

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF ILLINOIS  
EASTERN DIVISION**

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	No. 12 CR 723
	)	Judge Sharon Johnson Coleman
ADEL DAOUD,	)	
	)	
Defendant.	)	

**DEFENDANT’S REPLY IN SUPPORT OF HIS MOTION FOR DISCLOSURE  
OF FISA-RELATED MATERIAL AND TO SUPPRESS THE FRUITS OR  
DERIVATIVES OF ELECTRONIC SURVEILLANCE AND ANY  
OTHER MEANS OF COLLECTION CONDUCTED PURSUANT TO  
FISA OR OTHER FOREIGN INTELLIGENCE GATHERING**

This country, or at least civil liberties in this country as we have traditionally come to expect, is at another fear-laden crossroads. Not unlike the infamous and never ending “War on Drugs,” the eternal “War on Terror” as presented by the government intelligence agencies leaves us with another supposed Hobson’s choice between “national security” and civil liberties. Once again the Executive, aided by a Congress that appears capable only of agreeing upon the dire prediction that our national security is threatened daily by unknown terrorists lurking virtually everywhere, demands broader and more pervasive powers to monitor the comings and goings of virtually every American in the name of public safety. These expanded powers, at issue here, constitute an array of constitutionally suspect, and until recently, secret surveillance programs—including the mass acquisition of email and other Internet communications pursuant to the FISA Amendments Act (“FAA”), 50 U.S.C. § 1881a; the bulk collection of Internet metadata pursuant to 50 U.S.C. § 1841; as well as § 215 of the Patriot Act, 50 U.S.C. § 1861, which concerns the dragnet acquisition of third party telephone records or “telephony metadata,” not just of

Defendant Daoud, but virtually any American who uses a telephone, be it cellular or a land line.<sup>1</sup>

Thus, this Court is presented with the unprecedented opportunity to exercise its independent constitutional authority to stand in this crossroads and see to it that the fear mongering does not permit the government intelligence agencies to blow through the critical First and Fourth Amendment issues before it is too late. For the fact of the matter is that this is a fake choice between national security and civil rights, not unlike the fake war being conducted in our name against terror. All that is required to avoid another draconian step down this slippery and unconstitutional slope towards a permanent national security state is the attention of the independent federal judiciary—the only players in our bankrupt system of government insulated from the absurd political winds of fear. And, the first step in this process can be accomplished, counsel would submit, by merely allowing cleared defense counsel to meaningfully participate in ensuring the legality of the government’s surveillance of Defendant.

As counsel anticipated in their Memorandum of Law (Dkt. #52, p. 10), the prosecutors have invoked FISA’s *ex parte* and *in camera* review provisions by submitting a Declaration and Claim of Privilege from Attorney General Holder, dated October 16, 2013. (Dkt. #73-1). Consequently, the prosecutors’ unclassified Response (Dkt. #73) is heavily redacted and unfortunately devoid of substance. Due to these extensive redactions,<sup>2</sup> counsel simply cannot

---

<sup>1</sup> The telephony metadata practice has been described as being “akin to snatching every American’s address book—with annotations detailing whom we spoke to, when we talked, for how long, and from where.” Or, put another way, this information “gives the government a comprehensive record of our associations and public movements, revealing a wealth of detail about our familiar, political, professional, religious, and intimate associations.” See Exhibit A attached, the Complaint in *American Civil Liberties Union, et al., v. Clapper, et al.*, No. 13 CIV 3994, filed June 11, 2013, and still pending in the United States District Court for the Southern District of New York.

<sup>2</sup> No doubt, the prosecutors’ decision to use the bracketed phrase “[CLASSIFIED MATERIAL REDACTED]” rather than including the text and then redacting it is designed to have an intended effect. Only the prosecutors, the intelligence officials who reviewed the unredacted pleading, and the Court know how extensive the unredacted portions are—and thus how truly voluminous this pleading actually is.

meaningfully reply to the prosecutors' specific positions.

However, and notwithstanding these pervasive redactions, counsel still submit that there are more than adequate grounds to justify granting Defendant the relief requested in his Motion—particularly ordering the disclosure of the FISA materials to cleared counsel so that the Court can make an accurate determination of the legality of the surveillance in an adversary setting. (*See* 50 U.S.C. §§ 1806(f), 1825(g), 1806(g); Memorandum, pp. 24-26).

Such disclosure is fundamentally important because it may very well reveal how the FBI initially focused on Defendant—a critical fact that has been withheld. The origins of this investigation, whether through FISA, the FAA, bulk internet metadata collection, pen register/trap & trace authorization, warrantless wiretap, a “back door” search on traditional FISA collection,<sup>3</sup> or some other unknown surveillance program, is essential for the Court to accurately determine the legality of the surveillance. Recently disclosed FISC opinions underscore the importance of knowing the exact basis of how, when, and why the FBI started looking at Defendant, particularly in terms of how different surveillance programs require specific statutory notice and also how the different programs have had specific legal and compliance problems.<sup>4</sup>

**1. Recent Government Disclosures of FISA Materials, Including FISC Opinions and the Use of FAA Surveillance in Criminal Cases, Underscore the Significant Problems of Proceeding *In Camera* and *Ex Parte*.**

The recent and ongoing disclosures of FISA related-materials weigh heavily against conducting proceedings shrouded by the veil of secrecy that the prosecutors request here. These

---

<sup>3</sup> *See* Marcy Wheeler, *Was Adel Daoud Targeted Off of a Back Door Search of Traditional FISA Collection?*, Nov. 9, 2013, available at <http://www.emptywheel.net/2013/11/09/was-adel-daoud-targeted-off-of-a-back-door-search-of-tradition-fisa-collection/>.

<sup>4</sup> For example, if Defendant's online activity was initially collected through the NSA's bulk collection Internet metadata, a deeply problematic surveillance program discussed in a FISC opinion authored by Judge John D. Bates and publically disclosed on November 18, 2013, then prosecutors must provide notice of such collection pursuant to 50 U.S.C. § 1845. This opinion, which is discussed in greater detail below, is available at <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>.

disclosures are material to the Court's analysis for two principal reasons. First, they demonstrate that discussion of these once-secret issues in the public sphere is appropriate and, indeed, necessary. Second, and perhaps a corollary to the first point, the disclosures evidence how government attorneys have so far repeatedly mislead judges—either directly or through omission—in *ex parte* settings and why the disclosure of FISA materials and an adversarial hearing is necessary to guard against such misrepresentations. To appreciate this rather startling point, the Court need look no further than recently disclosed FISC opinions.

