NO. 14-30217

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

MOHAMED OSMAN MOHAMUD,

DEFENDANT-APPELLANT.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON
THE HONORABLE GARR M. KING, SENIOR U.S. DISTRICT JUDGE
USDC NO. 3:10-CR-00475-KI

ANSWERING BRIEF OF PLAINTIFF-APPELLEE

BILLY J. WILLIAMS
ACTING UNITED STATES ATTORNEY
DISTRICT OF OREGON
KELLY A. ZUSMAN
APPELLATE CHIEF
ETHAN D. KNIGHT
PAMALA R. HOLSINGER
RYAN W. BOUNDS
ASSISTANT UNITED STATES ATTORNEYS
1000 SW THIRD AVENUE, SUITE 600
PORTLAND, OREGON 97204-2902
TELEPHONE: (503) 727-1000

JOHN P. CARLIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
JOSEPH F. PALMER
ATTORNEY, APPELLATE UNIT
NATIONAL SECURITY DIVISION
U.S. DEPARTMENT OF JUSTICE
950 PENNSYLVANIA AVE, NW,
ROOM 6500
WASHINGTON, DC 20530
TELEPHONE: (202) 353-9402

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES
Federal Cases

TABLE OF AUTHORITES

Federal Cases

Federal Statutes, Laws & Rules

TABLE OF AUTHORITES
Federal Statutes, Laws & Rules

TABLE OF AUTHORITES
Dockets/Docketed Cases

Legislative Material

TABLE OF AUTHORITES
Other Material

STATEMENT OF JURISDICTION

The district court had subject matter jurisdiction pursuant to 18 U.S.C. § 3231. Defendant filed a timely notice of appeal (ER 236),[1] and therefore, this Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF ISSUES PRESENTED

1. A jury found defendant guilty of attempting to detonate a weapon of mass destruction; did the district court err in rejecting defendant's theory that he was entrapped as a matter of law?
2. In closing, the prosecutor argued that flattery and invocations of Allah were unlikely to induce an otherwise innocent person into committing this offense. Did the district court abuse its discretion when it refused to strike the argument or issue a curative instruction?
3. Did the district court abuse its discretion when it refused to modify a Ninth Circuit Model Jury Instruction on entrapment, when it declined to give an instruction on the First Amendment, and when it responded to a jury question about predisposition?
4. Did the district court clearly err when it found that nothing in the government's case was affected by an unrelated state investigation, so there was no need to decide if that investigation violated the Fourth Amendment?

---

[1] "ER" refers to defendant's Excerpts of Record; "GSER" refers to the government's Sealed Supplemental Excerpts of Record; "PSR" refers to the Presentence Report; "D. Br." refers to Defendant's Opening Brief; and "ACLU Br." refers to the ACLU's amicus brief. The lodged disks include all of the government's trial exhibits, including the surveillance audio and videotapes.

5. Did the district court abuse its discretion by admitting evidence of the investigators' state of mind to avoid leaving the jury with the false impression that the government "pounced" on defendant because of his religious beliefs?

6. Did the district court appropriately address Foreign Intelligent Surveillance Act (FISA) and Classified Information Procedures Act (CIPA) disclosures, and did it correctly reject defendant's constitutional challenges to the FISA Amendments Act (FAA)?

7. Did the district court err or abuse its discretion when it selected defendant's 30 year sentence?

CUSTODY STATUS

Defendant is in federal custody. His projected release date is January 26, 2037.

STATEMENT OF FACTS

A. Nature and Overview of the Proceedings

Defendant predicted a "dark day" for the United States. (Ex. 166). His plan? To detonate a bomb in Pioneer Square in downtown Portland, Oregon just as 25,000 people gathered to witness the annual tree lighting the day after Thanksgiving in 2010. After parking a van filled with fake explosives near the square, defendant dialed a phone number into a cell phone that he believed would detonate the bomb. He dialed the number—twice—and was promptly arrested by the FBI. Defendant had been preparing for this day for some time.

Defendant was born in Somalia in 1991, and he emigrated to the United States with his parents at age 3. (ER 5815–17; PSR ¶ 4). He was a college student studying

engineering at Oregon State University from September 2009 until a few months before his arrest in November of 2010. (PSR ¶ 44). At school he was described as "self-motivated," possessing a "high intellect and maturity," and someone who showed "initiative and personal drive." (ER 6086). While his life as a college student appeared typical—he had many friends, partied, smoked marijuana—he also wrote articles under various pseudonyms supporting jihad, joined encrypted pro-jihadi websites, and set up multiple email accounts to maintain an online persona as a violent Islamic jihad supporter. (ER 5862, 5960–61, 6089; PSR ¶¶ 11–15, 45, 65–68).

Just prior to starting college, defendant announced to his parents that he was leaving the country. (ER 5829; PSR ¶ 33). Fearing that his son might try to return to Somalia where his life would be in danger, defendant's father (Osman Barre) contacted the FBI. (ER 5831; PSR ¶¶ 35, 37). Barre described his son as "very sharp," but "easy to influence"; solo foreign travel was a concern because he felt that his son was "too young and immature." (ER 5829, 5853–54).

Barre later told the FBI that he had learned that his son intended to travel to Yemen to learn Arabic and study Islam. (ER 5118; PSR ¶ 41). He described his son as a "child," and said he wanted the FBI to help prevent his son from traveling. (ER 5118, 5156, 5831). A few days later, Barre called the FBI back and said that defendant had no ticket or visa to travel to Yemen, and that he had convinced defendant to stay in the United States and attend college. (ER 5120; PSR ¶ 41).

Barre forwarded to the FBI an email from defendant that described the school in Yemen; defendant's email address led the FBI to discover that defendant authored several articles in *Jihad Recollections*, an online, English language jihadi magazine edited by Samir Khan. (ER 5121–22, 5837; PSR ¶ 43). The concerns Barre raised, defendant's connections to Samir Khan, and defendant's email correspondence with Amro Al-Ali (a Saudi Arabian suspected of terrorist ties), ultimately triggered this investigation.[2]

None of these facts are in dispute, and because most of the events leading up to the day of the attempted attack on Pioneer Square were recorded or videotaped, most of the other relevant facts are uncontested. The key issue at trial was whether defendant was entrapped. Throughout this litigation, the district court took great pains to address classified materials, discovery and evidentiary issues, and challenges to the jury instructions; it conducted the trial in a manner that was fair.

At the conclusion of a 13-day trial, a jury found defendant guilty of the single charge of attempting to detonate a weapon of mass destruction in violation of 18 U.S.C. § 2332a(a)(2)(A). (PSR ¶ 1). The guideline range for this offense is life, but at the urging of both parties, the district court varied from that range. It ultimately

[2] When Barre contacted the FBI in August of 2009, FBI Agent DeLong thought at that time that defendant's connections to known terrorists might make him a valuable informant. (ER 5127). DeLong ultimately rejected the idea as too risky, because if it failed, it could compromise other active investigations. (ER 5128).

imposed a 30-year sentence. (PSR ¶ 231; ER 229–30). Defendant also appeals from that sentence in both his sealed and unsealed submissions.

B. Defendant's Correspondence with Samir Khan, the *Jihad Recollections* Editor.

Samir Khan was a United States citizen originally from Pakistan and the former publisher of *Jihad Recollections*, the first English language magazine aimed at Al Qaeda supporters. (ER 4047–48, 4133–34, 5705; Ex. 232). This online magazine featured stories about global jihad, and it included sound bites from Osama bin Laden and pro-jihadi embedded videos. (ER 5314–15; Ex. 232). It described America as a "bully" that "must be hurt." (ER 5323–27). Khan left the United States sometime in late 2009, and he was killed during a drone strike in Yemen in September of 2011. (ER 4048, 4133–34, 5143).

Between February and August of 2009, defendant and Khan exchanged 151 emails. (ER 5258; Ex. 223).[3] Defendant, using the screen name "man with disheveled hair," and the email address, "truthbespoken@googlemail.com," sought advice from Khan and told Khan he wanted to write for *Jihad Recollections*. (ER 5265). He explained that he was "the best writer in my state." (Ex. 223-5). When Khan

[3] Evan Kohlmann, an international terrorism expert who testified at trial described Khan as the "most well-known homegrown extremist still living in the United States." (ER 5721). Kohlmann was not aware of anyone, aside from defendant, who had corresponded with Khan this extensively.

asked where he lived, defendant refused to answer, explaining that it would "jeopardize a lot of ppl" to disclose that information. (Ex. 223-7). Defendant nevertheless filled out a questionnaire for Khan. (ER 5266; Ex. 223-23).

