1 2 3 4 5 6 7 8	MOHAMMAD TAJSAR (CA Bar No. 280152 mtajsar@aclusocal.org AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFO 1313 West 8th Street Los Angeles, CA 90017 Tel.: (213) 977-9500 ASHLEY GORSKI agorski@aclu.org NOOR ZAFAR nzafar@aclu.org PATRICK TOOMEY ptoomey@aclu.org		
9	AMERICAN CIVIL LIBERTIES UNION FOUNDATION		
10 11	125 Broad Street, 18th Floor New York, NY 10004 Tel.: (212) 549-2500		
12	1011. (212) 3 13 2300		
13	Attorneys for Amici Curiae		
14 15	UNITED STATES DISTRICT COURT CENTRAL DISTRICT OF CALIFORNIA		
16 17	UNITED STATES OF AMERICA,	Case No.: 8:19-cr-00117-JAK-1	
18	Plaintiff, v.	BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND	
20	ABDALLAH OSSEILY,	AMERICAN CIVIL LIBERTIES UNION OF SOUTHERN CALIFORNIA IN SUPPORT	
21	Defendant.	OF DEFENDANT'S MOTION FOR DISCLOSURE OF FISA-RELATED MATERIAL	
22			
23 24			
24 25			
26			
27			
28			

CORPORATE DISCLOSURE STATEMENT Amici curiae American Civil Liberties Union ("ACLU") and ACLU of Southern California state that they do not have parent corporations. No publicly held corporation owns 10% or more of any stake or stock in amici curiae. Dated: January 28, 2020 /s/Mohammad Tajsar Mohammad Tajsar Attorney for Amici Curiae

TABLE OF CONTENTS 1 2 3 Introduction ______1 4 5 I. 6 Mr. Osseily is entitled to challenge the lawfulness of the FISA surveillance revealed II. in discovery 4 7 The government cannot foreclose Mr. Osseily from challenging the FISA 8 surveillance simply by claiming that its evidence is not "derived from" the 9 10 The government has a history of making unjustified and self-serving claims B. 11 III.12 FISA's text, structure, and legislative history make plain that disclosure is 13 A. necessary in cases involving possible misrepresentations or raising complex 14 15 Disclosure is "necessary" to determine whether the factual claims in the B. 16 Disclosure is also "necessary" where the government's surveillance methods 17 18 Adversarial litigation substantially reduces the risk of error in cases involving 19 20 FISA must be construed to require disclosure consistent with the Fourth and Fifth 21 Conclusion 18 22 23 24 25 26 27 28

TABLE OF AUTHORITIES 1 2 Cases 3 [Redacted], 4 [Redacted], 5 6 ACLU v. Clapper, 7 8 Alderman v. United States, 9 Am.-Arab Anti-Discrimination Comm. v. Reno, 10 11 Carpenter v. United States, 12 13 Clapper v. Amnesty Int'l USA, 14 Franks v. Delaware, 15 16 Hooper v. California, 17 18 In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC, 19 In re All Matters Submitted to the FISC, 20 21 Kolod v. United States. 22 23 Kyllo v. United States, 24 *Mathews v. Eldridge*, 25 26 Murray v. United States, 27 28

ase 8:19-cr-00117-JAK Document 78 Filed 01/28/20 Page 5 of 25 Page ID #:437

1	Riley v. California, 573 U.S. 373 (2014)12	
2 3	Smith v. Black, 904 F.2d 950 (5th Cir. 1990)15	
4	United States v. Abu-Jihaad,	
5	630 F.3d 102 (2d Cir. 2010)	
6 7	United States v. Alwan, 2012 WL 399154 (W.D. Ky. Feb. 7, 2012)	
8	United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982)	
9 10	United States v. Chatrie, No. 3:19-cr-130 (E.D. Va. Oct. 29, 2019)	
11	United States v. Daoud, 755 F.3d 479 (7th Cir. 2014)17	
13	United States v. Gaines, 668 F.3d 170 (4th Cir. 2012)7	
14 15	United States v. Gamez-Orduno, 235 F.3d 453 (9th Cir. 2000)	
16	United States v. Gartenlaub, 751 F. App'x 998 (9th Cir. 2018)12	
17 18	United States v. James Daniel Good Real Prop., 510 U.S. 43 (1993)17	
19 20	United States v. Johns, 891 F.2d 243 (9th Cir. 1989)7	
21	United States v. Lundin, 817 F.3d 1151 (9th Cir. 2016)	
22 23	United States v. Mehanna, 2011 WL 3652524 (D. Mass. Aug. 19, 2011)	
24 25	United States v. Mubayyid, 521 F. Supp. 2d 125 (D. Mass. 2007)10	
26	United States v. Ott, 827 F.2d 473 (9th Cir. 1987)8	
27 28	United States v. Ramirez-Sandoval, 872 F.2d 1392 (9th Cir. 1989)	