**a. Released FISC Opinions Evidence the Excesses of NSA Surveillance Programs and Government Officials' Repeated Misrepresentations Regarding Those Programs.**

Director of National Intelligence (“DNI”) James R. Clapper has acknowledged that in June 2013 President Obama directed him “to declassify and make public as much information as possible about certain sensitive programs while being mindful of the need to protect sensitive classified intelligence activities and national security.”<sup>5</sup> Pursuant to the President's directive, DNI Clapper has made a number of disclosures, the most recent, as of writing, being on November 18, 2013. DNI Clapper has described the material disclosed as of that date to consist of the following:

Nearly 2000 pages of documents released to the public so far, including 20 orders and opinions of the Foreign Surveillance Court, 11 pleadings and other documents submitted to the Court, 24 documents provided to Congress, and 20 reports, training slides, and other internal documents describing the legal basis for the programs and how they operate.<sup>6</sup>

---

<sup>5</sup> See *DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act*, available at <http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov>.

<sup>6</sup> *Id.* These materials are available at: <http://icontherecord.tumblr.com/tagged/declassified>.

The disclosed FISC opinions have been particularly illuminating in revealing how the intelligence agencies have persistently exceeded the scope of lawful surveillance. However, these same FISC opinions—of course, the result of secret *ex parte* proceedings—demonstrate that the government and its intelligence agencies get what they want with at most modest limits on their authority, notwithstanding the fact that some judges have sternly rebuked government officials and questioned their truthfulness.

For example, in a FISC opinion dated March 2, 2009, in the matter captioned *In re Production of Tangible Things From [REDACTED]*, Dkt. BR 08-13, Judge Reggie B. Walton of the District Court for the District of Columbia documented a number of statutory violations of the NSA's electronic surveillance programs.<sup>7</sup> Judge Walton expressly rejected the government's explanations for its violations and criticized its repeated misrepresentations and non-compliance with FISC orders. Specifically, Judge Walton wrote:

- “[t]he government’s submission suggests that its non-compliance with the Court’s orders resulted from a belief by some personnel within the NSA that some of the Court’s restrictions on access to the BR [Business Records] metadata applied only to “archived data” . . . That interpretation strains credulity.” p. 5;
- “[t]he government compounded its non-compliance with the Court’s orders by repeatedly submitting inaccurate descriptions of the alert list process to the FISC.” *Id.* at 6;
- “[i]n summary, since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses BR metadata. This misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government’s submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systematically violated that it can fairly be said that this

---

<sup>7</sup> A copy of this opinion is available at [http://www.dni.gov/files/documents/section/pub\\_March%20202009%20Order%20from%20FISC.pdf](http://www.dni.gov/files/documents/section/pub_March%20202009%20Order%20from%20FISC.pdf).

critical element of the overall BR regime has never functioned effectively.” *Id.* at 10-11;

- “[t]he record before the Court strongly suggests that, from the inception of this FISA BR program, the NSA’s data accessing technologies and practices were never adequately designed to comply with the governing minimization procedures.” *Id.* at 14-15; and
- “[u]nder these circumstances, *no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures.* In fact, the government acknowledges that, *as of August 2006, ‘there was no single person who had a complete understanding of the BR FISA system architecture’.*” *Id.* at 15 (emphasis added).<sup>8</sup>

Judge Walton’s serious criticisms were in no way isolated to the issues before him. In a declassified FISC opinion dated October 3, 2011, Judge John D. Bates of the District Court for the District of Columbia, found the NSA’s surveillance under the FAA to be “deficient on statutory and constitutional grounds,” particularly with regard to the mass collection of emails of American citizens that were entirely domestic and not to or from a foreign intelligence target.<sup>9</sup> Judge Bates also found that the NSA had been acquiring Internet transactions before the FISC even approved of such acquisitions. The highly critical tone of Judge Bates’ opinion is unmistakable, as seen in the following passages:

- “for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different than what the Court had been led to believe.” p. 28;
- “the Court is also unable to find that NSA’s targeting and minimization procedures, as the government proposes to implement them in connection with MCT’s [multi-communication transactions], are consistent with the Fourth

---

<sup>8</sup> See also Scott Shane, “Court Upbraided N.S.A. on Its Use of Call-Log Data,” *The New York Times*, September 10, 2013, available at <[http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html?pagewanted=all&_r=0)> (noting that, according to a senior U.S. intelligence official who briefed reporters just prior to release of the 2009 FISC opinion, “only about 10 percent of 17,800 phone numbers on the alert list in 2009 had met [the RAS] test,” and that “[t]here was nobody at N.S.A. who really had a full understanding of how the program was operating at the time”).

<sup>9</sup> A copy of this opinion is available at <http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf>.

Amendment.” *Id.* at 29;

- “NSA’s minimization procedures, as the government proposes to apply them to MCT’s as to which the ‘active user’ is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. §1881a(e) with respect to retention[.]” *Id.* at 80;
- “[t]he sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of transactions is not feasible.” *Id.* at 31;
- “the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States.” *Id.* at 31-32;
- “[e]ven if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA’s upstream collection . . . it is impossible to define with any specificity the universe of transactions that will be acquired by NSA’s upstream collection at any point in the future.” *Id.* at 32;
- “the actual number of wholly domestic communications acquired may still be higher in view of NSA’s inability conclusively to determine whether a significant portion of the MCT’s within its sample contained wholly domestic communications.” *Id.* at 34-35; and
- “the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year.” *Id.* at 43.19

Judge Bates found serious problems with the NSA’s collection of information in another extensive FISC Opinion, which the DNI released to the public on November 18, 2013.<sup>10</sup> As stated at the outset of this 117-page opinion, Judge Bates reviewed the government’s “application to re-initiate in expanded form a pen register/trap and trace (PRITT) authorization for the National Security Agency (NSA) to engage in bulk acquisition of metadata about Internet

