UIC
REVIEW OF INTELLECTUAL PROPERTY LAW

THIS IS FISA CALLING TO LET YOU KNOW YOU MAY BE ELIGIBLE FOR A MOTION TO SUPPRESS: NEW NOTICE REQUIREMENT FROM *UNITED STATES V. MOALIN*

JENNIFER E. ARMSTRONG

ABSTRACT

The September 11th terrorist attacks claimed the lives of nearly 3,000 people. Immediately following the attacks, Americans rose to the challenge and willingly ceded some of their civil liberties to in order to strengthen national security. However, after Edward Snowden disclosed the National Security Agency's rampant bulk collection of metadata from U.S. citizens in 2013, concern about privacy returned to the forefront of conversation. The government contended that this was a necessary program that yielded positive results. However, the only case in which the bulk collection of metadata had successfully thwarted a terrorist plot was in the case of Moalin, a Somali man living in Southern California who sent money to al-Shabaab. To much surprise, the Ninth Circuit ruled that the bulk collection of metadata exceeded the scope of Congress' authorization under FISA. The Ninth Circuit held that the government is required to notify defendants that electronic surveillance occurred, and that the government intends to use the obtained information at trial, allowing defendants to file a motion challenging its admission. Despite creating this test, the Ninth Circuit refrained from applying it to Moalin's case. It remains to be seen if this decision is emblematic of the turning tides in privacy law in the twenty years following the September 11th attacks, or if this decision remains the outlier and the one success story of the government's bulk metadata collection program.

UIC JOHN MARSHALL LAW SCHOOL

Cite as Jennifer Armstrong, *This is FISA Calling to Let You Know You May Be Eligible for A Motion to Suppress: New Notice Requirement from United States v. Moalin*, 20 UIC REV. INTELL. PROP. L. 166 (2021).

THIS IS FISA CALLING TO LET YOU KNOW YOU MAY BE ELIGIBLE FOR A MOTION TO SUPPRESS: NEW NOTICE REQUIREMENT FROM *UNITED STATES V. MOALIN*

JENNIFER E. ARMSTRONG

THIS IS FISA CALLING TO LET YOU KNOW YOU MAY BE ELIGIBLE FOR A MOTION TO SUPPRESS: NEW NOTICE REQUIREMENT FROM *UNITED STATES V. MOALIN*

JENNIFER E. ARMSTRONG*

I. INTRODUCTION

On September 11th, 2001, the United States suffered the worst terrorist attack it had ever experienced on U.S. soil.[1] Nearly 3,000 people lost their lives in this coordinated attack that fundamentally changed the way Americans view national security.[2] In the aftermath of September 11th, the United States Government had to prove to Americans that they would be safe in their homeland and that the government would not fail them again.

In furtherance of this objective, Congress passed the USA PATRIOT Act,[3] which expanded many capabilities of the United States Government, including the Foreign Intelligence Surveillance Court ("FISA court").[4] Congress originally created the FISA court in 1978 in order to create a system where the executive branch could obtain authorization for surveillance on foreign actors.[5] The FISA court operates in a necessary layer of secrecy that often does not allow for non-governmental lawyers to be party to the hearings.[6] This secrecy is a necessary component of building cases against foreign threats to the United States, principally terrorists.[7]

Twelve years after the September 11th terrorist attacks, *The Guardian* published a series of articles[8] about the National Security Agency's ("NSA") practice of bulk collection of metadata with documents supplied by former NSA employee, Edward

---

* © Jennifer Armstrong 2021. J.D. Candidate, UIC John Marshall Law School (2022). B.A. in International Relations, Boston University (2018). I would like to thank my editors and my family for all of their support and guidance. No one accomplishes anything alone.

[1] Steven Brill, *Is America Any Safer?*, THE ATLANTIC (Sept. 2016), https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/.

[2] *Id.*

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.).

[4] REBECCA WOODS ET AL., DATA SECURITY AND PRIVACY LAW § 6.46 (2020).

[5] *Id.*

[6] *Id.* (The primary purpose of the FISA court is to review warrant applications from the Attorney General regarding the electronic surveillance for foreign intelligence purposes.).

[7] Privacy and Civil Liberties Oversight Board, Rep. on the Tel. Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 13 (Jan. 23, 2014), https://www.judiciary.senate.gov/imo/media/doc/PCLOBReport.pdf [hereinafter Privacy and Civil Liberties Oversight Board].

[8] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily,* THE GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. (This article was the first in a series of articles run by *The Guardian* based off of information given to them by Edward Snowden.).