Within the questionnaire, defendant identified a list of "scholars that you take knowledge from." (Ex. 223-23). Included within defendant's list were a number of radical Islamic extremists who "directly called upon Muslims, young Muslims, living in the West to abandon American society and either travel abroad to join a jihadi organization or to carry out acts of violence aimed at disbelievers or enemies of Islam wherever they were found." (ER 5730).[4]

In February 2009, defendant posted a comment about his perception of the Muslim view of Valentine's Day. (Ex. 223-25). According to defendant, "it is not permissible for a Muslim to celebrate any of the festivals of the kuffar [infidels]." (*Id.*). He further explained that festivals are important, "prominent symbols of the kuffar," so joining in them could "lead to complete kufr." (*Id.*).

One week later, defendant submitted his first article to Khan titled "Getting in Shape Without Weights." (Ex. 223-38). The article urged readers to exercise in order to prepare for "jihad." Comparing the draft version (Ex. 223-38) to the final version

[4] Anwar Al-Awlaki, Abdullah Azzam, Shaykh Omar Abdel Rahman, Shaykh Hammoud bin Uqla Ash-Shuaybi were among those included on defendant's list and identified by international terrorism expert Evan Kohlmann as individuals promoting violent jihadist activities. (ER 5703, 5727–33).

(Ex. 232-3, Bates #3820-3824) reveals that Khan removed the following, wherein defendant described how mujahideen demonstrated the value of speed: "An example for you is 9/11 when our brothers hit them so fast the Americans became dumbfounded. The Mumbai attacks were also a great display of quickly entering the arena of battle and just decimating the kuffar."

Khan also removed references in defendant's concluding paragraph about "preparing to meet Allah as a martyr." (ER 5268–69). And Khan refused to publish a photograph defendant submitted of the 9/11 attacks (Ex. 223-43, Bates #8166), explaining that he "did not want to give the impression that we're telling people to train for something in particular." (ER 5270–71; Ex. 223-45). Following its publication, defendant reviewed the entire first issue and shared his critiques with Khan. (ER 5275; Ex. 223-72).

In April, defendant sent Khan another article entitled "Preparing for the Long Night," which gave advice about how to mentally prepare for the hardships of "guarding the frontlines." (Ex. 223-74; 232). In this article, defendant described "ribaat" or guarding the Muslim homelands, and he discussed the mental and physical preparation needed to carry out this task. (*Id.*). As with defendant's first submission, Khan also edited this one, removing a sentence that praised the mujahideen in Afghanistan who, in 2001, "would attack landing Chinook helicopters and would retreat from air strikes in the caves only to return and finish off the wounded

American soldiers." (Ex. 223-74). And defendant again critiqued the entire issue after it was published. (ER 5279; Ex. 223-100).

In June, defendant submitted a third article praising As-Sahab Media as an outlet for Osama bin Laden. (Ex. 223-106; ER 5281). Defendant also sent a fourth article titled, "Raison d'Etre for Europe's Potential of Jihadi Assault." (Ex. 223-108). He opined that Europe posed a much easier target for jihad, and he argued that Europe "owes the Muslim Ummah equal to or more than the United States in terms of crimes they have committed, blood they have spilt and so on." (*Id.*).

The fourth issue of *Jihad Recollections* was to be dedicated to 9/11, and while defendant initially signed on to contribute an article, he withdrew in August because he was "going through a lot of things and I have a lot of things to do." (ER 5285–86; Ex. 223-145, 223-150).[5]

Khan left the United States sometime after the fourth issue of *Jihad Recollections*, but he restarted the magazine under a new title, *Inspire*, after joining Al Qaeda in the Arabian Peninsula. (ER 5705; Ex. 239-9). *Inspire* featured the "Global Jihadi movement," and served as a forum for fighters who saw the conflict in Afghanistan against the Russians as a good start. (ER 5706–09). *Inspire* was the first English language magazine aimed at recruiting individuals from the West to Al Qaeda. (ER

[5] August of 2009 was when defendant planned to travel to Yemen via Alaska. (ER 5286–87; Ex. 90).

5723). Khan's contribution to the inaugural issue of *Inspire* was entitled, "I'm Proud to be a Traitor to America." (Ex. 239-9).

Defendant drafted an article for *Inspire* as well. (ER 5495; Ex. 63). In this article, defendant counseled youth "unable to immigrate and perform jihad, then it is upon them to not waste their time. Much can be done to hurt the enemy or prepare for jihad. According to your circumstances you could perform jihad against the enemy where you are currently living by Mumbai-style attacks, but my article is directed towards those brothers waiting to travel to the lands of jihad rather than touch upon the issue of attacks within the Western nations." (*Id.*).[6] Defendant urged youth to "memorize" the Quran, but cautioned that prayers were not enough. (*Id.*).

C. Defendant's Correspondence with Amro Al-Ali, a Saudi Fugitive with Suspected Links to Terrorism.

Al-Ali was a Saudi Arabian citizen who traveled to the United States on a student visa in 2007. (ER 4119). He attended Portland State University in the Spring of 2008, and left the United States on June 29, 2008. (*Id.*). By 2011, Al-Ali was one of the top 47 wanted terrorists according to Saudi Arabian officials; he was known for

[6] The first issue of *Inspire* is dated "Fall 2010." (Ex. 239-9). Defendant's draft article is undated and it did not appear in *Inspire's* first issue; defendant emailed a copy to Youssef, an undercover FBI agent, along with copies of the four articles he wrote for *Jihad Recollections*. (Ex. 63).

having received explosives training and for recruiting Americans and other Westerners to join Al Qaeda. (ER 5717).

In the fall of 2009, Al-Ali and defendant exchanged a series of emails. (Ex. 224). Al-Ali was writing from Yemen and Pakistan, while defendant was living at home in Beaverton, Oregon. (ER 4031–32, 5288–91; Ex. 224). In 2009, Al-Ali was wanted by the Saudi government for suspected links to terrorism; the Saudis believed that Al-Ali was attempting to connect with an explosives expert. (ER 4026; Ex. 80).[7] The FBI considered Al-Ali a "dangerous person overseas," so his communication with defendant was concerning. (ER 4025–27, 5287).

In September, Al-Ali sent defendant information about a school in Yemen. (ER 4032, 5287). This school was founded by an "avid" jihadi supporter, and it served as a "steppingstone" to violent jihad, particularly for people from the West. (ER 5712). Al-Ali told defendant that if he "wants to come, there's a brother that will contact you about the proper paperwork you need to come. I can't go online for a while. I hope to see you soon." (ER 4033–34; Ex. 224-12). On December 12, 2009, Al-Ali instructed defendant to use an email drop-box to contact Abdul Hadi, someone

[7] Saudi Arabia's 2009 Red Notice (an international arrest warrant alert) (Ex. 80) summarized the following about Al-Ali: "On 13 October 2009, AL ALI was known to be connected to a fugitive wanted by Saudi Arabian authorities who is an expert in manufacturing explosives and who plays a coordinating role in facilitating the movement of extremists inside Saudi Arabia. He also helped AL Qaeda division in Yemen and other countries by providing them with foreign fighters to carry out terrorist attacks against western and tourist interests."

the FBI suspected was an Al Qaeda recruiter. (ER 4038–49; Ex. 224-15). Defendant immediately sent the email as instructed: "How are you brother Abdul Hadi? I was referred to you by a friend. Please get back to me as soon as possible." (ER 4040; Ex. 225-21). But defendant's message bounced. (ER 4041). Defendant made several attempts to contact Abdul Hadi, but none were successful. (ER 4042–43, 5295–98).

Several months later, on May 20, 2010, defendant sent a cryptic email blind-copied to paleroze@hotmail.com: "The products were wonderful. I received them in good time and in great condition. I was wondering if you were an associate of brother Amr [Al-]Ali who also sell electronics." (ER 4043–44, 4079; Ex. 225-51). Because Al-Ali did not sell electronics, and because this appeared to be a further attempt by defendant to reach Abdul Hadi, this email "was a grave concern" to the FBI. (ER 4044–45).

D. Defendant's Other Online Activities

While he was corresponding with Al-Ali and writing articles for Khan, defendant also registered for and posted comments and questions on six forums dedicated to Islamic extremism. (ER 5347, 5783–96; Ex. 225-76). He claimed in one of these forums to have read books about ammonium nitrate, and he expressed anger over his treatment in Customs when he traveled to London with his family in December 2008. (ER 5361, 5374–77). He also accessed an encrypted Al Qaeda video entitled "Repelling the Aggression." (ER 5767–68).

Other text messages and emails revealed that defendant was enjoying "typical" college life throughout this time period as well; he was using marijuana, drinking, and attending parties. (ER 5403–40). There was no evidence that he sought to purchase any explosives. (ER 5455).

E. Defendant's Arrest on Unrelated State Charges

In November 2009 defendant was the subject of a rape investigation. (ER 70, 75). He agreed to meet with local officers, and he was fully exonerated. The FBI was notified about this investigation, and FBI agents observed the local interview and polygraph test. (ER 75–76). The FBI also imaged and forensically analyzed defendant's computer, but federal investigators learned nothing that they did not already know based upon the FBI's earlier investigation. (ER 76–78).