---

<sup>10</sup> See *infra*, footnote 4. The opinion is available at <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf>. The opinion is undated, but is estimated to have been written between June 2010 and October 2011. See *A Secret Court Judge Warned The NSA It Was Close To Breaking The Law - Then Gave It More Power*, Nov. 20, 2013, available at: [http://www.huffingtonpost.com/2013/11/20/nsa-fisa-court-opinion\\_n\\_4311787.html](http://www.huffingtonpost.com/2013/11/20/nsa-fisa-court-opinion_n_4311787.html).

communications.” (p. 1).<sup>11</sup> In reviewing the government’s application, Judge Bates cited a number of the NSA’s “serious compliance problems” with the NSA’s collection of Internet metadata and its disregard of the limits imposed on it by the FISC.<sup>12</sup> These observations included the following:

- “the government acknowledges that the NSA exceeded the scope of authorized acquisition continuously during the more than [Redacted] years of acquisition under these orders.” (pp. 2-3).
- Judge Bates catalogued the NSA’s admitted “systemic” and “unauthorized” overcollection of American’s information that far exceeded the scope of what the FISC had approved, including:
  - “[t]he government disclosed that NSA had regularly accessed the bulk telephone metadata using a form of automated querying based on telephone numbers that had not been approved under the [reasonable articulable suspicion] standard.” *Id.* 14.
  - “[t]he government further disclosed that, apart from this shared database, NSA analysts made it a general practice to disseminate to other agencies NSA intelligence reports containing U.S. person information extracted from the PR/TT metadata without obtaining the required determination.” *Id.* at 18.
  - “[t]he government later advised that this continuous overcollection acquired many other types of data and that “[v]irtually every PR/TT record” generated by this program included some data that had not been authorized for collection. . . . The government has provided no comprehensive explanation of how so substantial an overcollection occurred, only the conclusion that [Redacted] there was a failure to

---

<sup>11</sup> The government also sought “Court authorization to query and use information previously obtained by NSA, regardless of whether the information was authorized to be acquired under prior bulk PR/TT orders of the [FISC] or exceeded the scope of previously authorized acquisition.” (pp. 1-2).

<sup>12</sup> According to Judge Bates’ order, the FISC initially granted the NSA’s collection of Internet metadata in an opinion by Judge Colleen Kollar-Kottely, who granted the NSA’s application for bulk pen register/trap & trace authorization. The DNI also released Judge Kollar-Kottely’s opinion on November 18, 2013, which is available at <http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf>. Notably, this bulk collection program—which had origins in the Bush Administration’s post-9/11 warrantless surveillance program—continued through 2011, when it was discontinued by the Obama Administration. See Glenn Greenwald and Spencer Ackerman, *NSA collected US email records in bulk for more than two years under Obama*, June 27, 2013, available at <http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorized-obama>.

translate the technical requirement [Redacted] into accurate and precise technical descriptions for the Court.” *Id.* at 19-20.

- “[a]s noted above, NSA’s record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained. See pages 18-19, *supra*. The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor.” *Id.* at 95.
- “the Court concludes that the government officials responsible for using and making disclosures of bulk PR/TT-derived information know or have reason to know that portions of the prior collection constitute unauthorized electronic surveillance.” *Id.* at 108.
- “[f]inally, insofar as the government suggests that the Court has inherent authority to permit the use and disclosure of all unauthorized collection without regard to Section 1809 .. the Court again must disagree. ... The plain language of Section 1809(a)(2) makes it a crime for any person, acting under color of law, intentionally to use or disclose information with knowledge or reason to know that the information was obtained through unauthorized electronic surveillance. The Court simply lacks the power, inherent or otherwise, to authorize the government to engage in conduct that Congress has unambiguously prohibited.” *Id.* at 112-113.

Despite the severity of Judge Walton’s and Judge Bates’ criticisms of the NSA’s abject failure to comply with the FISC’s orders, as well as the NSA’s repeated misrepresentations before the FISC, the NSA surveillance programs were ultimately allowed to continue with modifications and reporting requirements. The fact that the government almost inevitably prevails before the FISC, even where its compliance failures are clear, demonstrates the FISC’s extraordinarily accommodating approach to surveillance requests. This pattern is, without question, directly related to the absence of any adversarial process in the FISC, as well as the power of the government’s national security fear mongering rhetoric. Judge Bates’ Internet metadata opinion poignantly illustrates these points. Notwithstanding finding the “NSA’s longstanding and pervasive violations of the [FISC’s] prior orders, Judge Bates yielded in large

part to the government's request based on the government's assertion that "it has a strong national security interest in accessing and using the overcollected information." (Bates Order, pp. 115-16).

The FISC's acquiescence to the government's requests also underscores the importance of this Court's vigorous *de novo* review of the FISC's probable cause determinations. *See United States v. Dumeisi*, 424 F.3d 526, 578 (7<sup>th</sup> Cir. 2005); *United States v. Kashmiri*, 2010 U.S. Dist. LEXIS 119470, \*4 (N.D. Ill. Nov. 10, 2010) ("The court conducts a *de novo* review of the FISA materials to determine if the electronic surveillance authorization was based upon appropriate probable cause.") However, even a *de novo* review may have its limits, particularly given the government officials' demonstrated penchant for misleading the FISC and because, as discussed in detail below, the intelligence agencies routinely withhold critical information from the prosecutors. Disclosure of the FISA materials to cleared counsel and permitting a meaningful adversary hearing would go far in ensuring the fairness of proceedings and provide a significant boost to public perception that there is also meaningful Article III judicial review of what is now perceived as runaway, out of control, Executive Branch authority.<sup>13</sup>

**b. The Scope NSA Surveillance Programs Has Been Misrepresented to the Supreme Court.**

Government misrepresentations have not been limited to proceedings before the FISC in FISA-related matters. Indeed, such misrepresentations occurred before United States Supreme Court in the proceedings leading up to the Supreme Court's opinion, *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). In a November 20, 2013, letter from Senators Mark Udall (D-Colo.), Ron Wyden (D-Ore.), and Martin Heinrich (D-N.M.) to Solicitor General

---

<sup>13</sup> *See, e.g., Congress and Courts Want Restraints on N.S.A. Spying*, Adam Liptak and Jeremy W. Peters, N.Y. Times, Nov. 18, 2013, [http://www.nytimes.com/2013/11/19/us/politics/congress-and-courts-weigh-restraints-on-nsa-spying.html?pagewanted=1&\\_r=0&hp](http://www.nytimes.com/2013/11/19/us/politics/congress-and-courts-weigh-restraints-on-nsa-spying.html?pagewanted=1&_r=0&hp).