Snowden.[9] Metadata is information, "includ[ing] comprehensive communications routing information, including . . . identifying information (e.g., originating and terminating telephone number, communications device identifier, etc.) trunk identifier, and time and duration of call."[10] This release sparked a series of controversies over the legality of the NSA's metadata collection program and other mass data collection programs. On September 2, 2020, the Ninth Circuit ruled in *United States v. Moalin* that the NSA's bulk collection of metadata exceeded the authorization of Congress and violated section 1861 of the FISA Act.[11]

While this decision is a significant step towards curtailing the government's ability to collect bulk metadata, it was not the most important part of the opinion. On appeal, Moalin and his co-defendants challenged the metadata evidence under the Fourth Amendment, arguing that they were entitled to receive notice of any additional surveillance that they had been subjected to through a warrant authorized by FISA Subchapter I.[12] The Ninth Circuit developed a new test for notice, stating that, "the government is required only to inform the defendant that surveillance occurred and that the government intends to use the information obtained or derived from it [in a criminal prosecution]."[13] If the government does not feel comfortable disclosing the information for national security reasons, the court can review the information through *ex parte* communications or *in camera*.[14] Despite the Ninth Circuit creating this new notice test, it did not apply it in *Moalin* because it found that the exclusion of the metadata would not change the outcome of the case.[15]

This notice requirement has never been applied to additional electronic surveillance derived from a FISA warrant in a criminal prosecution because the government and FISA court traditionally have given the "derived from" language a narrow interpretation.[16] This new notice requirement may leave the door open for other circuits to determine that the government must provide notice to the defendant of any additional electronic surveillance derived from a FISA warrant, not just the surveillance that the government intends to use in court.[17]

This note argues that the new notice requirement established by the Ninth Circuit in *Moalin* is necessary to protect the Fourth Amendment rights of United States citizens who are being electronically surveilled by the United States

---

[9] Mattathias Schwartz, *The Whole Haystack: The N.S.A. Claims it Needs Access to All Our Phone Records. But is That the Best Way to Catch a Terrorist?*, THE NEW YORKER (Jan. 19, 2015), https://www.newyorker.com/magazine/2015/01/26/whole-haystack.

[10] *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]* ("2006" Primary Order), No. BR 06-05, slip op. at 2 (F.I.S.C. May 24, 2006), 2, https://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

[11] 973 F.3d 977, 996 (9th Cir. 2020) (The Ninth Circuit found that the bulk collection of metadata violated 50 U.S.C. § 1861. This section dictates the requirements the Attorney General must prove in its application in order to obtain a warrant for electronic surveillance from the FISA court.).

[12] *Id.* at 997-998. (FISA Subchapter I is comprised of 50 U.S.C. § 1801 – 1812.).

[13] *Id.* at 1001.

[14] *Id.*

[15] *Id.*

[16] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), https://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html.

[17] United States v. Moalin, 973 F.3d 977, 1001 (9th Cir. 2020).

Government. Part II provides an evolution of FISA law and its contention with the Fourth Amendment's notice requirement. Part III provides greater detail and background on *United States v. Moalin*.[18] Part IV analyzes the untested notice requirement and its implications on the FISA court and other circuits. Part V concludes that the notice requirement is necessary to ensure United States citizens are able to exercise their Fourth Amendment rights after being electronically surveilled by the United States Government.

II. BACKGROUND

In order to analyze Fourth Amendment challenges in FISA related cases, it is important to first examine how the Fourth Amendment's notice requirement operates in ordinary jurisprudence. Next, it is important to discuss the evolution of FISA law. After examining both of these topics, this section will explore how the Fourth Amendment applies in FISA related cases.

A. *Fourth Amendment Jurisprudence Regarding Notice*

The Fourth Amendment protects against unlawful searches and seizures.[19] The Fourth Amendment requires that the person be notified that they are subject to a search unless there are exigent circumstances.[20] When the Fourth Amendment was drafted, notice was easy to give and receive because the individual subject to the search would be able to physically observe officers of the government looking through their belongings.[21] However, when electronic surveillance of any kind is involved, it can work against the goal of the surveillance and prematurely alert the target of the on-going investigation. Courts have found that there is no requirement of advance notice in cases such as wiretapping, where the notice would encourage the target to discontinue use of that method of communication.[22] Under these circumstances, there needs to be a constitutionally adequate substitute for advance notice, such as notification upon completion of the operation.[23]

---

[18] *Id.*

[19] U.S. CONST. amend. IV.

[20] Berger v. State of N.Y., 388 U.S. 41, 60 (1967).

[21] Orin Kerr, *Did the Ninth Circuit Create a New Fourth Amendment Notice Requirement for Surveillance Practices?*, LAWFARE (Sept. 9, 2020, 7:01 AM), https://www.lawfareblog.com/did-ninth-circuit-create-new-fourth-amendment-notice-requirement-surveillance-practices.

[22] Katz v. United States, 389 U.S. 347, 355 n.16 (1967); Dalia v. United States, 441 U.S. 238, 248 (1979).

[23] United States v. Donovan 429 U.S. 413, 429 n.19 (1977).

B. *The Evolution of FISA Law from 1978 to Present*

1. *History of FISA*

When the FISA court was created in 1978, it was part of a major restructuring policy that completely changed how the United States conducted electronic surveillance for foreign intelligence.[24] Before FISA, wiretaps were authorized for national security under the President's Article II powers of the Constitution.[25] The original FISA court created a procedure for the Attorney General to obtain warrants that authorized the use of electronic surveillance for the purpose of foreign intelligence.[26]

A FISA warrant differs from a regular warrant in that in a FISA warrant, the government must show probable cause that the target of the surveillance is a "foreign power"[27] or an "agent of a foreign power"[28] and that there is a connection to the location that is being surveilled.[29] FISA was never meant to survive constitutional standards required under criminal law because it was created with the purpose of easing counterintelligence operations on foreign subjects.[30]

---

[24] Privacy and Civil Liberties Oversight Board, *supra* note 7, at 13.