F. The FBI Tested the Waters

Defendant's contacts with Al-Ali, his Internet postings, his correspondence with Samir Khan, and his writings for *Jihad Recollections* raised sufficient concerns within the FBI that it decided to contact defendant online through a paid undercover source who used the name "Bill Smith." (ER 4025, 4047, 4051–55, 4093). Smith and defendant never met in person; over the course of six months (between November 9, 2009, and May 13, 2010), they exchanged 43 emails. (Ex. 226).

With Smith, the FBI attempted to create a "like-minded individual" who might form a friendship with defendant. (ER 5179–81). Smith reached out in response to

one of defendant's Google group posts; Smith claimed that he lived in the West, he was "one of the only Muslims around," and he "wanted to get more involved in the fight for The Ummah. I want to help rid the occupiers from palestine [sic]." (Ex. 226-1).[8] The Arabic term "ummah" refers to the Islamic nation or community.

Smith's question was "purposefully vague," to try to discern how defendant might interpret it. (ER 5186; Ex. 226-2). Smith also referred to the "struggle" in the West to gauge defendant's reaction. (ER 5189, 5192). Defendant responded with advice later that same day: he urged Smith to move to a "more populated Muslim area" like Seattle, but he cautioned him against putting himself "out there" because "there are a lot of spies." (Ex. 226-4).

Smith continued to ask defendant for advice about what he (Smith)—as a Muslim isolated from the Muslim community—might do to "join with others who have the same desire. If we can get the west preoccupied with problems, and struggles here, then they will be less involved in Palestine." (Ex. 226-5). Defendant gave Smith advice, but he kept his distance. (Ex. 226-6, 226-7, 226-8, 226-11).

Smith expressed his own desire to "bring the fight here to the west," and he asked defendant for advice. (Ex. 226-12). The supervising FBI agent explained that

---

[8] Another FBI Agent (Elvis Chan) also attempted to reach out to defendant using an online undercover agent, unaware that Agent Dodson was using Bill Smith as an undercover source. (ER 5009). Chan directed two emails to defendant sometime in November of 2009, but defendant never responded to either of them. (*Id.*).

he used the word "fight" because it appeared in defendant's articles for *Jihad Recollections* and because the word was vague; it could refer to a physical fight or a fight for what you believe depending upon how the recipient interpreted it. (ER 5197–98).

Hearing no response, however, Smith wrote to defendant again a month later (January 1, 2010). Smith mentioned hearing about "some action against the West in the last few weeks," and he wondered "who is getting these guys set up." The FBI agent explained that this was not intended to refer to any specific event. (Ex. 226-13; ER 5199, 5226, 5251). Smith observed "how easy it should be to bring any community here in the west to its knees. I think these guys are making things way too complicated." (Ex. 226-13).

Defendant responded that same day, telling Smith "i don't think you should talk about such issues, especially online." (Ex. 226-14). Defendant later clarified that he did not mean that Smith shouldn't do or say anything, but simply that he should not talk online: "just find some brothers who share your views and talk with them but remember that you have to be cautious, you don't want to get arrested for just talking." (Ex. 226-16). Smith promised to be careful and mentioned that he might be moving to Portland, Oregon. (Ex. 226-17, 226-20). Defendant wished him well, but he neither revealed that he lived in Portland, Oregon, nor did he suggest an in-person meeting. (Ex. 226-18, 226-21, 226-23).

On August 1, 2010, defendant forwarded an email to Smith encouraging all recipients to boycott KLM airlines because a Dutch film ridiculed the Prophet. (Ex. 226-44). That was the last message defendant exchanged with Bill Smith.

G. The In-Person Undercover Investigation Commenced

The Bill Smith effort had failed to divine much information, but the FBI remained concerned that defendant could still pose a genuine threat. Based upon defendant's contacts with Khan and Al-Ali, his efforts to contact Abdul Hadi, his Internet postings, and his stated desire to become a "martyr," the FBI decided that defendant merited a closer look. (ER 4026, 4031, 4038, 4040–45, 4051, 4126, 4141).

The FBI knew that, in addition to these concerning actions, defendant was also drinking alcohol, smoking marijuana and partying at college in a manner inconsistent with Islamic rules. (ER 4151). The FBI was not aware at that time of any effort by defendant to research or obtain explosives. (ER 4175–77). But defendant's attempts to reach Abdul Hadi in May of 2010 (Ex. 225-51) provided an opening for the FBI to introduce defendant to undercover agents who could pose as Al-Ali's connection, and who could then further assess whether defendant posed a threat to national security. (ER 4050–51, 5006).

Just before the undercover operation commenced, defendant was prevented from boarding a plane to Alaska on June 14, 2010. (ER 4192). From its surveillance, the FBI knew that defendant intended to fly that day, and two agents met defendant

and his parents at the Portland airport after they had been turned away by airport authorities. (*Id.*). The FBI agents introduced themselves, and offered to answer any questions if they could. (ER 4194). Defendant's father was concerned that his son was unable to fly because he had contacted the FBI the prior summer (August of 2009). (ER 4194–95).

When asked if he knew anyone in Yemen, defendant said "Amr," but he claimed that he was unable to provide any other details. (ER 4195–96). Defendant denied that he had a visa or ticket for Yemen and denied having any interest in jihadi web sites. (ER 4195, 4197). Defendant was unaware of the fact that he was under surveillance and he was about to be contacted by an undercover FBI agent.

The initial goal of the undercover operation was for an agent to assume the role of Abdul Hadi (Al-Ali's contact). (ER 4049). Because the FBI feared that defendant would reconnect with Al-Ali, agents wanted to set up a meeting with defendant before that happened. (ER 4234). So an undercover agent known as Youssef, working with an FBI contact agent, sent an email to defendant on June 23, 2010, using an address similar to the one Al-Ali had given defendant. (ER 4053, 5012–13; Ex. 47).[9]

With that first email, Youssef told defendant to set up a "hushmail" account that would be secure and encrypted. (Ex. 47). Youssef explained that hushmail is commonly used by Al Qaeda, and he included this instruction to "add credibility" to

[9] Both undercover agents are practicing Muslims. (ER 4595).

his email. (ER 4237–38). He also interspersed his comments with Arabic phrases commonly used in the Islamic community. (ER 4239).

Defendant responded later that same day, "God be with you brother [in Arabic], how are you?" (Ex. 48). Two days later, Youssef asked if defendant was "still able to help the brothers?" (Ex. 49; ER 4053–55). He also mentioned that he had been "on the move," attempting to "continue the dialogue" defendant had going with Al-Ali. (Ex. 49; ER 4055).

Defendant responded the same day, telling Youssef that he was unable to travel right now, and asking that Youssef pray for his situation to change:

> i have been betrayed by my family, i was supposed to travel last year but Allah had decreed that i stay here longer than my heart desired. i am trying to find a way to go. i do not think i will be able to go for a while. i need to save up and also clear up somethings. Look for my emails [god willing], i will contact you when i am able to travel. Pray for me that allah will free my passage from the lands of the polytheists, peace be upon the messenger of Allah, his family and his companions.

(Ex. 50).

Three days later on June 28, 2010, Youssef sent another email expressing sympathy for defendant's frustration at not being able to travel. He wrote that he planned to travel to Seattle in July and, if defendant was "free sometime after July 19," he could stop by Portland to meet in person. (Ex. 51).

On July 16, 2010, defendant wrote to Youssef, telling him that he was available to meet any time after July 19, and he gave Youssef his cell phone number. (Ex. 53).

Defendant later suggested that they meet at the local mosque (Ex. 56), but Youssef demurred. (Ex. 58). By this point, defendant had demonstrated that his religious knowledge and sophistication was "much higher" than Youssef's. (ER 4240).

Youssef testified that it is contrary to FBI policy for investigations to take place within a mosque. (ER 4241, 4165). He nevertheless used religious phrases in many of his emails because "it had to look like a legitimate email." (ER 4154). To maintain his cover, he told defendant that he could not meet in a mosque because it would not be safe, he needed to meet with him privately, and "the kuffar [infidels] have eyes and ears in almost all masjids in the US." (Ex. 58). Defendant responded that he understood, but cautioned Youssef that he would "have a set of questions for you when we meet about your aqeeda to make [s]ure you are not a spy yourself." (Ex. 59). Defendant also mentioned that "amr" was the only person who could have given Youssef this particular email address, so he would also want to know how Youssef knows Ali "as a precaution." (*Id.*).

Because Youssef had never actually met Al-Ali, and because the FBI was concerned that he would not be able to answer many questions about Al-Ali, they invented a "council" to serve as a fictional intermediary between Al-Ali and Youssef. (ER 4064, 4244–45).

Youssef and defendant arranged to meet midday on July 30, 2010, in downtown Portland at a local bookstore (now closed). (ER 4245). The goal of that

first meeting was to "assess" defendant. (ER 4064–65; 4230). Youssef explained that he did not review the case file at all prior to meeting defendant to avoid bringing any "preconceived biases" into the case. (ER 4233). He also explained that "most undercover cases do not result in arrests." (ER 4231, 5007).