Donald Verrilli, the Senators expressed concern over misrepresentations that were made to the Supreme Court, and how such misstatements may have led to the Court's narrow 5-4 decision holding that the petitioners seeking to challenge the FAA lacked standing. The Senators' letter to the Solicitor General, which is attached hereto as Exhibit B, states as follows:

We are concerned that the Court's decision was not informed by a complete understanding of how the FISA Amendments Act (FAA) has been interpreted and implemented. Official records suggest that the Court was given misleading information that appears to have informed the majority's decision, and that some of these misleading statements have not yet been acknowledged or corrected.

The Senators' concerns focused on the government's statements that communications could only be intercepted under the FAA if the communications were actually to or from a foreign intelligence target. The Supreme Court relied on these representations. However, as the Senators observed, these representations were misleading in light of Judge Bates' October 2011 FISC opinion, in which Judge Bates found that the NSA collected "tens of thousands" of wholly domestic communications that were merely "about" a foreign intelligence target. The Senators concluded their letter by requesting "formal notification to the Supreme Court of the government's misrepresentations in [*Clapper*]"—both relating to its notice policy and relating to its practice of 'about' collection under [the FAA]."

**c. Recent Disclosures of the Use of NSA Surveillance in Criminal Cases Demonstrate that the DOJ's Policy Toward Greater Disclosure is Still Grossly Inadequate.**

In their November 20, 2013, letter, Senators Udall, Wyden, and Heinrich referenced how the DOJ recently acknowledged—for the first time—that the FAA was used in a criminal case. The Senators also noted the DOJ's prospective policy of notifying defendants when evidence against them was acquired or derived from the FAA. However, these changes in DOJ policy

came after five years of the DOJ implementing an untenable and legally unsupported interpretation of what was “derived” evidence. The Solicitor General, who learned of the DOJ’s interpretation only after his arguments in *Clapper*, concluded that the DOJ’s interpretation could not be justified legally.<sup>14</sup> While in one respect, this shift in DOJ policy toward greater transparency militates in favor of disclosure of the FISA materials to cleared counsel, the DOJ’s implementation of the policy has been woefully inadequate, and has highlighted the problems with its unjustifiable legal interpretation.

In terms of notice to criminal defendants, on October 25, 2013, prosecutors first disclosed the use of FAA surveillance to a criminal defendant in *United States v. Muhtorov*, 12-cr-00033-JKL (D. Colo.). This notice was not provided, however, until two years had passed since the initial FISA notice to the defense. In its one-paragraph supplemental notice, the prosecutors stated as follows:

[P]ursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the government intends to offer into evidence or otherwise use or disclose in proceedings in the above-captioned matter information obtained or derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

A copy of this notice is attached hereto as Exhibit C. Significantly, the *Muhtorov* case was one of the specific cases—along with Defendant’s case—that Senator Feinstein referenced in her December 27, 2012, Senate floor remarks in support of the re-authorization of the FAA.<sup>15</sup>

---

<sup>14</sup> See Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, Oct. 16, 2013, N.Y. Times, available at <http://mobile.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?from=us.politics>.

<sup>15</sup> The fact that the FAA was used in a case specifically referenced by Senator Diane Feinstein supports counsel’s reliance on the Senator’s statements as evidence that the FAA was used in this case—not that, as the prosecutors put it, counsel simply “misunderstand” the Senator’s remark. (Response, p. 49, footnote 25). Moreover, in light of the disclosure in the *Muhtorov* case, Senator Feinstein’s remark simply does not resemble the prosecutors’ description of it as “not a revelation that has any legal

However, neither Defendant nor any of the other defendants referenced by Senator Feinstein have been given notice of the use of FAA surveillance.

The DOJ has also begun to review all criminal cases in which the FAA was used, and to provide notice to defendants in some of those cases.<sup>16</sup> However, notice has only been provided to defendants who have already been convicted, and thus had no opportunity to challenge the surveillance in pre-trial motions or at trial.

On November 19, 2013, prosecutors filed a “Supplemental FISA Notification” in *United States v. Mohamud*, 10-cr-471-KI (D. Ore.), which indicated that evidence derived from FAA surveillance was in fact used against the defendant at the trial which resulted in his conviction. That supplemental FAA notice, attached hereto as Exhibit D, provides as follows:

This supplemental notice is being filed as a result of the government’s determination that information obtained or derived from Title I FISA collection may, in particular cases, also be “derived from” prior Title

---

implication.” Further, the FAA notice in the *Muhtorov* case also casts doubt—or at a minimum further confusion—on Senate Legal Counsel Morgan Frankel’s September 16, 2013, written explanation of Senator Feinstein’s comments provided to undersigned counsel. A copy of that explanation was attached as Exhibit B to Defendant’s September 18, 2013, Motion for FAA Discovery (Dkt. #70). The Senate Legal Counsel’s explanation of Senator Feinstein’s December 27, 2012, comments bears repeating here in light of the *Muhtorov* disclosure:

Without waiving Senator Feinstein’s or the Intelligence Committee’s legislative privileges, I would like to provide some clarification that may help explain a misunderstanding of the Chairman’s remarks on which your documentary request is predicated. Notwithstanding that she was speaking in support of reauthorization of Title VII of the Foreign Intelligence Surveillance Act, Senator Feinstein did not state, and did not mean to state, that FAA surveillance was used in any or all of the nine cases she enumerated, including Mr. Daoud’s case, in which terrorist plots had been stopped. Rather, the nine cases the Chairman summarized were drawn from a list of 100 arrests arising out of foiled terrorism plots in the United States between 2009 and 2012 compiled by committee staff from *FBI press releases and other public sources*.

(Dkt. #70, Exhibit B) (emphasis in original).