[25] *Id.* (U.S. CONST. art II, § 2, cl. 2. authorizes the President to control foreign relations).

[26] *Id.*

[27] 50 U.S.C. § 1801(a) defines a "foreign power" as:

> a foreign government . . . , a faction of a foreign nation . . . , an entity that is openly acknowledge by a foreign government(s) to be directed and controlled by such foreign government(s), a group engaged in international terrorism or activities in preparation thereof, a foreign-based political organization . . . , an entity that is directed and controlled by a foreign government(s), or an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

[28] 50 U.S.C. § 1801(b) defines an "agent of a foreign power" as:

> any person other than a United States person, who acts in the United States as an officer or employee of a foreign power . . . , acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interest of the United States . . . or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities, engages in international terrorism or activities in preparation therefore, engages in the international proliferation of weapons of mass destruction, or activities in preparation thereof, or engages in the proliferation of weapons of mass destruction, or activities therfor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities therfor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor.

[29] 3 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 11:2–5 (Thomson Reuters, 2019); 50 U.S.C. § 1804(a)(3)(A); & 50 U.S.C. § 1804(a)(3)(B). (A regular warrant must be based on probable cause and particularly describing the person, place, or things to be searched. A warrant must be submitted under oath and by a neutral and detached official.).

[30] KRIS & WILSON, *supra* note 29, § 11.12.

2. *Expansion of FISA Capabilities*

In the aftermath of September 11th, President Bush authorized a program that came to be known as the President's Surveillance Program, which was reauthorized every thirty to forty-five days.[31] This program authorized the NSA to collect bulk metadata on certain international communications.[32] This program was authorized as an emergency response to the September 11th terrorist attacks.[33] In 2004, the government asked the FISA court to expand its purview to include the President's Surveillance Program.[34] The bulk collection of metadata was an authorized government practice under Section 215 of the USA PATRIOT Act. Section 215 authorized the government to collect, "'books, records, papers, documents, and other items' that are 'relevant' to 'an authorized investigation'".[35] However, Section 215 of the USA PATRIOT Act has since ended, following the recommendation of the Privacy and Civil Liberties Oversight Board.[36]

In 2008, Congress passed the FISA Amendments Act ("FAA") which allows the government to conduct electronic surveillance of people believed to be outside of the United States without using the procedures required by FISA Subchapter I.[37] Prior to the passage of the FAA, President Reagan issued Executive Order 12333, which prohibited surveillance of United States persons; however, following the passage of the FAA, Executive Order 12333 continues to allow the incidental collection of metadata from United States persons.[38]

3. *Relevant FISA Statutes*

The meat of FISA Subchapter I comes from section 1802, which outlines the ability of the Attorney General to utilize electronic surveillance without a court order.[39] Section 1802 explains that the Attorney General may use electronic surveillance without a court order for up to one year when the electronic surveillance is solely directed at communications used exclusively among foreign powers and there is no substantial likelihood that any United States person is a party.[40] The exclusion of United States persons is a crucial distinction and part of what allows the FISA court to operate in the manner that it does.

---

[31] Privacy and Civil Liberties Oversight Board, *supra* note 7, at 9.

[32] *Id.*

[33] *Id.* at 37.

[34] *Id.* at 13.

[35] Schwartz, *supra* note 9.

[36] Privacy and Civil Liberties Oversight Board, *supra* note 7, at 168.

[37] United States v. Moalin, 973 F.3d 977, 998 (9th Cir. 2020) (If the government wants to use information that was gathered under the FAA in a criminal prosecution, they have the same notice requirements as under FISA Subchapter I. However, with the Snowden leaks, it came out that the government was using information gathered under the FAA for criminal prosecutions without notice. At this time, the Department of Justice contemplated adding a notice requirement to the FISA Act but decided not to.). *See* Savage, *supra* note 16.

[38] *Moalin*, 973 F.3d at 999; Exec. Ord. No. 12,333; *See* KRIS & WILSON, *supra* note 30, § 17:19.

[39] 50 U.S.C. § 1802.

[40] 50 U.S.C. § 1802(a)(1)(A)(i); 50 U.S.C. § 1802(a)(1)(B).

While the *Moalin*[41] court created a new notice requirement for FISA, there is already an existing notice requirement. Section 1806 states that:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person[42], any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.[43]

This notice requirement, unlike the one applied in *Moalin*[44], is only necessary if there was a warrantless collection of information.[45]

Furthermore, section 1806(e) includes a remedy for aggrieved persons who wish to challenge the entry of information. Under section 1806(e), the defendant has the ability to file a motion to suppress only if, "(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval."[46] The motion also, "shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion."[47] While the motion to suppress is an available remedy, there are strict restrictions that can make its use difficult.

C. *How the Fourth Amendment is Currently Applied in FISA Cases*

United States v. Cavanagh[48] ruled that while the FISA court gets to use a less stringent standard for electronic surveillance, it still needs to comply with the Fourth Amendment.[49] While the *Cavanagh* court did not discuss whether there was a notice requirement under the Fourth Amendment related to FISA, the court did confirm that the FISA warrant is only authorized for foreign intelligence.[50] The *Moalin* court used this confirmation to determine that if the FISA court only has purview over foreign

---

[41] *Moalin*, 973 F.3d at 1001.