ase 8:19-cr-00117-JAK Document 78 Filed 01/28/20 Page 6 of 25 Page ID #:438

1 2	United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972)		
3	United States v. Williams, 615 F.3d 657 (6th Cir. 2010)7		
4 5	Wong Sun v. United States, 371 U.S. 471 (1963)7		
6			
7	Statutes		
8	50 U.S.C. § 1803		
9	50 U.S.C. § 1804		
10	50 U.S.C. § 1805		
11	50 U.S.C. § 1806		
12	50 U.S.C. § 1822		
13	50 U.S.C. § 1823		
14	50 U.S.C. § 1824		
15	50 U.S.C. § 1825		
16 17	Classified Information Procedures Act, 18 U.S.C. App. 3		
18	Legislative History		
19	S. Rep. No. 95-604(I), reprinted in 1978 U.S.C.C.A.N. 3959		
20	S. Rep. No. 95-701, reprinted in 1978 U.S.C.C.A.N. 4033		
21			
22	Rules		
23	FISC Rule of Procedure 11		
24	Other Sources		
25 26	Charlie Savage & Nicole Perlroth, <i>Yahoo Said to Have Aided U.S. Email Surveillance</i> by Adapting Spam Filter, N.Y. Times, Oct. 5, 2016		
27 28	Charlie Savage, Door May Open for Challenge to Secret Wiretaps, N.Y. Times, Oct. 16, 20136		

ase 8:19-cr-00117-JAK Document 78 Filed 01/28/20 Page 7 of 25 Page ID #:439

1	Craig Timberg & Ellen Nakashima, FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance, Wash. Post, Dec. 6, 2013		
2	Highlights Use of Matware for Surveillance, Wash. Post, Dec. 6, 201512		
3	Declan McCullagh, FBI Pressures Internet Providers to Install Surveillance Software, CNET, Aug. 2, 2013		
4	DOJ Office of the Inspector General, A Review of the Department of Justice's Involvement with the President's Surveillance Program (July 2009)		
5			
6	DOJ Office of the Inspector General, Review of Four FISA Applications and Other		
7	Aspects of the FBI's Crossfire Hurricane Investigation (Dec. 2019)		
8	Jennifer Valentino-DeVries, <i>Tracking Phones, Google is a Dragnet for the Police</i> , N.Y. Times, Apr. 13, 2019		
9	John Kelly, Cell Phone Data Spying: It's Not Just the NSA, USA Today, Dec. 8, 201311		
10	Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand		
11	Computers, Vice, Jan. 5, 2016		
12	Office of the Director of National Intelligence, <i>IC on the Record</i>		
13	Robert Barnes & Ellen Nakashima, U.S. Tells Terror Suspect It Will Use Surveillance Evidence, Wash. Post, Oct. 25, 2013		
14			
15	Robinson Meyer, <i>How the Government Surveils Cellphones: A Primer</i> , Atlantic, Sept. 11, 2015		
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

STATEMENT OF INTEREST OF AMICI CURIAE

The ACLU is a nationwide, nonprofit, nonpartisan organization with nearly two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU of Southern California is a state affiliate of the national ACLU. The ACLU and ACLU of Southern California have appeared before federal courts in numerous cases implicating civil liberties and Foreign Intelligence Surveillance Act ("FISA") surveillance, including as counsel in *Fazaga v. FBI*, 916 F.3d 1202 (9th Cir. 2019), *United States v. Muhtorov*, No. 18-1366 (10th Cir. 2019), *Xi v. Haugen*, No. 17-cv-02132 (E.D. Pa. 2017), and *United States v. Moalin*, No. 13-50572 (9th Cir. 2015); and as amicus in *United States v. Gartenlaub*, No. 16-50339, 751 Fed. App'x 998 (9th Cir. 2018), *United States v. Mohamud*, 843 F.3d 420 (2016), and *United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014).

Counsel for amici certify that no party's counsel authored this brief in whole or in part, and no person other than amici, their members, or their counsel made a monetary contribution to its preparation or submission.

INTRODUCTION

By all indications, the government subjected Mr. Osseily to surveillance under the Foreign Intelligence Surveillance Act ("FISA") and disclosed the wiretap recordings to him in discovery. Yet the government nonetheless argues that Mr. Osseily's motion for disclosure of FISA materials is moot, based on a claim that prosecutors do not intend to use any evidence "derived from" FISA surveillance at trial. For the reasons below, the Court should hold that Mr. Osseily is entitled to pursue his challenge to the FISA surveillance, and it should grant the defense access to the underlying FISA applications, orders, and related materials pursuant to appropriate security measures.

Both FISA and due process authorize Mr. Osseily's motion for disclosure, regardless of whether the government concedes that its evidence is "derived from" FISA. Where a defendant has been subjected to FISA surveillance, he may challenge the lawfulness of that surveillance—as well as any government claim that its evidence is not derived from those electronic searches. The question of whether the government's evidence is the "fruit of the poisonous tree" is notoriously

Instead, the Court should follow the roadmap that FISA provides. FISA directs courts to address the lawfulness of surveillance before determining what evidence, if any, should be suppressed as the fruit of those searches. 50 U.S.C. § 1806(f)–(g). Specifically, the government must either disclose the FISA materials to the defense or, if the Attorney General claims that disclosure would harm national security, the government must file those materials with the Court in camera and ex parte. *See id.* § 1806(f). After assessing whether disclosure to the defense is "necessary" under the statute, the Court should proceed to determine whether the FISA surveillance was lawful. *Id.* If the Court finds the surveillance of Mr. Osseily illegal, it should then consider what evidence must be suppressed as a result, just as it would in any other suppression challenge. *Id.* § 1806(g).

On the question of whether disclosure is necessary in this case, recent revelations and technological advances leave no doubt.

When Congress enacted FISA, it made clear that disclosure is necessary in cases that involve possible misrepresentations of fact, as well as cases that raise complex legal or factual questions. In the presence of any of these factors, due process also requires disclosure, because the lawfulness of the surveillance cannot be accurately assessed without the benefit of informed, adversarial argument.