<sup>16</sup>See *Justice is reviewing criminal cases that used surveillance evidence gathered under FISA*, Sari Horwitz, Wash. Post., Nov. 15, 2013 (available at: [http://www.washingtonpost.com/world/national-security/justice-reviewing-criminal-cases-that-used-evidence-gathered-under-fisa-act/2013/11/15/0aea6420-4e0d-11e3-9890-a1e0997fb0c0\\_story.html](http://www.washingtonpost.com/world/national-security/justice-reviewing-criminal-cases-that-used-evidence-gathered-under-fisa-act/2013/11/15/0aea6420-4e0d-11e3-9890-a1e0997fb0c0_story.html)).

VII FISA collection. Based upon that determination and a recent review of the proceedings in this case, the United States hereby provides notice to this Court and the defense, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1881a.

Notably, counsel in the *Mohamud* case—which bears numerous striking similarities to this case, particular insofar as the FBI’s targeting of Muslim teenagers who express controversial views and equipping them with *faux* car bombs—specifically requested disclosure of FAA material in their pretrial motions. However, the government refused to disclose this critical evidence until *after* the defendant had already been convicted at a jury trial.

Similarly, in *United States v. Moalin*, 10-cr-4246-JM (S.D. Cal.),<sup>17</sup> the defendants specifically requested notice of any surveillance made pursuant to any warrantless wiretapping programs or under constitutionally infirm FISA Amendments. *See United States v. Moalin*, 10-cr-4246, Dkt. #92, pp.16-18. However, it was not until after the defendants were convicted that it was disclosed, initially on June 18, 2013, by intelligence officials from the NSA and FBI in testimony to the House Select Intelligence Committee, that the provisions of Section 215 were used to collect phone calls of the lead defendant *Moalin*, which ultimately led to the federal criminal charges.<sup>18</sup> Again, as in the *Mohamud* case, these material facts were not disclosed and could not be used by the defense to test the legality of the government’s investigation and the evidence it presented at trial. Perhaps even more significant is the fact that the prosecutors *still*

---

<sup>17</sup> *Moalin* involved charges against four defendants for providing material support to the designated foreign terrorist organization *al Shabaab*. Undersigned counsel represent Ahmed Nasir Taalil Mohamud, one of the four defendants.

<sup>18</sup> *See* Transcript of June 18, 2013, Hearing before House Select Intelligence Committee, pp. 5, 1, available at [http://www.fas.org/irp/congress/2013\\_hr/disclosure.pdf](http://www.fas.org/irp/congress/2013_hr/disclosure.pdf).

have not provided formal notice to defense counsel about the use of Section 215 surveillance in the *Moalin* case.

These cases illustrate how the government has used its wide-ranging and constitutionally suspect surveillance programs in an unknown number of criminal cases without any disclosure to defendants or accountability to the courts. Counsel respectfully submit that disclosure of the FISA materials should be made now, prior to trial, and that cleared counsel be allowed to participate in the testing of the legality of the FISA surveillance. This would eliminate the prospect of any post-trial disclosures in *Mohamud* and *Moalin* and the consequent irreparable harm to Defendant's fair trial rights.

**2. Disclosure of FISA Materials to Cleared Defense Counsel and an Adversarial Hearing are Necessary to Make an Accurate Determination of the Legality of the Surveillance in this Case.**

Even after the Attorney General submits an affidavit triggering *in camera*, *ex parte* review of the FISA materials, the Court has the authority to disclose those materials to defense counsel "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Here, disclosure is necessary for a number of reasons, particularly in light of prosecutors' demonstrated history of misleading the courts regarding intelligence matters, especially in terrorism cases.

**a. An Adversarial Hearing is Necessary Because the Court Cannot Rely on the Prosecutors in an *In Camera*, *Ex Parte* Setting to Inform it of All Material Facts, Particularly Those Adverse to the Government's Interests As Required by Rule 3.3(d) of the Illinois Rules of Professional Conduct and *Brady*.**

Terrorism cases are now being prosecuted by intelligence gathering agencies, not criminal investigative agencies as has traditionally been the case in Article III criminal prosecutions. This subtle but significant paradigm shift has resulted in the sad but inescapable

fact that the usually reliable representations of the U.S. Attorney's Office can no longer be trusted because the Intelligence Agencies—as has been adequately demonstrated by the FISC opinions—simply do not inform the local prosecutors of all material information.<sup>19</sup> As a result, the prosecutors do not—and cannot be expected to—present to the Court all the information it requires to make accurate and informed decisions.<sup>20</sup> This, perhaps above all, demands cleared counsel's participation in an adversarial proceeding.

The Intelligence Agencies' total dominion over what information is actually disclosed in terrorism prosecutions undermines the legitimacy of *in camera*, *ex parte* FISA proceedings, and prevents the Court from making accurate determinations as to the legality of the government's surveillance. Due to information withheld from prosecutors, the Court cannot expect the prosecutors to comply with their professional ethical duties to ensure that the defendant's rights are adequately represented in the *ex parte* proceedings. This subtle, but critical, shift in the

---

<sup>19</sup> Further underscoring this point are the revelations of “intelligence laundering” associated with the “parallel construction” investigations conducted by the Special Operation Division (SOD) of the DEA, which involved the SOD obtaining information from the NSA, and then recreating the source of the information to conceal its true origins. See Shiffman, John; Kristina Cooke (Aug 5, 2013), Exclusive: U.S. directs agents to cover up program used to investigate Americans, Reuters (available at <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>); Hanni Fakhoury, *DEA and NSA Team Up to Share Intelligence, Leading to Secret Use of Surveillance in Ordinary Investigations*, Electronic Frontier Foudnation, Aug. 6, 2013, available at <https://www.eff.org/deeplinks/2013/08/dea-and-nsa-team-intelligence-laundering>.