Defendant and Youssef walked the ten minutes to Youssef's hotel and spoke in the lobby. (ER 4247). Although Youssef was wearing a transmitter and a recording device, only the transmitter was working that day. (ER 4246). The tech agent responsible for the equipment accidentally turned on the recorder the day before the meeting, so it failed to record the initial meeting because the batteries were drained. (ER 5497–5504). Agent Chan listened to their conversation and wrote a report summarizing that initial face-to-face meeting. (ER 4255, 5017–19). Every other in-person meeting between defendant and the undercover agents was recorded and offered into evidence at trial.

Playing the part of an Al Qaeda recruiter, Youssef began by asking defendant what he had been "doing lately to be a good Muslim." (ER 4248, 4250, 5020). Defendant said that he had been writing poetry and articles for *Jihad Recollections*. (ER 4248–49, 5020). Defendant then asked Youssef how he obtained his email address, and Youssef explained that it had been forwarded to him by the "council." (ER 4249, 5021). At defendant's urging, Youssef described Al-Ali but suggested that he had only met Al-Ali "in passing" if at all. (ER 4249, 5021).

Youssef asked defendant if he could travel. (ER 4250, 5021). Defendant described his recent unsuccessful attempt, but omitted his meeting with the FBI. (*Id.*). Youssef then asked defendant what he was "willing to do for the cause?" (*Id.*). Defendant said that he had "originally planned to wage war within the United States," but then he'd had a "hadith" (dream) that he had traveled to Yemen, received training, and then "went to Afghanistan where he led an army against the kuffar (unbelievers)." (ER 4251, 5021–22).

Because defendant's answer referred to plans in the past, Youssef asked him again what his current plans were, providing five examples. (ER 4252, 5023). Youssef said that, to be a good Muslim, defendant could: (1) "just pray five times day"; (2) get his degree in engineering, "I'm sure they could use engineers overseas"; (3) raise money for the brothers, "We need money"; (4) become operational; or (5) become a martyr. (ER 4253, 5023, 5072). Defendant immediately responded that he wanted to become "operational." (ER 4253, 5073).

When Youssef asked what that meant, defendant said, "doing like the other brothers do when they get a car, fill it with explosives, park it near a target location, and detonate the vehicle." (ER 4253). Defendant explained that he had thought about doing this in Washington, D.C. "because of all the government buildings," but he admitted that he wasn't familiar with the area. (ER 4254, 5024).

If defendant had selected a non-violent option, Youssef believed that the FBI would have stopped the undercover operation "right away." (ER 4066). That sentiment was true throughout the course of the investigation. (ER 4482).

Youssef asked defendant if he was familiar with Portland, and defendant said that he was. (ER 4254,). Youssef then told defendant that he had a "brother that could help with explosives," and that defendant should "research possible places within the Portland area as possible targets." (*Id.*). As Youssef explained, he wanted to see if defendant was "serious," "because he may leave that day and I may never hear from him again." (ER 4254–55). This first face-to-face meeting lasted approximately 30 minutes. (ER 4255).

Without prompting, defendant sent an email to Youssef just three hours after their meeting. (ER 4256–57; Ex. 63). He attached copies of the four articles he wrote for *Jihad Recollections*. (*Id.*). Youssef replied, telling defendant he was "talented," in an effort to build some rapport. (ER 4258–59; Ex. 66). Defendant continued to send Youssef articles and poetry without prompting (Exs. 69, 73), and Youssef complimented him and counseled defendant not to talk to anyone, fearing defendant might reach out to Al-Ali. (ER 4261–65; Exs. 71, 75).

Twenty days after their initial in-person meeting, on August 19, 2010, Youssef introduced defendant to "Hussein," another undercover FBI agent posing as an Al

Qaeda explosives expert. (ER 4267).[10] This second meeting was also designed to "assess" defendant. (ER 4497).

Meeting in a hotel room in downtown Portland, defendant told the agents that he had been thinking about doing something since he was 15 years old; he also explained that he admired the Mumbai attacks: "I thought about you know, Mumbai you know like what happened in Mumbai to go somewhere you know to get some brothers with me and you know I, I used to be you know like I, you know like a rapper you know. So I could find someone would sell us you know like you know weapons you know like. I could find someone to give me you know a pistol or a AK." (ER 4281; Ex. 85).[11] He later elaborated that he "loved every second of it. I was happy you know," when he watched coverage of the Mumbai massacre on television. (Ex. 86).

Defendant also described his plan to travel to Yemen from Alaska, and how he had told his parents "the story was that I would go and study." (Ex. 85). But his parents foiled his efforts by, defendant believed, placing him on the no-fly list because they believed he'd been "the victim of some brainwashing." (*Id.*).

---

[10] The admitted video recordings from the August 19, 2010, meeting include: Exhibits 82–91. (ER 4267–4309).

[11] In November of 2008, ten Pakistani men associated with a terror group stormed buildings in Mumbai, India, killing 164 people. http://www.cnn.com/2013/09/18/world/asia/mumbai-terror-attacks/index.html.

Hussein explained that they complimented defendant both because he really was a good writer and to build rapport. Hussein also said that his many references to "Allah," were part of adding credibility to his role as an Al Qaeda bomb expert. (ER 4497, 4504, 4515–16, 4521, 4588–89).

Approximately 34 minutes into this meeting with the undercover agents (his second with Youssef, his first with Hussein), defendant said that he wanted to blow up Pioneer Square during the annual tree lighting ceremony on November 26, 2010, the day after Thanksgiving. (ER 4287–88; Ex. 84). Defendant explained that he had researched other potential targets, but he described several advantages of this one: he could drive a car right up into the square from the street, a lot of people would be in the square when the tree was lit at 5:30 p.m., no one expected an attack in Portland ("nobody really thinks about it"), and security would be light. (Ex. 84, 86). Hussein asked defendant if he planned on being in the car when it blew up, and defendant said yes because it would be "easier" that way. (*Id.*).

Defendant's demeanor was calm as he described his plan. Youssef wanted defendant to realize the import of what he was saying. (ER 4291). He confronted defendant: "you're talking like this like you're eating an ice cream. Do you understand what I'm saying?" (Ex. 86). Defendant assured him that he did. (*Id.*).

Defendant said that, "since I was fifteen I thought about all this things before." (*Id.*). And he explained his rationale: "imagine every day we see you know in Arab,

you know, newspapers and news you know our people are killed you know. So for us to see that you know it would be a smile from me to see them in the same . . . you know, you know what I like, what makes me happy? You know, what I like to see? Is when I see the enemy of God then they are you know their bodies are torn everywhere. Like when I see the pictures . . . That gives me you know like high hope and happiness you know." (*Id.*).

Carnage was not the only goal, however, as defendant also hoped that his plan would humiliate the local populace and alter international policy: "it also beneficial and it humiliates them you know and when they see that their own women and children are killed you know when they do that to others, then they, and they will refrain from doing that." (Ex. 84).

Youssef mentioned that there would be a lot of women and children at the event, thinking this might prompt defendant to change the venue, but it did not. (ER 4286–87). The presence of children, far from acting as a deterrent, made Pioneer Square an even more attractive target in defendant's eyes: "in general it's a huge mass that will, you know like for them you know to be attacked in their own element with their families celebrating their holidays. And then for later onto be saying this was them for you to refrain from killing our children, women." (Ex. 84).

The agents told defendant that there was "no shame" in leaving or dropping his plan. (ER 4290; Ex. 84). They reminded him that, "with us you always have a

choice." (ER 4291–92). After hearing defendant's plan to bomb Pioneer Square on Black Friday, Youssef again reminded him that he had options: he could pray five times a day to please Allah. But defendant was resolute. (Ex. 84). The agents also asked defendant what he would have done if he had not met them. (Ex. 90). Defendant planned to leave the country, "find the right people," "be somewhere they cannot capture you," and meet up with Al-Ali. (*Id.*).

The three left the hotel and walked to Pioneer Square where defendant explained the proposed attack in detail. (PSR ¶ 104).

Youssef's initial thought that defendant was "all talk" changed after the August 19 meeting; he became convinced that defendant was, in fact, "very serious." (ER 4308–09). He explained:

> Every attempt to get him to contemplate what he's saying, every attempt to scare him, every way out that we've given him, well, he didn't take any of them. He was not scared. He's very quick in his responses, and he's excited about it. He got emotional about an individual in Afghanistan ["Dawlat"], and everything he says is pro-jihad come November 26th.

(ER 4313–14).

Two days after the August 19 meeting, Youssef sent defendant an email stating that he and Hussein would present defendant's plan to the "council." (PSR ¶ 106; Ex. 92). In the meantime, Youssef wanted defendant to think about things to make sure this was what he really wanted to do. (*Id.*). Defendant replied that he had prayed for guidance and that his faith "was sky high for no apparent reason." (Ex. 93).