All these factors are present here. First, recent revelations of FISA abuse disclosed by the DOJ Inspector General underscore the likelihood of similar misrepresentations in this case—and

1 sl
2 re
3 ir
4 la
5 w
6 S
7 lir
9 re
10 er
11 g
12 l
13 l
14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

show that courts cannot identify such misrepresentations on their own. The Inspector General's report on the FBI's surveillance of Carter Page exposed inexcusable misstatements and omissions in the agency's FISA applications. Although one would have expected government agents and lawyers to be especially scrupulous in targeting a former campaign official, the FISA applications were nevertheless riddled with errors, prompting serious concerns by the Foreign Intelligence Surveillance Court ("FISC") that these problems are part of a larger, systemic pattern.

Second, recent technological advances have rendered the government's FISA searches increasingly broad and technologically complex, presenting difficult new questions for courts reviewing those searches. Disclosure of the FISA materials is "necessary" for this reason too: to ensure that the Court can accurately determine how the Fourth Amendment and FISA apply to the government's novel surveillance methods.

ARGUMENT

I. Statutory Background

In 1978, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the FISC and authorized the court to grant or deny government applications for surveillance orders in certain foreign intelligence investigations. *See* 50 U.S.C. §§ 1803(a), 1804–1805. To obtain an order authorizing electronic surveillance, the government must establish "probable cause to believe that the target . . . is a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A).

FISA permits defendants subject to surveillance to seek suppression of the resulting evidence. 50 U.S.C. § 1806(e). To facilitate such challenges, the statute requires the government to notify a defendant when it concludes that its evidence was "obtained or derived" from FISA surveillance of the defendant. *Id.* § 1806(c). But even absent notice, a defendant may seek to discover the relevant FISA applications, orders, and other materials in order to bring an informed suppression motion. *Id.* § 1806(f); *United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982).

When a defendant moves for disclosure of the FISA materials, the Attorney General must determine whether to file an affidavit asserting that disclosure or an adversary hearing would harm the national security of the United States. *See* 50 U.S.C. § 1806(f). If the Attorney General files

such an affidavit, the district court reviews the materials relating to the surveillance in camera and ex parte "as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.* § 1806(f).¹

The statute recognizes, however, that in some cases the district court's ex parte review will not be sufficient, and an adversarial process will be necessary. Thus, the statute provides that, following the court's initial review, the court may disclose FISA materials to the defendant under appropriate security procedures and protective orders "where such disclosure is necessary to make an accurate determination of the legality of the surveillance," 50 U.S.C. § 1806(f), or is required as a matter of due process, *id.* § 1806(g).

- II. Mr. Osseily is entitled to challenge the lawfulness of the FISA surveillance revealed in discovery.
 - A. The government cannot foreclose Mr. Osseily from challenging the FISA surveillance simply by claiming that its evidence is not "derived from" the FISA wiretaps.

There is little genuine question that FISA surveillance is part of this case. The government has disclosed wiretap recordings of Mr. Osseily that were not obtained under Title III of the Wiretap Act, and it has refused to identify their provenance. Moreover, it is clear that FBI investigators and DOJ prosecutors reviewed these wiretap recordings, regarded them as material to this case, and are open to using them at trial. *See* Def. Reply, Ex. A. Nonetheless, the government has refused to provide Mr. Osseily with a FISA notice, and it now claims that any effort to challenge the FISA surveillance is moot. That claim is wrong. Having decided to pursue this prosecution, the government is not permitted to dictate whether Mr. Osseily can challenge this intrusive surveillance.

Both Section 1806 and due process entitle Mr. Osseily to move for disclosure and suppression. Under Section 1806(f), an "aggrieved person" subject to FISA surveillance, like Mr. Osseily, may seek disclosure of materials related to that surveillance, regardless of whether the government believes that its evidence is "derived from" FISA. *See* 50 U.S.C. § 1806(f). As the D.C.

¹ To the extent that the government conducted not only electronic surveillance of Mr. Osseily under FISA, but also physical searches, FISA contains parallel provisions permitting individuals to seek disclosure and suppression. *See* 50 U.S.C. §§ 1822–1824; *id.* § 1825(f)–(h).

Circuit has held, a defendant's ability to pursue disclosure and suppression does not depend on whether the government concedes that its evidence flowed from FISA surveillance. *See Belfield*, 692 F.2d at 146 ("[E]ven when the Government has purported not to be offering any evidence obtained or derived from the electronic surveillance, a criminal defendant may . . . seek discovery of the logs of the overhears to ensure that no fruits thereof are being used against him.").

Allowing the government to unilaterally dictate whether its evidence is "derived from" FISA, and to thereby thwart suppression challenges, would violate due process. Due process entitles defendants to a meaningful opportunity to suppress the fruits of illegally acquired evidence. *See*, *e.g.*, *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000); *infra* Section IV. Crucially, that includes the chance to show that the government's evidence is tainted. As the Supreme Court explained in *Alderman v. United States*, fact-intensive questions about whether evidence should be suppressed as "fruit of the poisonous tree"—*i.e.*, whether evidence is "derived from" unlawful surveillance—must be litigated in an adversarial context. *See* 394 U.S. 165, 183–185 (1969); *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 324 (1972) (ordering disclosure to facilitate adversarial litigation under *Alderman*). The government cannot avoid litigation over whether its evidence is tainted by substituting its judgment for this Court's.