[42] 50 U.S.C. § 1801(k) ("An 'aggrieved person' means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance").

[43] 50 U.S.C. § 1806(c).

[44] *Moalin*, 973 F.3d at 977.

[45] Savage, *supra* note 16.

[46] 50 U.S.C. § 1806(e)(1)-(2).

[47] *Id.*

[48] United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987).

[49] *Id.*

[50] *Id.* at 788.

intelligence, then it cannot use the information gleaned from electronic surveillance for criminal prosecution.[51] The court then determined that this leaves the Fourth Amendment notice requirement intact and requires the government to provide notice to criminal defendants when their information has been obtained through electronic surveillance so that the defendant has adequate time to file a motion to suppress.[52]

In *United States v. Mohamud,*[53] the court discussed the notice requirement under the Fourth Amendment with regard to the FISA court's electronic surveillance.[54] In this case, the defendant was notified of the electronic surveillance after the verdict when the government filed a supplemental notice.[55] The government used electronic surveillance to look at Mohamud's emails, which became the basis for the FISA warrant.[56] The defendant argued that the late admission of notice mandated suppression of the evidence.[57] The court found that suppression of the evidence was not warranted in this situation because the defendant was not prejudiced by the late notice as the government never actually used the emails in court.[58] The court refused to evaluate the possible Fourth Amendment violation of the emails without a showing that the defendant suffered an injury as a result of the omission.[59] This case is a clear example of how narrow the notice requirement is interpreted and how difficult it can be to satisfy under the FISA requirements.

III. THE CASE

United States v. Moalin[60] concerns the appeal of four defendants who are members of the Somali diaspora that were convicted of sending $10,900 USD to the foreign terrorist organization ("FTO"), al-Shabaab.[61] Somalia has been in a civil war since 1991 after the military dictator, Siad Barre, was ousted.[62] An interim government was set up in 2004, but faced a great deal of distrust and opposition.[63] To protect themselves against the interim government and the Ethiopians, a number of

[51] United States v. Moalin, 973 F.3d 977, 1000 (9th Cir. 2020).
[52] *Id.*
[53] 843 F. 3d 420, 431 (9th Cir. 2016).
[54] *Id.*
[55] *Id.*
[56] *Id.* at 438.
[57] *Id.* at 436.
[58] United States v. Mohamud, 843 F.3d 420, 437-438 (9th Cir. 2016).
[59] *Id.* at 438 n.21. *See* United States v. Posey, 864 F.2d 1487, 1491 (9th Cir. 1989).
[60] United States v. Moalin, 973 F.3d 977, 1000 (9th Cir.2020).
[61] *Id.* at 984-985.
[62] *Id.* at 985 (In addition to the civil war, there has been widespread famine, drought, and violence where tens of thousands of people have died and hundreds of thousands have been displaced. Around three million Somalis fled, creating the Somali diaspora).
[63] *Moalin*, 973 F.3d at 985.

insurgency groups have emerged, one of which is al-Shabaab.[64] The United States designated al-Shabaab as a FTO in 2008.[65]

At the time of this appeal, defendants Basaaly Saeed Moalin and Issa Doreh were citizens of the United States, defendant Mohamed Mohamed Mohamud had refugee status in the United States, and defendant Ahmed Nasir Taalil Mohamud had a visa.[66] All of the defendants immigrated to the United States a number of years ago from Somalia and lived in Southern California.[67] All of the defendants were charged with conspiracy to provide material support to terrorists,[68] conspiracy to provide material support to a FTO[69], and conspiracy[70] to launder monetary instruments.[71] Defendants Moalin, M. Mohamud and Doreh were charged with added count[72] of providing material support to an FTO.[73] Defendant Moalin received an additional charge[74] of conspiracy to provide material support to terrorists.[75]

The government had obtained a FISA warrant under Subchapter I to have access to Moalin's calls.[76] During the time of surveillance, Moalin was calling a man who went by the name of "Shikhalow," aka "Ayrow," that the government believed was a key leader in al-Shabaab.[77] For over a year, Moalin and the other defendants kept in contact with Shikhalow and sent money through their local hawala[78] to Shikhalow.[79] Defendants argued that Shikhalow was not Ayrow and that the money was going back to Somalia for humanitarian purposes.[80]

---

[64] *Id.* (al-Shabaab is known for using improvised explosive devices and suicide bombings.); *see also* Press Release, Department of State, Amendments to the Terrorist Designations of al-Shabaab (July 19, 2018) (on file with author), https://www.state.gov/amendments-to-the-terrorist-designations-of-al-shabaab/. Pertinent language of the press release states the following:

> Since al-Shabaab's initial 2008 FTO designation, it has killed numerous civilians throughout East Africa. Al Shabaab's attacks included the October 2017 attack in Mogadishu where the group detonated a truck bomb that killed over 500 people, the September 2013 Westgate Mall attack in Kenya that killed more than 70 people, and the July 2010 suicide bombings in Kampala, Uganda that took place during the World Cup and killed 76 people, including one U.S. citizen.