Youssef and defendant exchanged emails (Ex. 93, 95–98) to set up another in-person meeting for September 7, 2010. (ER 4318–19; Ex. 102). During this meeting, the agents succeeded in convincing defendant not to kill himself; operationally, defendant's plan to martyr himself on Pioneer Square presented a number of safety concerns (ER 4068), and the agents offered defendant a good reason to live: they would help him leave the country. (Exs. 102, 103). So although they presented defendant with two options regarding the manner of the bombing, they clearly hoped that he would agree not to martyr himself. (ER 4318–19).

To test his resolve, the agents also gave defendant several jobs: they gave him a list of bomb components to purchase and ship, they tasked him with coming up with a plan about where to park the van filled with explosives, and they talked to him about crafting a cover story for travel overseas via Mexico. (ER 4319–20, 4323). (Ex. 102–110). They gave defendant these assignments to test his resolve: "He'll realize —we hope that he'll realize what he's doing, the magnitude of his plan, and it gives him time to reconsider." (ER 4320, see also ER 4069). The agents showed defendant a mock jihadi training camp video (created by the FBI) to gauge his reaction; defendant's response: "It's beautiful." (ER 4326, 4511; Ex. 108).

Youssef also told defendant to rent his own apartment and a separate storage unit for the van that would carry the bomb, and he eventually gave defendant $2800 in cash to accomplish these tasks. (ER 4368). Defendant also had passport photos

taken that he provided to Youssef. (ER 4374; Ex. 35). Youssef explained that the FBI did not want defendant to have any roommates because it would be easier to maintain surveillance and it would reduce the chance that defendant could take matters into his own hands. (ER 4316–17). Youssef and Hussein nevertheless encouraged defendant to "go on with life as usual," and they urged him to maintain contact with his family. (ER 4401, 4514).

Between September 10 and October 2, defendant and Youssef exchanged 29 emails. They arranged to meet again in Corvallis, Oregon, on October 3. By this time, defendant had purchased cell phones and other components and shipped them to Hussein for use in building the bomb. (ER 4364–66). Defendant described his plan for parking the van in a 15-minute zone next to the Ben Bridge jewelry store located just one block east of Pioneer Square. (Ex. 133). Defendant also suggested that they change their email addresses. (Ex. 134). Their conversation that day ended with defendant's prediction that, "It's gonna be a, a firework display. A spectacular show . . . *New York Times* will give it two thumbs up." (Ex. 134).

H. The FBI Detonates a "Test" Bomb; Defendant Responds Enthusiastically.

In what turned out to be a very long day because they became lost, defendant and the agents drove to a remote location to "test" a scaled-down version of the bomb they were planning to detonate at Pioneer Square. (ER 4378–79; Ex. 150–153).

Hussein explained that they wanted to be sure defendant understood the magnitude of what he was proposing to do. (ER 4527).

During the drive, defendant talked about his desire to learn "the inside and out of weaponry" and "bomb-making." (Ex. 150). He also wanted to teach "special operations," which to him meant "making the enemies you know afraid." (Ex. 150, 151). The "enemies" defendant described included "these people who live in this country [who] are the most evil people on the earth." (Ex. 154).

As on prior occasions, Hussein reminded defendant that they could drop the plan and that there would be no repercussions: "I can disappear and you never know me, so." (Ex. 158). Defendant ignored him, instead commenting on the irony of the term "Black Friday." (*Id.*).

Hussein also reconfirmed that defendant had not told anyone else about the plan—fearing interference by a real terrorist partner—and defendant assured him that he had not. (*Id.*). Defendant explained that his "image in Corvallis is I'm just a college student, you know," so "nobody even knows that I have you know, that I'm inclined toward jihadi, or even towards even like being Islamic." (*Id.*).

After believing he had detonated the small bomb (ER 4525, 4972), defendant said that he felt "good," and observed that the test "is just motivation for me." (Ex. 159). When Youssef and Hussein asked defendant if he had ever actually seen a "person's insides," or dead bodies, defendant responded:

> MOHAMED: [R]emember when nine eleven happened when those people were jumping from sky scrapers?
>
> YOUSSEF: Yeah.
>
> MOHAMED: I thought that was awesome.

(Id.).

Youssef and Hussein drove defendant back to Corvallis. During the drive home, Youssef suggested that defendant make a "good bye" video to explain his actions because it could be "inspirational." (ER 4388, 4441). Defendant agreed without hesitation, and he wrote the script for the video using topics Youssef suggested. (ER 4388, 4443–46, 4480).

In that video, which defendant made later that day, he explained that his intended actions on November 26, the day of the planned attack on Pioneer Square, would be a "message to those who have wronged themselves." (Ex. 166). He described the "dark day" that was coming, and said that no one would be safe "for as long as you threaten our security." (*Id.*). Living in the United States "is a sin," and he urged Muslim parents living in the west not to do what his parents did to him; not to "hold others back from completing their obligation" to Allah. (*Id.*). He finished by reading a poem that he wrote that extolled the virtues of Muslims and jihad, and ended with a call to "carry on oh brothers, and march on ahead to meet your creator and lie on silk beds, and the martyrs don't die, so don't say they're dead. Explode on

our Explode on these [unbelievers]. Alleviate our pain. Assassinate their leaders, commanders, and chiefs from your brother to his brothers a poem in brief." (*Id.*).

I. The Final Planning Stages

Just days after defendant viewed the explosion of the test bomb, he was exchanging emails with Daulat, his friend in Afghanistan. Daulat asked defendant to "investigate" predator and reaper strike drones to figure out "how to down them." (PSR ¶ 127). Defendant responded that he would help, but told Daulat not to try to reach him at his old email address anymore. (PSR ¶ 128). He signed off telling Daulat: "I hope we meet again soon [god willing]." (*Id.*).

Defendant met the agents again in Corvallis on November 18; they picked defendant up from his apartment and drove to the storage unit defendant had rented. (ER 4532; Ex. 178; PSR ¶ 129). Defendant selected the storage location, in part, because there were no surveillance cameras. (ER 4535–36).

They then drove to a hotel in Portland where defendant showed them potential parking spots he had researched on his computer. (PSR ¶ 129). They walked to Pioneer Square again, and defendant (unprompted) suggested they mount hidden cameras so that they could tell when the Max light rail trains were nearby. Defendant hoped they could time the blast to maximize casualties. (ER 4542, 4729; Ex. 187).

Defendant appeared "excited" at this meeting. (ER 4533–34). Hussein told him to spend time with his family. (ER 4533).

During this November 18 meeting, Youssef asked: "what's a victory gonna be for you?" (Ex. 182). Defendant replied: "Try to get most, the most casualties." (*Id.*). Defendant anticipated that the bombing would generate a lot of publicity because "America's boasting it so 'oh we haven't been attacked since 9/11.'" (*Id.*).

Defendant revealed how he first became interested in jihad: his friend "Shukri" introduced him to the idea, and when defendant asked him if jihad was the same thing as terrorism, Shukri responded "brother, to be honest we love anything that terrorizes [the unbelievers]." (Ex. 192)

Shukri counseled defendant not to "tell anybody what I told you just keep to yourself." (Ex. 192). Shukri also told defendant that he was being "monitored," and so any further communication would have to be in person: "If I come to Portland I see you then that's how we meet but don't like you know call me or email me." (*Id.*).

Defendant and the agents met again on November 23 in Corvallis. Hussein and defendant loaded bomb components into the storage unit. (PSR ¶ 131). Defendant purchased disguises for the event: they would pose as water workers wearing reflective vests, hard hats, and gloves. (ER 4549; PSR ¶ 132).

On Thanksgiving Day, defendant rode up to Portland and spent the day with friends. (PSR ¶ 133). He was "happy" that day, although at dinner he became "reserved." (ER 5539, 5548–49). He went shopping at an outlet mall that night with

his friends, and the next day he confirmed with them several times that they were all returning to Corvallis. (ER 5540–41, 5550).

J. Black Friday 2010

Early the next morning, on November 26, defendant ran into a friend in front of a store, and he told his friend, "I'm having the greatest morning of my life." (ER 5574). Later that morning, Hussein met defendant and Youssef at a hotel in downtown Portland. (ER 4880). Defendant appeared "happy and excited." (*Id.*). The three of them drove about a mile to where the van was parked. (ER 4882). When Hussein opened the back door to the van to reveal the bomb and the smell of diesel fuel, defendant responded that it was "beautiful." (ER 4885).[12]

Government's Exhibit 245

[12] An FBI Agent, certified as a bomb technician, built the device. (ER 4971). He duplicated defendant's purchases, and made it look as realistic as possible; if it had been real, it would have looked "exactly the same." (ER 4980).