B. The government has a history of making unjustified and self-serving claims that its evidence is not "derived from" FISA.

The *Alderman* Court recognized the inherent dangers of allowing the government to conclusively determine whether its evidence is "derived from" controversial surveillance. The legal and factual questions are difficult, and the government's interest in avoiding court review of novel surveillance tools is obvious. If anything, these dangers have only grown. As recent history shows, the government often adopts narrow and self-serving views of what evidence counts as "derived," thus thwarting judicial review of invasive surveillance.

The government's long-running failure to give notice of FISA surveillance in certain criminal cases showcases this problem. Under FISA, the government must provide notice when it has surveilled an individual and intends to use evidence "obtained or derived from" that surveillance against the person in a criminal prosecution. 50 U.S.C. § 1806(c). Like other notice

⁴ *Id*.

requirements, Section 1806(c) is meant to ensure that individuals have the opportunity to challenge secret searches of their communications and obtain judicial review, especially when facing criminal prosecution.

Yet the government has relied on secret, narrow interpretations of this statutory obligation to wrongly withhold notice from criminal defendants. In 2012, the government sought to defeat the plaintiffs' standing in a civil case challenging warrantless surveillance under Section 702 of FISA. The government repeatedly assured the Supreme Court that others were better situated to challenge the law—namely, defendants in criminal prosecutions where the government would provide notice of Section 702 surveillance. *See* Br. of Pet'rs at 8, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013) (No. 11-1025); *see also* Tr. of Oral Arg. at 4:12–17, *Amnesty*, 568 U.S. 398. However, in 2013, the *New York Times* reported that, for five years, DOJ had a policy that deprived defendants of notice that they had been surveilled under Section 702.² According to the *Times*, DOJ's National Security Division had "long used a narrow understanding of what 'derived from' means" in FISA to avoid giving notice of Section 702 surveillance to *any* criminal defendant.³ When the Solicitor General learned of DOJ's narrow interpretation, he concluded that the policy "could not be justified legally."⁴

Although DOJ later modified its notice policy and provided notice of Section 702 surveillance to a handful of criminal defendants, it still refuses to disclose how it interprets "derived from" in FISA. Because of this continuing secrecy, Mr. Osseily is unable to assess whether DOJ's new interpretation comports with Congress's intent or the Constitution. But there are indications that the government may be improperly relying on exceptions to the "fruit of the poisonous tree" doctrine to withhold notice. ⁵ This doctrine controls whether *suppression* is ultimately warranted,

² See Charlie Savage, Door May Open for Challenge to Secret Wiretaps, N.Y. Times, Oct. 16, 2013, https://nyti.ms/36ccH0G; Robert Barnes & Ellen Nakashima, U.S. Tells Terror Suspect It Will Use Surveillance Evidence, Wash. Post, Oct. 25, 2013, http://wapo.st/1qdl8g2.

³ Savage, Door May Open for Challenge to Secret Wiretaps, supra.

⁵ See DOJ Office of the Inspector General, A Review of the Department of Justice's Involvement with the President's Surveillance Program, 351 (PDF page 687) (July 2009), https://bit.ly/2PkLV35. The report explains that the government used the Classified Information Procedures Act to argue—ex parte—that materials related to warrantless surveillance were not discoverable, because defendants

not whether a defendant is entitled to *notice* of surveillance in the first place. *See Wong Sun v. United States*, 371 U.S. 471, 485–87 (1963).

Moreover, the "derived" analysis is often highly fact-specific, and the government has provided no information about how that analysis proceeded based on the facts of this case. The government's one-sided claim that it will not use evidence "derived from" FISA surveillance presents complex factual and legal questions that cannot be resolved on a unilateral or ex parte basis. *See Alderman*, 394 U.S. at 182 n.14, 184.

Given this complexity, the government's bald claim simply cannot be credited here. At the suppression stage, with the benefit of adversarial process, courts often reject the government's arguments about whether its evidence is derived from a given search or surveillance. *See, e.g.*, *Wong Sun*, 371 U.S. at 485–87 (rejecting government's argument that its evidence was not tainted); *United States v. Lundin*, 817 F.3d 1151, 1161–62 (9th Cir. 2016) (rejecting government's argument that an exception to fruit-of-the-poisonous tree doctrine applied); *United States v. Johns*, 891 F.2d 243, 245–46 (9th Cir. 1989) (same); *United States v. Ramirez-Sandoval*, 872 F.2d 1392, 1396 (9th Cir. 1989) (same); *United States v. Gaines*, 668 F.3d 170, 176 (4th Cir. 2012) (same); *United States v. Williams*, 615 F.3d 657, 671 (6th Cir. 2010) (same); *see also Kolod v. United States*, 390 U.S. 136 (1968) (per curiam) (rejecting the government's unilateral determination that evidence was not derived from challenged surveillance and requiring adversarial proceedings). There is no reason the government's undisclosed analysis in this case should be deemed any more conclusive.