<sup>20</sup> This is in no way a criticism of the U.S. Attorney's Office or the particular prosecutors in this case whose integrity is beyond question. However, as is often said, one cannot know what one does not know. The simple fact of the matter is that the U.S. Attorneys are literally at the mercy of the intelligence agencies insofar as it concerns what information will be revealed even to them. In many ways, it seems that the spy agencies are as fearful of the prosecutors as they are defense counsel since what seems to concern the spies the most is their spying capabilities and techniques that can be just as easily compromised from their perspective by a prosecutor as a defense lawyer, not to mention a judge based upon the behavior in the FISC. But then again, this should surprise no one since Mr. Clapper himself could not see fit even to trust Congress. See Ruth Marcus, *James Clapper's 'least untruthful' answer*, Wash. Post, June 13, 2013, available at [http://articles.washingtonpost.com/2013-06-13/opinions/39950057\\_1\\_oversight-national-intelligence-national-security-agency](http://articles.washingtonpost.com/2013-06-13/opinions/39950057_1_oversight-national-intelligence-national-security-agency) (discussing how DNI Clapper admitted that he responded in the “least untruthful manner” to Senator Wyden who asked if the NSA was collecting data about millions of Americans).

paradigm of federal criminal prosecutions has not received the attention it deserves, but is one for which a seasoned trial judge should well be on the alert. In that times have changed, judicial attitudes must change as well. The days of the unspoken trust between the U.S. Attorney's Office and the courts are now as antiquated—at least in terrorism related cases—as the days of getting on board an airplane without screening.

In terms of the aforementioned ethical duties, Rule 3.3(d) of the Illinois Rules of Professional Conduct, entitled “Candor Toward the Tribunal” provides as follows:

In an *ex parte* proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Rule 3.3(d) (emphasis added).<sup>21</sup> Thus, because disclosure is conditioned upon what is “known” to the prosecutors, the “new normal” of Intelligence Agency-driven terrorism prosecutions should give the Court little faith that it will be provided with all material facts necessary to make an informed decision.

Setting this professional ethics dilemma aside, the withholding of evidence by the intelligence agencies from the local prosecutors is all the more problematic because it also

---

<sup>21</sup> The Illinois Rules of Professional Conduct are available online at: [http://www.state.il.us/court/supremecourt/rules/art\\_viii/default\\_new.asp](http://www.state.il.us/court/supremecourt/rules/art_viii/default_new.asp). Illinois Rule 3.3 is identical to ABA Model Rule 3.3. The comment to Illinois Rule 3.3, which also mirrors the comment to the ABA Model Rule, emphasizes the duty of the represented party as well as the Court to protect the rights of the party not before the Court. The comment is as follows:

Ordinarily, an advocate has the limited responsibility of presenting one side of the matters that a tribunal should consider in reaching a decision; the conflicting position is expected to be presented by the opposing party. However, in any *ex parte* proceeding, such as an application for a temporary restraining order, there is no balance of presentation by opposing advocates. The object of an *ex parte* proceeding is nevertheless to yield a substantially just result. The judge has an affirmative responsibility to accord the absent party just consideration. The lawyer for the represented party has the correlative duty to make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an informed decision.

prevents prosecutors from meaningfully fulfilling their legal obligations under *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny. Prosecutors have a “duty to learn of any favorable evidence known to others acting on the government’s behalf in the case, including the police.” *Kyles v. Whitley*, 514 U.S. 419, 437 (1995). Indeed, the U.S. Attorney’s Criminal Resource Manual recognizes that prosecutors have an obligation to search intelligence community files under certain circumstances, including when the intelligence community has played an active role in the investigation or prosecution of a case, or when the facts and circumstances of a case indicate that there may be *Brady* material in the intelligence community files. *See Contacts with the Intelligence Community Regarding Criminal Investigations or Prosecutions*, available at [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/crm02052.htm](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm02052.htm). However, as anyone who has been involved in terrorism cases can readily attest, prosecutors must navigate a bureaucratic gauntlet imposed to even obtain classified information, which is then subject to the non-disclosure provisions of CIPA. It would be naïve to assume that Intelligence Agencies readily ensure that prosecutors comply with their *Brady* obligations.

The disconnect between the Intelligence Agencies and prosecutors is precisely why Senators Udall, Wyden, and Heinrich were compelled to ask Solicitor General Verrilli to clarify precisely what was known about the NSA’s collection of domestic communications “about” an FAA target and what was told to the Supreme Court.

**b. Adversarial Testing, not Secret *Ex Parte* Proceedings is the Rule in Criminal Prosecutions.**

Indeed, counsel has already discussed at length the importance of the adversarial process. (Memorandum, pp. 26-30). Rather than respond to those arguments in its unclassified response, the prosecutors simply conclude that the “rule” for these proceedings is *in camera, ex parte*

review, and then go on to boast how no court has ever allowed disclosure of classified FISA materials or ordered the suppression of FISA-derived or-obtained evidence. (Response, pp. 20-21). The “perfect record” argument can be quickly dispatched.

It is obvious that the government’s nearly perfect track record in the FISC is a direct result of the absence of disclosure and the lack of any adversarial process. Counsel submit instead that a unanimous rubber-stamp FISC approval proves the opposite. That is, it proves not that the system is working, but that there is most certainly something inherently flawed with the process. This is even truer with respect to the fact that, as the government stresses, no federal district court has ordered an adversarial hearing regarding the legality of FISA surveillance in a criminal case.

The prosecutors also argue that its FISA submissions “are well-organized and easily reviewable,” as if that were sufficient to obviate the need for adversarial proceedings. (Response, p. 21). However, the organization of the materials is not the touchstone for making an accurate determination of the legality of the surveillance. The only true test is subjecting those materials to adversarial inquiry.

The prosecutors further argue that “there is nothing extraordinary about the instant FISA-authorized electronic surveillance and physical searches that would justify this case becoming the first ‘exception’ to the rule of all previous FISA litigation.” (Response, p. 20). The “extraordinary” nature of a case is legally irrelevant for the Court to decide whether to allow disclosure of the FISA materials to defense counsel, and the Court should reject the government’s position out-of-hand.<sup>22</sup>

---

<sup>22</sup> It must also be noted that the government used almost the exact same language to describe the *Moalin* case, when it wrote in its unclassified response to the defendants’ FISA motion to suppress the following: “There is nothing extraordinary about this case that would prompt the Court to be the first to order the disclosure of *highly* sensitive and classified FISA materials.” (*United States v. Moalin*, 10-cr-4246, Dkt.

**c. The FISA Materials Should be Disclosed to Cleared Defense Counsel to Ensure Accurate Determinations of the “Agent of a Foreign Power” and “Foreign Intelligence Information” Factors.**

A valid FISA order could have been issued only if there was “probable cause to believe that (A) the target of the electronic surveillance and/or search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power.” 50 U.S.C. § 1805(a)(2).