They returned to their hotel, ate, talked, and prayed. (ER 4733). They watched the local news, and defendant was pleased to hear that 25,000 people were expected to gather in Pioneer Square for the 5:30 p.m. tree lighting. (PSR ¶ 136). Shortly before 5:00 p.m., the three left the hotel and drove to the van; Youssef dropped defendant and Hussein off, then drove to a pre-arranged meeting location a few blocks west of Pioneer Square. (ER 4733, 4887; PSR ¶ 137).

Hussein and defendant drove the van towards Pioneer Square, while the FBI ensured that the parking spot defendant had pre-selected would be available; it was not the "miracle" defendant assumed. (ER 4888, 4899). Before exiting the van, Hussein told defendant that he had to connect the wires for the detonator to work. (ER 4889). Defendant did so, then taking the cell phone detonator with him, they walked several blocks to join Youssef in his car. (ER 4733, 4890).

As the three drove north towards the railroad station, defendant told the others that he had just seen his mother driving in front of them. (Ex. 221; PSR ¶ 139). He was surprised but undaunted. Hussein dropped Youssef off, then he and defendant parked a few blocks from the railroad station. (ER 4890–91; Ex. 221). Defendant pulled out the cell phone and Hussein read off for him the number to call to detonate the bomb; defendant looked at the paper Hussein was reading from, attempting to dial in the number as quickly as possible. (ER 4892). When nothing happened,

Hussein suggested that they should step out of the car for better reception, and this was the signal for the arrest. (*Id.*).

Defendant was dialing the number into the cell phone again when FBI agents announced their presence and arrested them both. (ER 4913; Ex. 221). Hussein was screaming, "Allahu Akbar!" as he was being arrested. (Ex. 221). Defendant was quiet initially, but during transport he began to kick violently at the agents and had to be restrained. (PSR ¶¶ 144–146).

Agents found an undated email printout defendant had received from Al-Ali in defendant's pocket or wallet. (ER 4929–30, 4940). During a search warrant executed right after the arrest, agents found two videos on defendant's computer of the Portland Christmas Tree Lighting Ceremony for 2007 and 2008. (ER 5613; Ex. 240-1, 240-2). They also found a downloaded Al Qaeda video, an MP3 file titled "no peace with the Jews," and numerous references to "jihad." (ER 5641–70). In a composition notebook found in his apartment, defendant wrote: "Non-Muslims are the eternal enemy of Islam and they must be subdued and humiliated." (Ex. 10). He also described the need to "mistrust" everyone and to act normal "to secure myself from the FBI." (*Id.*).

Throughout their interactions with defendant, Youssef and Hussein described defendant as "very determined," (ER 4506, 4510–11), "happy and excited," (ER

4880), he displayed no hesitation (ER 4892), and "he knew what he wanted to do—and it was to kill Americans—before I met him." (ER 4478).

SUMMARY OF ARGUMENT

Defendant was presented with an opportunity to fulfill a dream he had when he was 15 years old. That dream was to fight the infidels as a mujahideen for Allah. When two purported Al Qaeda operatives contacted him and implied it was on behalf of a wanted Saudi terrorist named Al-Ali, defendant embraced them and presented them with his dream: he wanted to detonate a car bomb during the annual Portland tree lighting ceremony.

As a festival of the "kufar," defendant knew that a deadly attack at a family-oriented event would be particularly devastating to the local community and the nation. That is precisely what he wanted—something to generate "two thumbs up" from the New York Times. Fortunately, however, the Al Qaeda operatives were actually undercover FBI agents and the bomb was a carefully constructed fake. But defendant's intent could not have been clearer: for months, he completed tasks designed to help accomplish his goal, he never wavered, and when the final moments came, he eagerly dialed the numbers he thought would detonate the bomb and kill or injure thousands of people. Twice. He was predisposed to commit this crime.

Defendant was, and is still, a young man. As are many terrorists and aspiring terrorists. That fact alone cannot insulate someone from a criminal investigation.

Entrapment was the sole issue at trial, and the jury was able to watch and listen to the undercover agents' interactions with defendant because all but one of their meetings were videotaped; jurors were able to observe defendant's demeanor and see how keenly he participated in the charged crime.

Although defendant may have lacked the wherewithal to build a bomb on his own, he actively wanted to commit an act of terrorism on United States soil. The government gave defendant the opportunity to prove if his intentions were real or illusory. The jury found that defendant's intentions were real because he was either predisposed to commit the crime charged or he was not induced into committing the crime by anything the government agents said or did. Because that verdict is based on ample evidence in the record, it should be affirmed.

Defendant also received a fair trial. Represented by three experienced criminal defense attorneys, defendant's interests were vigorously protected throughout the proceedings. Discovery was complicated by national security concerns, but the district court examined each classified matter in camera and ordered the government to disclose to the defense what was needed to protect defendant's interests. There was nothing unconstitutional about the process or the court's conclusions. Moreover, the government's post-trial disclosure that certain evidence obtained or derived from the Foreign Intelligence Surveillance Act (FISA) was also derived from surveillance

authorized by the FISA Amendments Act (FAA) did nothing to undermine the fairness of the pretrial rulings, trial, or sentencing hearing.

The district court also carefully considered all of the parties' disputes about evidentiary rulings, jury instructions, and the government's closing argument, and it reached decisions consonant with the rules of evidence and constitutional principles. Both the trial court and the government accurately described the entrapment defense, the jury was permitted to hear limited information about why the FBI was investigating defendant, and defendant presented evidence (through others) of his own state of mind. There was no abuse of discretion with any of these rulings.

The district court properly denied defendant's motion to suppress evidence derived from surveillance authorized under the FAA (more specifically, Section 702 of FISA). The Section 702-authorized collection at issue in this case, which was conducted pursuant to court-approved procedures reasonably designed to target non-U.S. persons located outside the United States, was reasonable under the Fourth Amendment. First, the Fourth Amendment generally does not apply to non-U.S. persons abroad. The fact that collection targeting such persons also incidentally collects communications of U.S. persons does not trigger a warrant requirement or render the collection constitutionally unreasonable. Second, surveillance conducted pursuant to Section 702 falls within the well-recognized "foreign intelligence exception" to the warrant requirement because (1) the government's purpose –

protecting against terrorist attacks and other external threats – extends beyond routine law enforcement, and (2) a warrant requirement would materially interfere with the accomplishment of that purpose.

Because no warrant is required for surveillance targeting non-U.S. persons abroad, the challenged collection need only meet the Fourth Amendment's general reasonableness standard. That standard is satisfied here. The government has interests of the utmost importance in obtaining foreign intelligence information to protect national security. The privacy interests of U.S. persons whose communications are incidentally collected under Section 702 are amply protected by stringent safeguards the government employs in implementing the collection. Those safeguards include (1) certifications by Executive Branch officials concerning the permissible foreign intelligence purpose of the collection; (2) a prior judicial finding that the targeting and minimization procedures are consistent with the Fourth Amendment; (3) court-approved targeting procedures designed to ensure that only non-U.S. persons abroad are targeted; (4) court-approved minimization procedures to protect the privacy of U.S. persons whose communications are incidentally acquired; (5) the requirement of a significant purpose to obtain foreign intelligence information; and (6) extensive oversight by all three branches of government.

Defendant's other challenges to Section 702 collection also lack merit. Section 702 does not violate the First Amendment by creating an unconstitutional "chilling

effect." Nor does judicial approval of Section 702 targeting and minimization procedures violate separation-of-powers principles. Judicial review of those procedures is analogous to judicial review of warrant applications, and thus, Section 702 collection does not violate separation of powers principles. And the district court did not abuse its discretion under its supervisory powers in denying defendant's motion to suppress evidence as a sanction for alleged misconduct related to the timing of the government's notice of Section 702 surveillance. Even if defendant's claims were meritorious, the good-faith exception would preclude suppression because government agents reasonably relied on a duly enacted statute, orders issued by a neutral magistrate, and appellate precedent.

Finally, the court selected a 30-year sentence after carefully considering all of the evidence it heard at trial and at sentencing. The court acknowledged that the case was one of the most difficult it had encountered, and it selected a sentence that it felt was reasonable given all of the circumstances. The judgment should be affirmed.

ARGUMENTS

I. The Jury Reasonably Concluded that Defendant Was Not Entrapped.

Standard of Review: Entrapment as a matter of law requires "*undisputed evidence* making it patently clear that an otherwise innocent person was induced to commit the illegal act." *United States v. Staufer,* 38 F.3d 1103, 1108 (9th Cir. 1994) (emphasis in original). Evidence is sufficient to support a conviction when, viewing

the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime—including the elements negating entrapment—beyond a reasonable doubt. *United States v. Si,* 343 F.3d 1116, 1123, 1125 (9th Cir. 2003).