III. Disclosure of the surveillance applications and orders is "necessary" under FISA.

The defense has moved for disclosure of the FISA applications, orders, and related materials. FISA dictates how this motion should be resolved: the government must either disclose those materials to the defense or, if the Attorney General claims that disclosure would harm national security, the government must file those materials with the Court in camera and ex parte, so that the Court can review the lawfulness of the surveillance. 50 U.S.C. § 1806(f). After the Court's initial review, it may order disclosure to the defense under appropriate security measures

would not ultimately succeed in suppressing the government's evidence. It repeatedly claimed in ex parte proceedings that its evidence was not "tainted" by the surveillance, even though the report shows otherwise. *See id.* at 271–331 (PDF pages 607–667).

where disclosure is "necessary" to accurately determine the lawfulness of the surveillance. *Id.* For the reasons that follow, disclosure is unquestionably necessary here.

A. FISA's text, structure, and legislative history make plain that disclosure is necessary in cases involving possible misrepresentations or raising complex questions of fact or law.

The text and structure of Section 1806 are clear that disclosure of FISA materials is appropriate in certain circumstances. As explained above, the statute allows defendants to move for disclosure of FISA materials, and it empowers district courts to order the disclosure of those materials, notwithstanding the government's secrecy claims.

The statute's legislative history confirms that Congress anticipated that FISA materials would be disclosed in cases involving possible misrepresentations, or complex issues of fact or law. In enacting FISA, Congress sought to "strik[e] a reasonable balance" between "mandatory disclosure" and "an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself." S. Rep. No. 95-604(I), at 58, reprinted in 1978 U.S.C.C.A.N. 3959; S. Rep. No. 95-701, at 64, reprinted in 1978 U.S.C.C.A.N. 4033. The congressional reports also describe factors that Congress expected courts to consider when assessing whether disclosure is "necessary": "indications of possible misrepresentations of fact"; the "complex[ity]" of the questions at issue; and the "scope, volume, and complexity" of the surveillance materials. *Id*.

In cases involving potential misrepresentations, or novel, complex, or far-reaching surveillance, adversarial litigation substantially enhances the accuracy of the proceedings, and disclosure is required. *Belfield*, 692 F.2d at 147–48; *see also United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987); *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010).

B. Disclosure is "necessary" to determine whether the factual claims in the government's FISA applications were accurate and complete.

Revelations about egregious misstatements and omissions in the FBI's applications to surveil Carter Page have made the necessity of disclosure in FISA cases clearer than ever. The DOJ Inspector General Report shows that courts simply are not in a position to identify, by themselves, material misrepresentations and omissions that appear in the government's FISA applications. Disclosure to defense counsel and adversarial litigation are necessary.

On December 9, 2019, the DOJ Inspector General released a long-awaited report examining the FBI's surveillance of Carter Page under FISA. DOJ Office of the Inspector General, *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* (Dec. 2019) ("Horowitz Report"), https://bit.ly/2sOu8H4. The report's conclusions were explosive and sobering. The Inspector General identified seventeen separate problems with the FBI's applications to the FISC—including repeated misrepresentations, factual inaccuracies, and material omissions. *See id.* at viii—xii. For example, after in-depth investigation, the Inspector General found that the FBI had omitted potentially exculpatory statements by Page, and had failed to confirm the reliability of a key confidential source with his FBI handler. *See id.* at viii—ix, x. Even as the FBI became aware of information contradicting its original claims, government attorneys failed to update and correct inaccuracies when they sought renewal orders from the FISC. *See id.* at xi—xii.

The problems documented in the Inspector General's Report went to the heart of the government's applications, undercutting its claims that there was probable cause to intercept Page's communications. And nothing suggests that the Page applications were unique in their defects. To the contrary: one would expect FBI and DOJ officials to exercise special care to ensure that the Page applications were scrupulously accurate, given that the surveillance of a former campaign official was likely to draw intense scrutiny. *See id.* at xiv.⁶

Following these revelations, many—including the FISC—have expressed pointed concern that the misrepresentations and omissions in the Page applications are part of a larger, systemic pattern. "The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable." Order at 3, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02 (FISC Dec. 17, 2019), http://bit.ly/2sRChus. The Inspector General apparently shares this concern. He has announced that the Office of the Inspector General is

⁶ This is not the first time grave problems have emerged with the government's FISA applications. In September 2000, the FISC disclosed that the government had acknowledged errors "in some 75 FISA applications." *In re All Matters Submitted to the FISC*, 218 F. Supp. 2d. 613, 620 (FISC 2002). There, too, the errors related to repeated "misstatements and omissions of material facts" in the FBI affidavits submitted to establish probable cause. *Id.* at 620.

1

4

5

3

6 7

9 10

8

1112

13 14

15 16

17

18

19 20

21

22

2324

25

2627

28

conducting a wide-ranging audit of FISA applications to "assess the FBI's compliance with Department and FBI FISA-related policies" that are supposed to protect the civil liberties of U.S. persons. Horowitz Report at xiv.

The problems with the Carter Page applications have exposed a persistent blind spot in the ex parte process by which FISA applications are reviewed: neither the FISC, nor any other court, is in a position to singlehandedly assess whether the government's applications are accurate and complete. A number of courts have acknowledged this problem in the abstract, as well as the corresponding difficulties that defendants face without access to the FISA applications and orders. See, e.g., United States v. Mubayyid, 521 F. Supp. 2d 125, 130–31 (D. Mass. 2007) ("The Court obviously recognizes the difficulty of defendants' position: because they do not know what statements were made by the affidavit in the FISA applications, they cannot make any kind of a showing that those statements were false."); United States v. Alwan, 2012 WL 399154, at *9–10 (W.D. Ky. Feb. 7, 2012) ("Hammadi cannot offer any proof that statements in the FISA applications were false or were deliberately or recklessly made because Hammadi has not been able to examine the applications. The Court is cognizant of the substantial difficulties Hammadi has encountered in trying to assert a Franks violation."); United States v. Mehanna, 2011 WL 3652524, at *2 (D. Mass. Aug. 19, 2011) ("The Court recognizes the defendant's difficulty in making such a preliminary showing where the defendant has no access to the confidential FISA-related documents here."); see also Belfield, 692 F.2d at 148 ("We appreciate the difficulties of appellants' counsel in this case."). But until now, many courts seem to have accepted the notion that the FISA process was immune to serious error. That view is no longer tenable. The Court should require disclosure of the FISA materials to defense counsel under appropriate security precautions because, on the present record, it is "necessary" to ensure that the surveillance of Mr. Osseily was lawful.