[65] United States v. Moalin, 973 F.3d 977, 985 (9th Cir. 2020).
[66] *Id.* at 985 n. 2.
[67] *Id.* at 985.
[68] 18 U.S.C. § 2339A(a).
[69] 18 U.S.C. § 2339B(a)(1).
[70] 18 U.S.C. § 1956(a)(2)(A) & (h).
[71] United States v. Moalin, 973 F.3d 977, 985-986 (9th Cir. 2020).
[72] 18 U.S.C. § 2339B(a)(1)-(2).
[73] *Moalin*, 973 F.3d at 985-986.
[74] 18 U.S.C. § 2339A(a).
[75] *Moalin*, 973 F.3d at 986.
[76] *Id.*
[77] *Id.*
[78] Schwartz, *supra* note 9 (A "hawala" is an informal network of Islamic money-transfer agents. The hawala that Moalin and the other defendants were going to was called Shidaal Express, where Issa Doreh worked.); United States v. Moalin, 973 F.3d 977, 985-986 (9th Cir. 2020) (The hawala is necessary to send money to Somalia because Somalia has no formal banking system and operates mainly through the use of these hawalas.).
[79] United States v. Moalin, 973 F.3d 977, 986 (9th Cir. 2020).
[80] *Id.* at 987.

Before the trial began, Moalin filed a motion to suppress all electronic surveillance made under FISA and the fruits of that surveillance because Moalin argued that the information obtained under FISA had been obtained illegally, violating the Fourth Amendment.[81] The district court denied the motion, and further denied Moalin's counsel access to the FISA documents.[82] Two days before the trial began, the government introduced an email from a redacted Federal Bureau of Investigation ("FBI") linguist that suggested there were other agencies monitoring Moalin.[83] After the trial had commenced, the defendant learned about the NSA's bulk metadata collection through the Snowden disclosures.[84] Moalin further learned that public officials had used the bulk metadata collection program to open investigations into Moalin personally.[85] The defendants then filed a motion for a new trial, which was denied.[86]

In this appeal, the Ninth Circuit found that the bulk collection of metadata by the NSA exceeded the scope of the authorization Congress granted FISA.[87] The Ninth Circuit also ruled that the government is required to notify the defendant that electronic surveillance occurred and the government intends to use information obtained or derived from it at trial.[88] This case created a new test for the Fourth Amendment notice requirement under the FISA act and will likely change the way FISA cases are heard. However, the Ninth Circuit did not apply this test to Moalin's case, finding that the defendants had not been prejudiced by the lack of notice.[89]

---

[81] *Id.*

[82] *Id.*

[83] *Id.* (The email said: "We just heard from another agency that Ayrow tried to make a call to Basaaly [Moalin] today, but the call didn't go through. If you see anything today, can you give us a shout? We're extremely interested in getting real-time info (location/new #'s) on Ayrow.").

[84] United States v. Moalin, 973 F.3d 977, 987 (9th Cir. 2020) (The government's disclosure of the bulk metadata used Moalin as an example that bulk collection helped stop terrorist attacks); Schwartz, *supra* note 9.

[85] *Moalin,* 973 F.3d at 987 ("These statements reported that the FBI had previously closed an investigation focused on Moalin without bringing charges, then reopened that investigation based on information obtained from the metadata program."); Schwartz, *supra* note 9 ("The government has not shown any instance besides Moalin's in which the law's metadata provision has directly led to a conviction in a terrorism case.").

[86] *Moalin*, 973 F.3d at 988.

[87] *Id.* at 996.

[88] *Id.* at 1001.

[89] *Id.*

IV. ANALYSIS

A. *New Notice Requirement Under United States v. Moalin*

1. *How the New Notice Requirement Arose*

On its surface, the new notice requirement in *United States v. Moalin*[90] can be difficult to distinguish from that already existing in FISA subchapter I.[91] FISA subchapter I requires that the government shall notify the aggrieved party and the district court prior to the start of trial of any information that it intends to use in court and disclose any information obtained or derived from electronic surveillance conducted under FISA authorization.[92]

In this case, the government failed to notify defendant Moalin that it had collected his metadata through the NSA's bulk metadata collection program.[93] However, when the government submitted a redacted email from the FBI to the defendants two days before the commencement of trial, it became clear that the FISA authorized surveillance was being used by other agencies for other purposes.[94] This is an issue because depending on the type of electronic surveillance, when it occurred, and how it was authorized, it is possible that the FBI surveillance was used as evidence in the original FISA wiretap applications.[95] The use of electronic surveillance obtained under a FISA warrant as evidence in domestic criminal proceedings represents a huge problem for agencies who perform both foreign intelligence surveillance and participate primarily in domestic law enforcement, where there is supposed to be a sort of 'Chinese wall'[96] between the two.[97]

This issue was further exposed by the Snowden disclosures. Edward Snowden explained that the government was collecting bulk metadata through FISA authorization and then turning around and using that same metadata in criminal prosecutions without notifying the defendants of the surveillance.[98] This alerted the defendants in this case that their metadata was likely being used for additional surveillance, which is when they went to the Ninth Circuit to request the additional surveillance that was not available during their first trial.[99] The defendants argued

---

[90] 973 F.3d 977, 1001 (9th Cir. 2020).

[91] 50 U.S.C. § 1806(c).

[92] *Id. See also* United States v. Moalin, 973 F.3d 977, 998 (9th Cir. 2020) ("[T]he government notified them and the district court that it intended to 'use or disclose' in 'proceedings in this case information obtained or derived from electronic surveillance conducted pursuant to the authority of [FISA].'") (citing 50 U.S.C. § 1806(c)).