"The question of entrapment is generally one for the jury, rather than for the court." *Mathews v. United States,* 485 U.S. 58, 63 (1988). The government had to negate entrapment beyond a reasonable doubt. *Ninth Circuit Model Jury Instruction* 6.2 Entrapment (2010). To do so, the government had to establish either: (1) defendant was predisposed to commit the crime before government agents contacted him; or (2) government agents did not induce defendant into committing the crime. *United States v. McClelland,* 72 F.3d 717, 722 (9th Cir. 1995).

Predisposition is a "defendant's willingness to commit an offense *prior* to being contacted by government agents." *United States v. Poehlman,* 217 F.3d 692, 698 (9th Cir. 2000). Five factors guide the predisposition inquiry: (1) defendant's character or reputation; (2) who initially suggested the criminal activity; (3) whether defendant engaged in the activity for profit; (4) whether defendant exhibited any reluctance to commit the offense that was overcome by repeated government inducement or persuasion; and (5) the nature of any government inducement or persuasion. *United States v. Williams,* 547 F.3d 1187, 1198 (9th Cir. 2008).

No single factor is controlling, but a "defendant's reluctance to engage in criminal activity is the most important." *Id.* (citation omitted). And the government need not satisfy each and every factor. *McClelland,* 72 F.3d at 722 (affirming conviction when government's evidence sustained three of the five factors). Evidence developed during the course of the investigation—i.e., after defendant's contact with the government—is also relevant to predisposition. *United States v. Thickstun,* 110 F.3d 1394, 1397 (9th Cir. 1997). A defendant may be predisposed to commit the crime charged "if he was ready and willing to do so and likely would have committed it without the government's intervention, or actively wanted to but hadn't yet found the means." *United States v. Mayfield,* 771 F.3d 417, 438 (7th Cir. 2014) (en banc).

For inducement, the mere fact that the government initiates contact, solicits the crime or furnishes the opportunity to commit the crime does not necessarily constitute entrapment. *Mayfield,* 771 F.3d at 420–21. The Supreme Court has found inducement as a matter of law when, for example, government agents originated a crime and engaged in a 2½-year effort to convince defendant to order child pornography that it claimed should have been legalized. *Jacobson v. United States,* 503 U.S. 540 (1992).

The district court denied defendant's motion for judgment of acquittal because sufficient evidence negated defendant's entrapment defense during trial. (ER 132–38). The court focused upon defendant's statements that he began thinking of taking

part in violent jihad at the age of 15 and that he originally planned to wage war in the United States, defendant's articles for *Jihad Recollections* advocating violent jihad against Americans, and his online contacts with Khan and Al-Ali. (*Id.*). All of these facts, and others, provide ample support for the jury's verdict.

Any jury could reasonably conclude based upon the evidence adduced at trial that defendant was predisposed to commit the crime charged and that he was not induced. Defendant told the undercover agents that he had been thinking about becoming operational since the age of 15. He told the agents that he admired the 2008 Mumbai attacks, and that comment simply reiterated what he had written in February of 2009 in his first article for *Jihad Recollections*. (Ex. 223-38).

In response to questions about what he wanted to do to "support the brothers," defendant stated without any hesitation that he wanted to be "operational." Less than two weeks later, after conducting his own independent research, defendant laid out a plan to detonate a car bomb at Pioneer Square during a popular local event. Even if the specific plan did not become fully realized until after defendant met Youssef, defendant's own words constitute strong evidence that he was in fact primed for this crime. And his motivation was well-rooted in his history from his interactions with Al-Ali, Khan, and his friends Shukri and Daulat.

Defendant's motive to commit the crime is also apparent from his actions prior to the undercover operation: his articles for *Jihad Recollections* revealed his belief that

non-Muslims were the enemy and that good Muslims prepared to fight the infidels. And defendant repeatedly expressed a desire to be a "good" Muslim as he defined that term. He also maintained contact with Amro Al-Ali, who had referred defendant to a Yemeni training camp known as a "steppingstone" for people from the West seeking to join Al Qaeda. (ER 5712).

Defendant's predisposition is also evidenced by his willingness to engage in the crime charged once the undercover agents presented the opportunity. *See Si,* 343 F.3d at 1125 (noting that the mere fact the government provided a fictional robbery target was not enough to prove entrapment). The fact that defendant lacked the wherewithal to commit the crime without the agents was a relevant factor for the jury to consider, but it was not dispositive.

Most critically, the plan itself was defendant's brainchild. The undercover agents were not even familiar with the city or its traditions. In the Spring of 2009, well before any contact with the government, defendant expressly recognized the import of holiday "festivals of the kuffar," revealing that he knew just how devastating an attack on the tree lighting ceremony would be. (Ex. 223-25).

After his first meeting with Youssef when defendant said he wanted to be "operational," defendant created the plan that would eventually form the basis for the indictment. Defendant's own terrorism expert (Dr. Mark Sageman) agreed that defendant was an "extremist" while he was writing for *Jihad Recollections* (ER 6160–61),

and that by November 26, 2010, defendant "met all of the criteria for a genuine threat." (ER 6164–65). Kohlmann, after reviewing the defendant's hard drive, saw evidence of six common characteristics defendant shared with people engaged in jihadist behavior. (ER 5694–95, 5802).

Defendant's vision for what it meant to be "operational" was his own creation, and the jury was free to disregard defendant's theory that Bill Smith "implanted" that thought by mentioning in an email several months' prior that he (Smith) wanted to bring his "fight" to the West. Smith never mentioned violence, and he never suggested that defendant commit an act of violence in the United States.[13] The 44 emails exchanged between the two over the course of six months reveal only that Smith repeatedly sought "guidance" from defendant and that, while defendant was willing to offer advice, he also was cautious enough to keep Smith at a distance because he was a complete unknown.

Defendant's predisposition can also be seen in his motivation to commit the crime. This is not a case about greed or profit; instead, defendant was motivated by radical extremism. The composition book seized shortly after his arrest revealed a

[13] Defendant also suggests that Youssef deliberately implanted the notion of targeting Pioneer Square because, in his first phone call with defendant, he mentioned it. A reasonable jury could, however, have seen that call for what it was: Youssef giving defendant directions to the bookstore (located directly across the street from Pioneer Place Mall) where they planned to meet. Even Portlanders commonly and mistakenly refer to the mall as "Pioneer Square."

young man whose private thoughts differed significantly from his public persona. Although his friends from OSU testified that he was outgoing, fun, and friendly, defendant disdained nearly every aspect of his college life. Women, sex, drugs, and alcohol were all evil Western temptations. These thoughts mirrored earlier criticisms defendant leveled at the U.S. military in his articles for *Jihad Recollections*: American soldiers were lazy, weak, and lacked the discipline of his admired mujahideen. And as he explained in his notebook and in the video he scripted, the West had to be humiliated to remediate its intervention in the Middle East; defendant was going to do his part to see that this happened.

If a defendant's reluctance to engage in criminal activity is the most important factor in assessing predisposition, then this record amply supports the jury's verdict because defendant consistently evinced no hesitation whatsoever. Despite every task he was given, and even when confronted with an example of the blast, defendant pushed on. From his first meeting with Youssef when he said he wanted to be "operational," to his subsequent meetings in which he revealed the details of his plan, to the final day when he thought he saw his own mother driving downtown near Pioneer Square, to the final moments when he dialed the number into the cell phone, defendant remained resolute.

This resolve was neither the product of government suggestion, nor the result of government inducement. Unlike the facts in *Jacobson*, 503 U.S. 540, the agents did

not have to engage in a two-year campaign to convince defendant to become operational; and unlike the facts in *Sorrells v. United States*, 287 U.S. 435 (1932), defendant showed no hesitation whatsoever.

To the contrary, defendant appeared eager and enthusiastic throughout: as captured by the video surveillance, defendant was "happy," the bomb was "beautiful," and after settling on his plan to detonate a bomb at Pioneer Square, defendant said his "eeman (faith) was high." Defendant was convinced that his plan would please Allah, and that in turn made him a most enthusiastic participant. He dialed the number into the cell phone detonator twice, confirming his commitment to carry out his planned attack in terms that leave no room for doubt. Defendant wanted to kill a lot of people that Black Friday and his desire to do so had been building for years.

Defendant's argument that he was reverting to the role of a normal college student when the government suddenly placed him back on the track towards terrorism is also something a reasonable jury could reject given defendant's repeated efforts to connect with Al-Ali and Abdul Hadi throughout this period, and his continued on-line activities on pro-jihadi websites. A reasonable jury could well have concluded that defendant's drinking and active social life were simply a cover, particularly given defendant's description of non-Muslims as the "eternal enemies of Islam" who "must be subdued and humiliated," and his own efforts to "hold normality to secure myself from the FBI lest they should monitor me." (Ex. 10).

A reasonable jury could also have rejected defendant's claim that government agents induced him by isolating him from his friends and family. Several of defendant's friends testified at trial about what a likeable, social person defendant was; indeed, he spent Thanksgiving Day with many of these friends, singing on the drive up from Corvallis and shopping with them that night. Defendant was not an isolated loner starved for attention or praise from the FBI.