C. Disclosure is also "necessary" where the government's surveillance methods present novel or complex questions of fact or law.

In enacting FISA, Congress recognized that informed adversarial litigation is necessary in cases involving novel or complex surveillance—and the complexity of today's surveillance tools plainly meets that threshold. The lawfulness of these novel techniques, which expose enormous

quantities of private information to government scrutiny, cannot fairly be assessed on an ex parte basis. Courts must not only ascertain how these surveillance methods operate at a detailed, technical level, but they must evaluate how the government's new capabilities implicate Fourth Amendment-protected interests. Among other things, courts must consider the breadth of the intrusion, the ways in which private information is aggregated or exploited, and the proper limits on the government's use and retention of this data. Each of these factors bears on whether a FISA search is lawful under the Fourth Amendment. And without the benefit of informed adversarial litigation, the ability of courts to evaluate these factors is substantially limited.

While the government has not provided even a basic accounting of the surveillance methods it deployed under FISA in this case, it is clear that its searches are increasingly broad and technologically complex. Examples of novel surveillance techniques include:

1. Dragnet Geofence Searches, Cell Tower Dumps, and Stingrays

The government is increasingly relying on novel surveillance tools to collect data about all the individuals in a given area over a given period. Geofence searches give police access to dragnet location data that is collected through Google devices and Google apps, and then stored in Google's "Sensorvault." Similarly, law enforcement agencies obtain "cell tower dumps" by compelling communications providers to disclose information from all the phones that connected to a specified cell tower over a period of time. These data dumps can involve the collection of sensitive location information about thousands of individuals. Investigators are also deploying cell-site simulators (sometimes known as "Stingrays"), which masquerade as cell towers and "trick" all cell phones in the area into revealing their locations and identifying information.

Although these techniques are sometimes accompanied by a warrant, there are considerable Fourth Amendment questions about whether those warrants adequately protect the privacy interests

⁷ See Jennifer Valentino-DeVries, *Tracking Phones, Google is a Dragnet for the Police*, N.Y. Times, Apr. 13, 2019, https://nyti.ms/2TFpzdo.

⁸ See John Kelly, Cell Phone Data Spying: It's Not Just the NSA, USA Today, Dec. 8, 2013, http://bit.ly/2v4wna5.

⁹ See Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, Atlantic, Sept. 11, 2015, http://bit.ly/368cKKX.

of the many individuals for whom there is no suspicion of wrongdoing. 10

2. Searches of Personal Digital Devices

Searches of personal digital devices, such as cell phones and computer hard drives, implicate vast quantities of private information. An electronic device "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Riley v. California*, 573 U.S. 373, 396–97 (2014); *see also id.* at 394 (describing types of sensitive data found on electronic devices). As the Ninth Circuit has recently recognized, when these searches are conducted pursuant to FISA, the constitutional concerns are compounded. *See United States v. Gartenlaub*, 751 F. App'x 998, 1000 (9th Cir. 2018) (FISA computer search came "perilously close to the exact abuses against which the Fourth Amendment was designed to protect"). Not only are FISA searches predicated on relaxed standards as compared to traditional search warrants, but the object of a FISA search—"foreign intelligence information"—is both broad and elastic.

3. Malware and Hacking Techniques

The FBI has a broad range of surveillance malware and hacking techniques at its disposal, from malware that can covertly log individuals' IP addresses and operating system details, to malware that can remotely download a user's private files, photographs, and emails. Although malware and other forms of hacking are technologically complex, government agents often describe these techniques in vague terms in the warrant application, making it difficult for judges to decipher the precise activities that they are authorizing. In one case, the government has relied on a single warrant to deploy malware in thousands of computers across the country. 12

4. Bulk Scanning of Internet Communications

The FBI has developed other types of novel surveillance technologies to collect and comb

¹⁰ See, e.g., Mot. to Suppress Evidence Obtained From a "Geofence" General Warrant, *United States v. Chatrie*, No. 3:19-cr-130 (E.D. Va. Oct. 29, 2019), ECF No. 29.

¹¹ See Craig Timberg & Ellen Nakashima, FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance, Wash. Post, Dec. 6, 2013, https://wapo.st/2udq1Vu.

¹² See Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers, Vice, Jan. 5, 2016, http://bit.ly/3alHSdv.

through vast amounts of communications data. Devices called "port readers" copy entire emails and instant messages as they move through networks, and then funnel the metadata from those communications to the FBI for longer-term storage and use. According to news reports, the FBI has pressured reluctant telecommunications providers to install port readers on their internal networks. ¹³ In addition, under FISA, the FBI has reportedly ordered Yahoo to conduct bulk scans of users' emails and copy any messages containing a digital "signature" tied to the communications of a foreign organization. ¹⁴ These technologies give law enforcement access to enormous quantities of private data, far beyond the data associated with any particular target.

