from "the acquisition of Muhtorov's *communications* pursuant to Executive Order 12,333." Gov't Suppl. Br. 14 (emphasis added); *id.* at A43-49.[6] But E.O. 12,333 surveillance is not limited to the collection of "communications"; instead, the government uses it to obtain many different types of personal data. The government's unilateral assertion does not—and legally cannot—resolve the question of whether Mr. Muhtorov is entitled to notice of E.O. 12,333 surveillance. Def. Br. 72-74, 77-88; Def. Reply 34-45.

First, as explained above, the Supreme Court's decision in *Alderman* forecloses ex parte litigation over whether the government's evidence was "obtained or derived" from a particular form of surveillance, given the complexity of that Fourth Amendment question. *See supra*.

[6] Until now, the government's public filings had made a much broader claim, asserting that its trial evidence was not "the primary product of, or . . . obtained by the exploitation of, surveillance conducted pursuant to Executive Order 12,333 as to which defendants are aggrieved." Gov't Br. 62-63.

Second, even if the government's assertion here were taken at face value, it is too narrow to resolve the notice question, because the government does not rule out the possibility that E.O. 12,333 surveillance contributed to the investigation of Mr. Muhtorov. Instead, the government claims that its evidence was not obtained or derived from *communications* acquired under E.O. 12,333. Gov't Suppl. Br. 14; *id.* at A46-48. That leaves open the possibility that its evidence was obtained or derived from other types of private *data* acquired under E.O. 12,333, such as the bulk acquisition of call records, location information, or internet metadata. Def. Br. 72-73.

Third, the government errs by focusing exclusively on 18 U.S.C. § 3504 as a basis for notice. *See* Gov't Suppl. Br. 14; *id.* at A44; Gov't Br. 60-61. Regardless of the applicability of Section 3504, the Constitution and Federal Rule of Criminal Procedure 16 separately require notice where the government's surveillance of Mr. Muhtorov's private data contributed to its investigation. Def. Br. 77-80; Def. Reply 34-40. Indeed, in *Moalin*, the defendants sought notice of the government's collection of their telephony metadata, and the Ninth Circuit made clear that the "constitutional notice requirement" applies where the government uses information in a prosecution that was obtained or derived from a defendant's metadata. 973 F.3d at 997-98, 1000-01. The court also observed that several provisions in FISA codify the constitutional notice requirement, including 50 U.S.C. § 1845(c), which

requires notice to defendants whenever the United States intends to use information obtained or derived from a FISA pen register or trap-and-trace device—surveillance devices that do not obtain the content of communications. *Id.* at 1000-01.

Finally, there are serious questions going to the accuracy of the government's claim about the collection of Mr. Muhtorov's communications. The government's ex parte response in the district court to Mr. Muhtorov's motion for notice states that, in February 2013, the prosecutors sent "Prudential Search Requests" to the NSA and CIA, and that "[m]aterials responsive to the search request were made available to the prosecution team for review." Gov't Suppl. Br. A46-48 & n.5. That the search request resulted in at least *some* responsive materials suggests that prosecutors made a judgment call to withhold surveillance materials "arguably relevant" to a motion to suppress, contrary to Supreme Court precedent. *Alderman*, 394 U.S. at 168, 181-82 (rejecting government proposal to submit "arguably relevant" surveillance materials to a judge for in camera review, and instead requiring disclosure of even these materials to the defendant).

III. The government's belated disclosures are illustrative of the procedural unfairness that has plagued each stage of these proceedings.

Ultimately, the government's disclosures are too little, too late. By withholding this information from Mr. Muhtorov for six years—information insufficiently sensitive to remain classified—the government deprived him of the

opportunity to fully brief the above arguments to the district court. And even more importantly, the government continues to withhold the surveillance materials essential to Mr. Muhtorov's ability to make the full set of arguments that a court must analyze in reviewing Section 702 and FISA surveillance, Def. Br. 51-68, and essential to his ability to meaningfully challenge the other novel surveillance tools the government may have used in its investigation, Def. Br. 71-76.

Respectfully submitted,

VIRGINIA L. GRADY
Federal Public Defender

/s/ John C. Arceci
JOHN C. ARCECI
Assistant Federal Public Defender
633 17th Street, Suite 1000
Denver, Colorado 80202
(303) 294-7002
Email: John_Arceci@fd.org

/s/ Patrick Toomey
PATRICK TOOMEY
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: ptoomey@aclu.org

/s/ Ashley M. Gorski
ASHLEY M. GORSKI
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500
Email: agorski@aclu.org

Counsel for Appellant Jamshid Muhtorov

**CERTIFICATES OF COMPLIANCE,
DIGITAL SUBMISSION, AND SERVICE**

I certify that the foregoing ***Appellant's Supplemental Reply Brief to the Government's Classified, Ex Parte Brief*** is proportionally spaced and contains 3,382 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f). I relied on my word processor, Microsoft Word 2016, to obtain the count. I certify that the information on this form is true and correct to the best of my knowledge and belief formed after a reasonable inquiry.

I hereby certify that with respect to the foregoing ***Appellant's Supplemental Reply Brief to the Government's Classified, Ex Parte Brief*** (1) all required privacy redactions have been made; (2) the ECF submission is an exact copy of the filed hard copy; and (3) the ECF submission was scanned for viruses with Symantec Endpoint Protection version 14.2.5569.2100, Virus Definition File Dated: Thursday, October 29, 2020 r17 and, according to the program is free of viruses.

I hereby certify that on October 29, 2020, I electronically filed the foregoing ***Appellant's Supplemental Reply Brief to the Government's Classified, Ex Parte Brief*** using the CM/ECF system, which will send notification of this filing to counsel for the government, James C. Murphy, at james.murphy3@usdoj.gov, and Joseph Palmer, at joseph.palmer@usdoj.gov. I further certify that I also will send a copy of this filing by email to Caleb Kruckenberg, Counsel for Appellant Bakhtiyor Jumaev, at caleb.kruckenberg@ncla.legal.

/s/ John C. Arceci
JOHN C. ARCECI
Assistant Federal Public Defender