[93] *Moalin*, 973 F.3d at 998.

[94] *Id.* at 987.

[95] *Id.*

[96] *Ethical Wall*, BLACK'S LAW DICTIONARY (11th ed. 2019) (A Chinese Wall, also called an Ethical Wall is, "a screening mechanism maintained by an organization . . . to protect client confidences from improper disclosure to lawyers or staff who are not involved in a particular representation.").

[97] *See* Schwartz, *supra* note 9.

[98] *Moalin*, 973 F.3d at 998 (9th Cir. 2020). *See* Privacy and Civil Liberties Oversight Board, *supra* note 7, at 1.

[99] *Moalin*, 973 F.3d at 998.

that they had a Fourth Amendment[100] right to be notified of the additional surveillance, other than the surveillance authorized under FISA subchapter I because notice is a critical part of the Fourth Amendment.[101]

The defendant's Fourth Amendment argument seems like the logical approach to this situation because in any other criminal prosecution, the government would be required to give the defendant notice if a search had occurred.[102] However, in one of the only other instances where the Ninth Circuit decided a Fourth Amendment case involving FISA, the Ninth Circuit held that while the Fourth Amendment is not directly applied, "a [d]ifferent standard[] [of probable cause] may be compatible with the Fourth Amendment if [it is] reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[103]

2. *The New Notice Requirement*

The Ninth Circuit agreed with the defendants in part, stating that, "the government is required only to inform the defendant that the surveillance occurred and that the government intends to use information obtained or *derived* from it."[104] This creates a whole new area of notice where the government will now be required not only to give notice of information gathered by the FISA authorized warrant that they wish to use in court, but also any other information derived from the original surveillance that they plan to use as well.[105]

Traditionally under the Fourth Amendment, if the government fails to notify the defendant that a search has occurred, the defendant would be able to file a motion to suppress in order to keep the unlawfully gathered evidence out of trial.[106] However, under FISA, a motion to suppress the evidence of electronic surveillance is only available if the evidence was "unlawfully acquired" or the evidence was not "in conformity with the authorization or approval."[107] This section is essentially useless

---

[100] U.S. CONST. amend. IV. The Fourth Amendments states the following:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[101] *Moalin*, 973 F.3d at 1000.

[102] Berger v. State of N.Y., 388 U.S. 41, 60 (1967); *Moalin*, 973 F.3d at 999; Katz v. United States, 389 U.S. 347, 355 (1967).

[103] United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 2020).

[104] *Moalin*, 973 F.3d at 1001 (emphasis added).

[105] *Id.*; *see* Kerr, *supra* note 21. In opinion about the notice rule, Kerr states:

> This notice rule seems pretty different. This is a notice rule that is all about making the exclusionary rule meaningful. You don't get notice unless you are criminally charged, and the notice you get is designed to alert you that you might have a plausible motion to suppress that you should look into and consider filing.

[106] *Moalin*, 973 F.3d at 1000. *See Berger*, 388 U.S. at 52-53.

[107] 50 U.S.C. § 1806(e)(1)-(2). The pertinent language of the statutory provision states:

because often times, there is virtually no way for a defendant or defendant's attorney to gain access to the original FISA court issued warrant to ascertain whether it was unlawfully acquired or made in conformity with the warrant's authorization.[108] Furthermore, prior to the new notice requirement from *United States v. Moalin*[109], the FISA court and the government read the "derived from"[110] requirement narrowly.[111] The Ninth Circuit in *Moalin* essentially widened this interpretation, making it a requirement that the government notify defendants even when the information they are using in court is merely derived from information authorized under a FISA warrant.[112]

After the government has given the defendant notice that the surveillance and any information derived from it will be used in court, the Ninth Circuit allows the defendant to file a motion challenging the evidence and its admission into court.[113] However, there is no telling how this new notice requirement will work in reality, as the Ninth Circuit refused to apply the test to *Moalin's* case, finding that the lack of notice did not prejudice the defendants.[114]

> Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial . . . in or before any court . . . may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval. Such a motion shall be made before the trial . . . unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

[108] Savage, *supra* note 16. Savage explains the what limited information regarding surveillance evidence prosecutors are required to provide:

> In national security cases involving orders issued under the Foreign Intelligence Surveillance Act of 1978, or FISA, prosecutors alert defendants only that some evidence derives from a FISA wiretap, but not the details like whether there had just been one order or a chain of several. Only the judges see those details.

[109] 973 F.3d 977 (9th Cir. 2020).

[110] 50 U.S.C. § 1806(d).

[111] Savage, *supra* note 16. Savage discusses an instance of where the narrow interpretation of the "derived from" language was invoked:

> The national security lawyers explained that [the failure to notify defendants that the evidence in their case stemmed from wiretap conversation without a warrant] was a misunderstanding, the officials said. Because the rules on wiretapping warrants in foreign intelligence cases are different from the rules in ordinary criminal investigations, they said, the division has long used a narrow understanding of what 'derived from' means in terms of when it must disclose specifics to defendants.

[112] United States v. Moalin, 973 F.3d 977, 1001 (9th Cir. 2020).