Before their redacted argument, the prosecutors quip that “the defendant offers a naïve understanding of the level of criminality in which individuals of his age can engage in.” (Response, p. 50). Whatever is set forth in the redacted argument, it cannot be any reference to Defendant’s criminality—that is before the government targeted him and through the concerted efforts of multiple agents online and in person and supplied him with a *faux* car bomb. Indeed, Defendant had no criminal history prior to this case, which means that the government’s observation about the “criminality in which individuals of his age can engage in” is simply an abstract observation. Nevertheless, speaking of naivety, this meaningless general observation could not possibly be used as a basis for probable cause in this specific FISA application.

Rather than “criminality,” Defendant, like millions of other Americans (and in particular teenagers) was a frequent visitor to internet websites such as YouTube and Yahoo. While some of his comments on those websites may be deemed objectionable—particularly by the government—they are certainly not criminal or grounds for FISA surveillance. That is

---

123, p. 19) (emphasis in original). However—and contrary to the government’s flippant comment about that case not being extraordinary and the “*highly*” sensitive nature of the FISA materials—the *Moalin* case was, in fact, extraordinary by the intelligence officials’ own statements before Congress, as it was publicly lauded as an example of the successful use of Section 215 programs in a federal terrorism prosecution.

particularly so because FISA specifies that “no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the First Amendment.” § 1805(a)(2)(A).

Indeed, even the government’s own documents cast doubt on the existence probable cause to believe that Defendant was an “agent of a foreign power.” Counsel submit that a report concerning the opening of the investigation into Defendant raises serious questions about whether there existed probable cause to believe that Defendant was an agent of a foreign power. This declassified report is attached hereto as Exhibit E and filed under seal pursuant to the terms of the Protective Order. While Counsel believe that the problems raised by this report are plain on its face, should the Court require, counsel would most certainly address any additional questions in an appropriate setting.

Likewise, disclosure of FISA materials to counsel is necessary for the Court to determine whether the prosecutors’ certification that a “significant purpose of the surveillance is to obtain foreign intelligence information”<sup>23</sup> was clearly erroneous. *See* § 1804(a)(6)(B); 1805(a)(5). Cleared counsel can provide the court with a unique and important perspective that prosecutors simply cannot offer. Specifically, based on their knowledge of Defendant and his communications, cleared counsel can help the Court contextualize any communications or comments that were used in the FISA certification. This would assist in making an accurate determination of whether the surveillance could obtain “foreign intelligence information.”

Thus, given the fundamental First Amendment concerns and the necessity for providing

---

<sup>23</sup> Pursuant to 50 U.S.C. § 1801(e), “foreign intelligence information” is defined as: Information that relates to and is necessary to the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

the appropriate context, meaning, and weight of Defendant's online activity as well as the fact that the government's own reports fail to evidence probable cause that Defendant is an agent of a foreign power, disclosure to counsel "is necessary to make an accurate determination of the legality of the surveillance." §1806(f).

**d. Disclosure of the FISA Materials is Necessary to Determine if the FISA Surveillance was Based on any Unlawful or Constitutionally Infirm Surveillance or Data Collection.**

The prosecutors contend that disclosure based on the FAA "is unwarranted here because the FAA is simply not at issue in this case" because they say that they "do[ ] not intend to use any such evidence obtained or derived from FAA-Authorized surveillance in the course of this prosecution." (Response, pp. 48-49). However, that self-serving argument does not answer the fundamental question raised by this issue—whether the FAA or any other constitutionally infirm surveillance provided or led to any information that was presented to the FISC in a FISA application or certification. The government could—and could have long ago—put this issue to rest with a simple "yes" or "no" answer to the question of whether the FAA had any role in this case. Instead, the prosecutors, likely at the insistence of the Intelligence Agencies, have again opted for opacity.

Obviously, if cleared counsel are to raise any meaningful suppression motion or challenge the legality of the FISA surveillance in this case, the Court should examine, and disclose to cleared counsel as necessary, "the nature, genesis, and provenance of the information in the FISA application." (Memorandum, p. 16).

**3. The Prosecutor's Minimization and "Good Faith" Doctrine Arguments Would Eviscerate the Exclusionary Rule and Should be Rejected.**

In their discussion of minimization in the FISA context, the prosecutors focus on factors

that they argue would excuse the over-collection of communications, such as the use of coded communications, false identities, and clandestine activities associated with foreign powers and their agents. (Response, pp. 34-36). In essence, the prosecutors argue that only interceptions that were not properly minimized need to be suppressed. However, accepting this circular argument would effectively give prosecutors immunity to avoid minimization altogether. In other words, no law enforcement agent would need to care about minimization if the only consequence for failing to minimize was the exclusion of the non-pertinent intercepts that should have been minimized in the first place. As seen in Judge Walton's and Judge's Bates' FISC opinions, even the FISC has expressed serious concerns over the government's cavalier approach to minimization in the FISA context.

Based on the discovery and counsel's understanding of Defendant's extensive online communications on popular websites, proper minimization is a matter of serious concern here. Given counsel's familiarity with the nature of Defendant's communications, disclosure of the FISA materials to cleared counsel would certainly help the Court accurately determine the legality of the FISA surveillance. At a minimum, the Court should not merely accept the government's arguments regarding minimization—which, of course, counsel cannot respond to as they are redacted.

Along similar lines, the government should not accept the government's attempt to import into the FISA process the doctrine of "good faith," either in the minimization context or with regard to probable cause. (Response, pp. 29-31). First, the good faith exception does not apply to FISA suppression, because suppression is statutorily mandated if the Court determines that the surveillance was not lawfully authorized or conducted. 50 U.S.C. 1806(g).<sup>24</sup> Moreover,

---

<sup>24</sup> Section 1806(g) provides: "If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, *it shall*, in accordance with the

FISA already includes substantially reduced standards for probable cause, minimization, and judicial review. If the “good faith” doctrine were imported, the statutory protections of FISA would be further diluted. *See also Davis v. United States*, \_\_\_ U.S. \_\_\_, 131 S. Ct. 2419, 2440 (2011) (Breyer, J., dissenting) (criticizing “trend” of good faith exception swallowing the exclusionary rule). Additionally, given that the *in camera*, *ex parte* setting would further insulate any challenge to the declarations in the government’s FISA certifications and applications, the “good faith” doctrine would render any meaningful challenge virtually impossible. Lastly, the government’s horrendous track record for honesty before the FISC, as noted in the FISC opinions cited *infra*, should give the Court serious pause before crediting any of the representations FISA applications and certifications.