* * *

Because technologically advanced and intrusive surveillance techniques raise complicated Fourth Amendment and statutory issues, a district court's review of the lawfulness of this surveillance must be particularly searching. That is especially true where the government has relied on FISA to conduct its surveillance, given the broad objective of a FISA search and the relaxed showing required to obtain a FISA order. *See* 50 U.S.C. § 1804(a)(3).

To assist the Court in identifying complex questions raised by the surveillance of Mr. Osseily, the government should describe to the Court the specific surveillance techniques it employed, including any novel issues those methods present. *Cf.* FISC Rule of Procedure 11. The Court should then conduct its own review of the FISA materials and decide whether disclosure to defense counsel is "necessary" for "an accurate determination" of the legality of surveillance. 50 U.S.C. § 1806(f).

D. Adversarial litigation substantially reduces the risk of error in cases involving potential misrepresentations, or novel or complex surveillance.

A number of recent rulings in surveillance cases illustrate how judicial reliance on one-sided submissions from the government dramatically increases the risk of error. These opinions underscore both the complexity of the government's surveillance and the inherent limitations of ex

¹³ See Declan McCullagh, FBI Pressures Internet Providers to Install Surveillance Software, CNET, Aug. 2, 2013, https://cnet.co/36as8Xj.

¹⁴ See Charlie Savage & Nicole Perlroth, *Yahoo Said to Have Aided U.S. Email Surveillance by Adapting Spam Filter*, N.Y. Times, Oct. 5, 2016, https://nyti.ms/2G1v262.

parte proceedings in cases involving novel surveillance techniques.

For example, in *ACLU v. Clapper*, 785 F.3d 787, 822–24 (2d Cir. 2015), the Second Circuit held that bulk collection of Americans' call records under Section 215 of the Patriot Act was illegal. Although the FISC had authorized the surveillance in secret for years, the outcome was markedly different in the face of adversarial litigation. Similarly, in *Carpenter v. United States*, 138 S. Ct. 2206, 2216–17 (2018), the Supreme Court recognized that individuals have a privacy interest in the cell-site location information ("CSLI") generated by their cell phones. For years, the government had insisted that the third-party doctrine foreclosed any Fourth Amendment challenge to the collection of CSLI. However, with the benefit of adversarial briefing on the technical details of the surveillance and its constitutional implications, the Supreme Court ultimately ruled otherwise. *See id.* at 2217–18.

In 2011, in a case involving Section 702 surveillance of communications in transit, the FISC held that the government's program violated the Fourth Amendment. It did so only after discovering that the surveillance was much broader than the government had been representing to the court for years. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011) (explaining that the "volume and nature of the information" the government had been collecting was "fundamentally different from what the Court had been led to believe").

More recently, the FISC has identified other significant problems with the government's handling of data collected under Section 702. *See, e.g.*, [*Redacted*], No. [*Redacted*], at 19–23, 68–96 (FISC Apr. 26, 2017), https://perma.cc/7X2S-VAS7. After belatedly disclosing one of these problems, the NSA struggled for months to "ascertain the scope and causes" of its violations, attributing its failure to "the complexity of the issues involved." *Id.* at 5. This complexity was coupled with, in the FISC's words, "an institutional 'lack of candor' on the NSA's part." *Id.* at 19, 67–68 & n.57.

"When applying the Fourth Amendment to innovations in surveillance tools," courts must assure "preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). As "seismic shifts in digital technology" provide government agencies with

evermore sophisticated and invasive tools of surveillance, *id.* at 2219, it is imperative that courts conduct a searching review of the lawfulness of the government's surveillance, including the underlying FISA applications, orders, and related materials. In cases involving novel or complex surveillance, Congress recognized that disclosure of these materials to defense counsel—and informed adversarial litigation—is an essential part of this review.

IV. FISA must be construed to require disclosure consistent with the Fourth and Fifth Amendments.

Together, the Fourth and Fifth Amendments entitle defendants to a meaningful opportunity to seek suppression of evidence obtained illegally, and FISA's disclosure provisions must be construed in light of this constitutional right. In cases involving indications of possible misrepresentations of fact, or novel or complex questions, the principle of constitutional avoidance mandates that Section 1806 be read to require disclosure. *See, e.g., Hooper v. California*, 155 U.S. 648, 657 (1895) ("[E]very reasonable construction must be resorted to in order to save a statute from unconstitutionality."). In these cases, disclosure of FISA materials under appropriate security measures is "necessary" for "an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). It is also necessary as a matter of constitutional right.

Under the Fifth Amendment's Due Process Clause, defendants must have a meaningful opportunity to pursue suppression, which is the primary means of enforcing the Fourth Amendment's guarantees. *See, e.g., Murray v. United States*, 487 U.S. 533, 536–38 (1988) (describing right to seek suppression of evidence "derived" from an unlawful search); *Alderman*, 394 U.S. at 183–185. Because Fifth Amendment due process protections apply in the pretrial suppression context, the government must disclose information to a defendant that could affect the outcome of a suppression hearing. *See Gamez-Orduno*, 235 F.3d at 461 ("The suppression of material evidence helpful to the accused, whether at trial or on a motion to suppress, violates due process if there is a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different."); *Smith v. Black*, 904 F.2d 950, 965–66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression

hearing").