[113] *Id.*

[114] *Id.*

B. *The Impact of the New Notice Requirement on Future Cases*

1. *Will the Decision Be Accepted?*

While the Ninth Circuit refused to apply their own test in *United States v. Moalin*,[115] it is unclear how the Ninth Circuit, or other courts for that matter, will apply this new notice requirement in future cases, if they choose to use apply it at all. Of the appellate circuits, the Ninth Circuit is known for putting out controversial opinions that often times get reversed or vacated by the Supreme Court.[116]

2. *Moalin Follows the Current Trend of Privacy Concerns with FISA*

Regardless of the fact that this case came out of the Ninth Circuit, it is sure to have a lasting impact on Fourth Amendment jurisprudence as it follows the general feeling of a nation nineteen years following September 11th. Following the Snowden disclosures, the Privacy and Civil Liberties Oversight Board recommended that the practice of bulk collection of metadata should be terminated[117] and the government should implement heightened privacy protocols to reduce the effects of the bulk collection of metadata collection.[118]

---

[115] *Id.*

[116] Linda Que, *Does the Ninth Circuit Have the Highest Reversal Rate in the Country?*, N.Y. Times (Nov. 26, 2018), https://www.nytimes.com/2018/11/26/us/politics/fact-check-trump-ninth-circuit.html. The author discusses the reversal and vacating rate of Ninth Circuit decisions that are appealed to the Supreme Court:

> From 2006 to 2015, the Supreme Court heard 160 cases from the Ninth Circuit, reversing 106 decisions and vacating 24 . . . [t]hat is a reversal or vacating rate of about 81 percent, which is higher than the average reversal rate of nearly 73 percent . . . . In the 2016 term, the Ninth Circuit's rate was nearly 88 percent, still behind the 100 percent reversal or vacating rates of four other circuit courts.

[117] Privacy and Civil Liberties Oversight Board, *supra* note 7, at 16-17. The Privacy and Civil Liberties Oversight Board argued the following about the veracity of Section 215:

> The Section 215 bulk telephone records program lacks a viable legal foundation under Section 215, implicates constitutional concerns under the First and Fourth Amendments, raises serious threated to privacy and civil liberties as a policy matter, and has shown only limited value. As a result, the Board recommends that the government end the program.

[118] *Id.* at 17. The Privacy and Civil Liberties Oversight Board report further states that:

> The recommend[ed] changes can be implemented without any need for congressional or FISC authorization. Specifically the government should: (a) reduce the retention period for the bulk telephone records program from five to three years; (b) reduce the number of "hops" used in contact chaining from three to two; (c) submit the NSA's 'reasonable articulable suspicion' determinations to the FISC for review after they have been approved by NSA and used to query the database; and (d) require a 'reasonable articulable suspicion' determination before analysts may

Furthermore, the Attorney General and the FBI have been advocating for reforms to the FISA court.[119] While the reforms will be focused on the FBI's investigation of elected officials, Attorney General Barr said that,

> FISA is a critical tool to ensuring the safety and security of Americans, particularly when it comes to fighting terrorism. However, the American people must have confidence that the United States Government will exercise its surveillance authorities in a manner that protects the civil liberties of Americans, . . . and complies with the Constitution and law of the United States.[120]

In the many years following September 11th, Americans are looking to regain some of the privacy rights they gave up in order to fight terrorism.[121] The Ninth Circuit's decision in *United States v. Moalin* is a huge step for privacy reform in the realm of national security, not only for the addition of the notice requirement, but also for holding that the bulk metadata collection program exceeded the scope of FISA.[122]

> submit queries to, or otherwise analyze, the 'corporate store,' which contains the results of contact chaining queries to the full 'collection store.

[119] Press Release, Department of Justice, The Department of Justice and the Federal Bureau of Investigation Announce Critical Reforms to Enhance Compliance, Oversight, and Accountability at the FBI (Sept. 1, 2020) (On file with author), https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance. FBI Director Christopher Wray explained:

> That's why I immediately ordered more than 40 corrective actions, including foundational FISA reforms, many of which went beyond those recommended by the Inspector General. The FBI has been working diligently to implement these corrective actions. The additional reforms announced today, which we worked on closely with the Attorney General's office, will build on the FBI's efforts to bolster its compliance program. FISA is an indispensable tool that the FBI uses to protect our country from national security threats, and Americans can rest assured that the FBI remains dedicated to continuously strengthening our FISA compliance efforts and ensuring that our FISA authorities are exercised in a responsible manner.

[120] *Id.*

[121] Shiva Manium, *Americans Feel the Tensions Between Privacy and Security Concerns*, PEW RESEARCH CENTER (Feb. 19, 2016), https://www.pewresearch.org/fact-tank/2016/02/19/americans-feel-the-tensions-between-privacy-and-security-concerns/ ("In an early 2015 online survey, 52% of Americans described themselves as 'very concerned' or 'somewhat concerned' about government surveillance of American's data and electronic communications, compared with 46% who described themselves as 'not very concerned' or 'not at all concerned' about the surveillance."); *see also Public Opinion on Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/survey/ (last updated May 2020).

[122] United States v. Moalin, 973 F.3d 977, 996 (9th Cir. 2020).