**4. The National Security Interests of the Intelligence Agencies Do Not Trump Defendant’s Constitutional Rights to a Fair Trial.**

As counsel previously noted, any security concerns regarding the disclosure of FISA materials are adequately addressed by the fact that counsel for Defendant possess security clearances. (Memorandum, p. 25, footnote 14). Counsel would also consent to any protective orders deemed necessary by the Court. Rather than address these points regarding “appropriate security procedures and protective orders”—which are expressly mentioned in § 1806(f) in the context of disclosure to the defense—the prosecutors, presumably at the behest of the Intelligence Agencies, once again play their ace—the ubiquitous War on Terror fear card. In a stunning sentence that has become a tenet of the all-encompassing national security complex, the prosecutors essentially tell the Court to defer to the intelligence agencies because they “know better,” and acting to the contrary would allegedly put the nation’s security at risk:

---

requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person.” (emphasis added).

When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States.

(Response, p. 22). If that were not enough, the prosecutors go so far as to say that permitting an adversary hearing would “*create* potential dangers that courts have consistently sought to avoid.”

(Response, p. 23) (emphasis in original).

However, the mere reference to national security interests and the far-fetched risk that “spies” might “piec[e] together a mosaic information” does not compel the Court to abdicate its constitutional duties. Defense counsel, who possess the same security clearances as the prosecutors and the Court, are not comprised of “foreign agents, spies, and terrorists[,]” and do not seek any public disclosure or dissemination of the FISA materials.

It is precisely under these unique circumstances when the Court should be more, rather than less vigilant of protecting individual constitutional rights, rather than bowing to the preferences of a co-equal branch of government. Indeed, the prosecutors’ prerogatives must give way to Defendant’s constitutional rights to defend this case, as the prosecutors cannot bring a prosecution and then refuse to disclose evidence simply on the ground that such disclosure could reveal secrets and harm the national interest. Indeed, in *United States v. Reynolds*, 345 U.S. 1, 12 (1953), the Supreme Court observed:

The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

Similarly, in *United States v. Nixon*, where the Supreme Court considered a claim of executive privilege in the infamous Watergate case, the Court emphasized the prevailing due process principles when it observed:

But this presumptive privilege must be considered in light of our historic commitment to the rule of law. This is nowhere more profoundly manifest than in our view that ‘the twofold aim (of criminal justice) is that guilt shall not escape or innocence suffer.’ *Berger v. United States*, 295 U.S., at 88, 55 S.Ct., at 633. We have elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense.

*United States v. Nixon*, 418 U.S. 683, 708-709 (1974).<sup>25</sup>

It is these fundamental due process concerns that present this Court with the unique opportunity to exercise its Article III authority and curtail the continued secrecy that has led to rampant violations that have gone on virtually unchecked. Allowing disclosure of FISA

---

<sup>25</sup> Likewise, in *United States v. Fernandez*, 913 F.2d 148 (4<sup>th</sup> Cir. 1990), a case involving the Classified Information Procedures Act (CIPA), the Fourth Circuit Court of Appeals affirmed the dismissal of an indictment when the government refused to turn over information that it deemed classified to the defendant. The Court described the problem caused by the government’s stance in these terms: “the government is simultaneously prosecuting the defendant and attempting to restrict his ability to use information that he feels is necessary to defend himself against the prosecution.” *Fernandez*, 913 F.2d at 154. The Court further observed that, notwithstanding CIPA’s “streamlined” procedures for using classified information “courts must not be remiss in protecting a defendant’s right to a full and meaningful presentation of his claim to innocence.” *Id.* See also *Zoltek Corp. v. United States*, 86 Fed. Cl. 738, 743 (Fed. Cl. 2009) (observing principle in criminal cases “in which courts held that it was unconscionable (and unconstitutional) for the Government to bring charges against a defendant while using the state secrets privilege to deny the defendant access to evidence that may have been material to his or her defense”); *United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950) (L. Hand, J.) (“[T]he prosecution must decide whether the public prejudice of allowing the crime to go unpunished [is] greater than the disclosure of such ‘state secrets’ as might be relevant to the defence.”).

materials and providing for an adversary hearing regarding the legality of the FISA surveillance would not only discharge this Court's Article III duties, but would help restore the integrity and accountability of the federal criminal justice system. The status quo alternative would be to simply perpetuate the pretense of the one-sided process conducted in secret where a defendant has no legitimate chance to prevail. In short, this decision leaves the Court with a stark alternative—to restore the federal criminal justice system to its traditional adversarial context—or simply admit that we have become too fearful to permit use of the adversarial process in terrorism related cases when the Attorney General, at the behest of the Intelligence Agencies, tells the Judicial Branch to back off and accept the Executive Branch's word on nothing more than its own say-so.

Respectfully submitted,

/s/ Thomas Anthony Durkin  
**THOMAS ANTHONY DURKIN,**

/s/ Janis D. Roberts  
**JANIS D. ROBERTS,**

/s/ Joshua G. Herman  
**JOSHUA G. HERMAN,**  
Attorneys for Defendant Adel Daoud.

**DURKIN & ROBERTS**  
2446 N. Clark Street  
Chicago, Illinois 60614  
(312) 913-9300  
tdurkin@durkinroberts.com  
jdroberts@durkinroberts.com  
jherman@durkinroberts.com

**CERTIFICATE OF SERVICE**

Thomas Anthony Durkin, Attorney at Law, hereby certifies that Defendant's Reply in Support of His Motion for Disclosure of FISA-Related Material and to Suppress the Fruits or Derivatives of Electronic Surveillance and Any Other Means of Collection Conducted Pursuant to FISA or Other Foreign Intelligence Gathering was served on November 25, 2013, in accordance with Fed.R.Crim.P.49, Fed.R.Civ.P.5, LR 5.5, and the General Order on Electronic Case Filing (ECF) pursuant to the district court's system as to ECF filers.

/s/ Thomas Anthony Durkin

**THOMAS ANTHONY DURKIN**

2446 N. Clark Street

Chicago, IL 60614

(312) 913-9300

tdurkin@durkinroberts.com