Section 1806 must be interpreted against this constitutional backdrop: it must be construed to require disclosure of FISA materials in at least those cases where the surveillance involves potential misrepresentations, or where it raises novel or complex questions.

As a general matter, adversarial proceedings are likely to enhance the court's ability to make accurate determinations of the legality of surveillance. *Cf.* 50 U.S.C. § 1806(f). Information that is seemingly inconsequential to a judge in an ex parte setting—"a chance remark, a reference to what appears to be a neutral person or event . . . or even the manner of speaking"—may have "special significance" to those who know the more intimate facts of a defendant's life. *Alderman*, 394 U.S. at 182; *see also Franks v. Delaware*, 438 U.S. 154, 155, 169 (1978) (observing that a magistrate judge "has no acquaintance with the information that may contradict" the affidavit and rejecting the argument that ex parte review by a magistrate judge would sufficiently protect defendants' rights).

Adversarial process is almost always preferable, but it is especially necessary where potential misrepresentations, or novel or complex surveillance techniques are involved. As the Supreme Court has explained:

[T]he need for adversary inquiry is increased by the complexity of the issues presented for adjudication. . . . Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.

Alderman, 394 U.S. at 182 n.14, 184.

A traditional due process analysis also underscores the necessity of adversarial litigation. Applying the familiar three-factor test in *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976), each factor weighs in favor of requiring disclosure where there are potential misrepresentations, or where the government has deployed novel or complex surveillance techniques. First, defendants have a substantial interest in an accurate determination of whether the government's surveillance violated their rights, and thus whether the fruits of that surveillance may be suppressed. Second, where the government has misstated or omitted material facts, or where factual or legal issues are particularly complex, a district court's ex parte review of the materials carries an unacceptably high risk of

error. Cf. United States v. James Daniel Good Real Prop., 510 U.S. 43, 55 (1993) ("The practice of		
ex parte seizure creates an unacceptable risk of error."); AmArab Anti-Discrimination Comm.		
v. Reno, 70 F.3d 1045, 1069 (9th Cir. 1995). Finally, the government's interest in secrecy in this		
context is substantially weakened by its myriad disclosures of FISA materials—including multiple		
versions of standard FISA minimization procedures, multiple versions of Section 702 targeting and		
minimization procedures, dozens of FISC opinions, and reports by intelligence agencies, inspectors		
general, and the Privacy and Civil Liberties Oversight Board. See, e.g., Office of the Director of		
National Intelligence, IC on the Record, http://bit.ly/2RvlANO. Insofar as the government does		
have a legitimate interest in maintaining the secrecy of particular materials, that interest can be		
accommodated through "appropriate security procedures and protective orders." 50 U.S.C.		
§ 1806(f); see also Classified Information Procedures Act, 18 U.S.C. App. 3.		

It bears emphasis that disclosure in this context does not necessarily mean disclosure to all, or disclosure of everything. Both the statute and the Constitution permit—indeed, require—a more nuanced approach. *See* 50 U.S.C. § 1806(f). The mere fact that the government has a legitimate interest in withholding some FISA information does not mean that it has an interest in withholding all of it; and the mere fact that the government has a legitimate interest in withholding FISA information from the general public (or even from the defendant) does not mean that it has a legitimate interest in withholding it from defense counsel.

A narrow interpretation of Section 1806(f) also conflicts with *Franks*, 438 U.S. at 155. There, the Supreme Court held that criminal defendants are entitled to an evidentiary hearing upon a "substantial preliminary showing" that a warrant affidavit includes a knowing or reckless false statement. *Id.* at 155–56. But as a practical matter, defendants like Mr. Osseily will virtually never be able to make the "substantial preliminary showing" required by *Franks*, because they cannot identify falsehoods or omissions in FISA affidavits they have not seen. *See United States v. Daoud*, 755 F.3d 479, 486 (7th Cir. 2014) (Rovner, J. concurring) ("As a practical matter, the secrecy shrouding the FISA process renders it impossible for a defendant to meaningfully obtain relief under *Franks*."), *cert. denied*, 135 S. Ct. 1456 (2015). Indeed, many courts that have construed Section 1806 narrowly acknowledge that their construction of the statute is implicitly in conflict

1	with Franks. See supra Section III.B.	
2	CONCLUSION	
3	For the foregoing reasons, the Court should grant Mr. Osseily's motion to disclose FISA-	
4	related material.	
5	$5 \parallel$	
6	Dated: January 28, 2020	Respectfully submitted,
7		,
8	3	/s/Mohammad Tajsar Mohammad Tajsar (CA Bar No. 280152)
9		mtajsar@aclusocal.org AMERICAN CIVIL LIBERTIES UNION
10		FOUNDATION OF SOUTHERN CALIFORNIA
11	1	1313 West 8th Street
12	$2 \parallel$	Los Angeles, CA 90017 Tel.: (213) 977-9500
13	3	
14	4	Ashley Gorski
15	5	agorski@aclu.org Noor Zafar
		nzafar@aclu.org
16		Patrick Toomey ptoomey@aclu.org
17		AMERICAN CIVIL LIBERTIES UNION FOUNDATION
18	3	125 Broad Street, 18th Floor
19	9	New York, NY 10004 Tel.: (212) 549-2500
20)	Fax: (212) 549-2564
21	1	
22	$2 \parallel$	Attorneys for Amici Curiae
23	3	
24	4	
25		
26		
27		
28		