3. *Issues with the Ninth Circuit's Interpretation of Moalin*

There are a few issues with the Ninth Circuit's interpretation of *Moalin* that could cause the decision to be interpreted in a way that the new notice requirement is less restrictive than mentioned above. The first being the actual access the defendants and the defendant's attorneys will have to surveillance evidence. Even if the government gives the defendant some sort of notice, the defendant will not necessarily get direct access to the information that the government possesses.[123] The government is able to keep this information from the defendants because of our country's concern for national security, especially with regard for foreign intelligence.[124] If the government believes the information to have national security implications, it can present the information to the court through an *ex parte* or *in camera* hearing, excluding the defendants.[125]

The second issue is that the government is only required to notify the defendant of the surveillance if they plan to use the surveillance or any other information derived from it.[126] This was part of the problem in *United States v. Mohamud,*[127] where the defendant argued that he had a Fourth Amendment right to view the emails the government alleged were part of his contact with a foreign national.[128] The issue that the defendant encountered in this case is that the emails were only used to get the FISA warrant in the first place and were never introduced at trial; thus, the government was not required to notify the defendant of its use of them.[129] The worry is that the government will continue to read their obligations narrowly until the Supreme Court or a number of other circuits come to the same conclusion that the Ninth Circuit did.

The third issue with this opinion is that the new notice requirement only applies to notice, not disclosure.[130] This is a problem because there will not necessarily be a difference in outcome if the defendant is notified that the surveillance occurred, but is never given full access to that information. While the new notice requirement allows for defendants to get more access to information surrounding their case, the Ninth Circuit's inability to extend notice to disclosure leaves a valuable gap in information which leaves the established power imbalance in place.[131] There will always be an imbalance in power in favor of the government in national security cases, but the new notice requirement established by *Moalin* provides defendants some evidentiary tools to help tip the scales.

Despite these issues, the *Moalin* opinion is sure to change the way defendants interact with the FISA courts. This opinion has even more weight as it is championed

---

[123] *Id.* at 1001.

[124] *Id.*

[125] *Id.* ("*See, e.g.*, 50 U.S.C. § 1806(f), allowing in camera, ex parte review of the legality of electronic surveillance under FISA Subchapter I if 'the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.'").

[126] *Id.*

[127] 843 F.3d 420, 438 (9th Cir. 2016).

[128] *Id.*

[129] *Id.* (This case is similar to Moalin in many ways. The defendant was also born in Somalia and living in Southern California. The Ninth Circuit decided this case in 2016, just four years before the same circuit decided Moalin.).

[130] United States v. Moalin, 973 F.3d 977, 1001 (9th Cir. 2020).

[131] *Id.*

as the only instance where bulk metadata collection was able to catch a terrorist.[132] While the practice of collecting bulk metadata has been heavily scrutinized, it is important for the United States Government to make it seem like it was a worthwhile program at the time of its use. *Moalin* exposes how the FISA courts and the NSA have exploited defendants with any connection to foreign nationals whose actions can be interpreted in any way as suspicious.

V. CONCLUSION

Nineteen years following the September 11th terrorist attacks, Americans are looking to regain some of the privacy rights they exchanged for protection from foreign adversaries. While the new notice requirement derived from *United States v. Moalin*[133] removes one brick from the wall the United States Government built against foreign threats, it returns Fourth Amendment notice protections to those facing criminal prosecution in the United States.[134]

The Ninth Circuit in *United States v. Moalin* determined that the United States Government must provide notice to defendants in criminal prosecutions when the government intends to introduce evidence obtained or derived from electronic surveillance authorized by the FISA Court.[135] This new notice requirement goes even further to add that once the defendant is notified, they are able to file a motion to challenge the legality of the introduction of the electronic surveillance.[136]

This new notice requirement is a step in the right direction for defendants in criminal prosecutions who have been electronically surveilled through a FISA authorized warrant. However, there is great uncertainty in how this rule will be applied, as it was not applied in *Moalin,*[137] or even if it will be applied at all.[138] There is hope that this decision will be followed by other circuits because it reflects Americans' desire to move away from electronic surveillance, particularly the bulk collection of telephony metadata.[139]

The biggest obstacle affecting the utility of the new notice requirement is the importance of protecting the ever expanding definition of national security and its

---

[132] Schwartz, *supra* note 9.

[133] 973 F.3d 977, 1001 (9th Cir. 2020).

[134] *Id.*

[135] *Id.*

[136] *Id.*

[137] *Id.* at 1001. The court stated:

> Based on our careful review of the classified record, we are satisfied that any lack of notice, assuming such notice was required, did not prejudice the defendants. Our review confirms that on the particular facts of this case, information as to whether surveillance other than the metadata collection occurred would not have enabled defendants to assert a successful Fourth Amendment claim. We therefore decline to decide whether additional notice was required.

The Ninth Circuit refused to apply its own test or even walk through the analysis of why it chose not to so this leaves the new notice requirement open to interpretation for other courts.

[138] *See* Que, *supra* note 116.

[139] *See* Privacy and Civil Liberties Oversight Board, *supra* note 7 at 16-17.

information, methods, and sources. The emphasis on national security in the United States makes the information in the FISA court almost impossible to reach. This new notice requirement will be a crucial step in the national conversation regarding the contention between privacy, national security, and the Fourth Amendment. Other circuits should adopt the test set forth in *United States v. Moalin* and work to restore the rights guaranteed under the Fourth Amendment.