The few cases that have found entrapment as a matter of law stand in stark contrast to this one. Excepting the brief email exchange between defendant and Bill Smith (43 emails between November 2009 and May 2010), the undercover investigation in this case spanned just five months from the initial email contact in June to Black Friday. Within that five-month period, defendant met with the agents in person just eight times with few email and telephone contacts in between. That is approximately one meeting every two weeks. This is not a case in which the agents moved in with defendant, surrounded him, badgered and cajoled him. The lapses in time between meetings, and Youssef's availability via email and text would have made it easy and painless for defendant to have cut off contact at any point.

Moreover, the agents repeatedly reminded defendant that he could withdraw and take another route such as prayer or studying to become an engineer or a doctor. Hussein told defendant that he (Hussein) could easily "disappear," so defendant knew that there would be no negative repercussions if he were to change his mind. (Ex.

158). Youssef repeatedly warned him about the devastation and carnage the plan would bring about and, rather than deterring him, such dire predictions only strengthened defendant's resolve: "what makes me happy? You know, what I like to see? Is when I see the enemy of God then they are you know their bodies are torn everywhere . . . That gives me you know like high hope and happiness." (Ex. 86).

The suggestion that defendant lacked the maturity or wherewithal to withdraw is something the jury could easily have rejected for several reasons. One of his college instructors—a witness defendant called—described him as particularly intelligent and mature. The jury saw examples of his writing skills and could consider how thoughtful and articulate—albeit misguided—he was. And the jury heard about two instances in which defendant demonstrated that he knew how to say no. Despite his enthusiasm for *Jihad Recollections*, defendant withdrew from participating in the fourth issue and he suffered no adverse repercussions; Khan simply wished him well. Defendant also demonstrated his caution and independence with Bill Smith by the manner in which he demurred from ever meeting or more directly engaging with Smith. While Smith talked about traveling to Portland, defendant neither revealed that he lived in Portland, nor did he disclose any other details that might have revealed his true identity. He followed his own advice by remaining cautious.

Guided by jury instructions that directed them to consider a variety of factors relevant to inducement, a reasonable jury could have considered Youssef's and

Hussein's praise for defendant's poetry and Hussein's invocations to Allah as part and parcel of their roles as Al Qaeda operatives. Had the agents done nothing to develop a rapport with defendant, they would not have been believable; as it was, their compliments were mild enough not to have crossed the line from rapport-building into active persuasion. And the law does not require or expect undercover agents to act like robots who show no compassion or emotion towards their targets. *See, e.g.*, *United States v. Slaughter*, 891 F.2d 691, 695 (9th Cir. 1989) (recognizing that informants must develop a rapport with their targets).

Moreover, a reasonable jury could fairly have measured the type and quantity of inducement against the crime charged. Even if mild inducement such as flattery and a shared religion were sufficient to induce someone to jaywalk, they would not normally suffice to convince an otherwise innocent person to detonate a weapon of mass destruction at a crowded public event. And nothing in this case rose to the level necessary to sustain an outrageous government conduct claim under the Due Process Clause. Defendant's age was relevant to inducement, but it does not insulate him from criminal investigation.[14] The jury was also free to reject defendant's claim that

[14] Defendant repeatedly describes himself as a "vulnerable teen," and yet there was no evidence at trial that he was any more vulnerable than any other 19-year old. An expert merely explained that the prefrontal cortex is not fully developed until age 25. (ER 6027). Teenagers are often the intended audience for Internet proselytizers who seek to encourage acts of violence: Dzhokhar Tsarnaev was 19, and twelve of the nineteen 9/11 hijackers were under the age of 25.

the agents induced him by interfering with his family relations given that Hussein and Youssef repeatedly told defendant to spend time with his family.

Because there is ample evidence in this record to support the jury's determination that defendant was either predisposed to commit the crime or not induced to commit the crime, the district court properly denied defendant's motion for judgment of acquittal.

II. The Government Correctly Described Entrapment During Closing Argument.

Standard of Review: Whether the government misstated the elements of entrapment is reviewed de novo; if there was a misstatement, however, defendant is not entitled to relief unless the error was "so gross as probably to prejudice" his defense. *United States v. Del Toro-Barboza,* 673 F.3d 1136, 1153 (9th Cir. 2012).

According to defendant, the government repeatedly asked the jury to "treat the defense as categorically unavailable." (D. Br. 65). The government did nothing of the sort.

At no point did the prosecutor state or even suggest that entrapment was not a legally viable basis for acquittal. Instead, the prosecutor urged the jury to use its common sense when assessing the facts; if it did so, he reasoned, it could not conclude that defendant could be entrapped into committing an offense of this magnitude. The argument was entirely proper.

What the prosecutor said, several times throughout his presentation, was that if the jury were to employ its common sense it would conclude that defendant made his own choices, and that "an individual . . . cannot be entrapped to commit an offense such as this." (ER 6223), see also ER 6236 ("it is hard to entrap someone to commit an offense like this"); (ER 6255: "there can be no entrapment under these facts"); (ER 6258: "This notion that saying nice things would cause an otherwise innocent person—and that's the legal standard—to commit this offense is not supported by the facts"); (ER 6354–55: "what could the agents do to make a person push the button in this manner? And the Government's position based on this evidence, based on the evidence you have before you, is nothing.").

He properly emphasized the nature of the offense as relevant to the inducement question: "this is the type of offense that one commits only because they wholeheartedly want to." (ER 6226); ER 6359 ("It's not a situation where someone could be persuaded to do such a remarkable thing."). He also explicitly told the jury that whether defendant was entrapped was an issue that it had to decide: "[t]he real legal issue in this case, as applied to the facts, we believe, is the question of entrapment. Was this defendant entrapped, as the law defines entrapment?" (ER 6224); see also ER 6268 ("It's did they induce him to take an otherwise law-abiding person and have them push the button? That is the issue.").

There was also no burden shifting. On five separate occasions throughout the closing and rebuttal, the prosecutor reminded the jury that the government bore the burden of proving beyond a reasonable doubt that defendant was not entrapped. (ER 6224, 6277, 6354, 6361). Coupled with the court's jury instructions, the jury heard only that the government bore the burden of proof.

Defendant's reliance upon *United States v. Segna*, 555 F.2d 226 (9th Cir. 1977), is entirely inapposite because, in that case, the government erroneously told the jury that the defendant was presumed sane in a case in which insanity was the sole issue and the defense had clearly come forward with sufficient evidence of insanity to eliminate the presumption.

The district court recognized that the prosecution "must have reasonable latitude to fashion closing arguments." (ER 144, citing *United States v. Moreland,* 622 F.3d 1147, 1161 (9th Cir. 2010)). Reasonable latitude includes commenting upon the evidence and urging the jury to interpret the evidence in a manner favorable to the government's view of the case. The prosecutor never said or suggested that this jury should presume that defendant was not entrapped or that entrapment was unavailable as a matter of law. Instead, he argued that entrapment was not supported by the facts because common sense suggested that most people could not be "induced" to detonate a weapon of mass destruction at a crowded local event. There was no error in the government's closing argument.

Moreover, any harm from a prosecutor's misstatement may be minimized by proper jury instructions on the elements, along with an instruction reminding the jury that counsels' arguments are not evidence. *United States v. Mendoza,* 244 F.3d 1037, 1045 (9th Cir. 2001). Jury instructions "carr[y] more weight than an argument." *United States v. Begay,* 673 F.3d 1038, 1046 (9th Cir. 2011) (en banc). And any erroneous comment may be further mitigated if the prosecutor accurately describes the elements during other points of his argument. *Id.*

The district court mitigated the potential effects of anything the prosecutor may have said during argument when it instructed this jury that the lawyers' questions, statements, and arguments "are not evidence." (ER 6213). The court also told the jury that the government bore the burden of proving beyond a reasonable doubt that defendant was not entrapped. (ER 6218). Relying upon this Court's model instructions, the court correctly explained that to be found guilty, defendant either had to be predisposed to commit the crime or not induced by government agents to commit the crime. (*Id.*). The court never suggested that defendant could not have been induced because of the nature of the crime; instead, it appropriately left these issues for argument. There was no error.

III. The District Court Neither Erred Nor Abused Its Discretion in Formulating the Jury Instructions.

Standard of Review: This Court reviews *de novo* whether jury instructions properly state the elements of the charged offenses and adequately cover the

defendant's theory of the case. *United States v. Whittemore,* 776 F.3d 1074, 1077 (9th Cir.), *cert. denied*, 136 S. Ct. 89 (2015). On appeal, however, defendant bears the burden of demonstrating "(1) that his theory had some foundation in evidence; (2) that it is supported by law; and (3) that the given instructions did not adequately encompass his theory." *Id. at* 1078. A defendant is "not entitled to the instructions of his choice." *Id.* at 1080.

Defendant's first and second claims regarding the district court's jury instructions overlap with his objection to the manner in which the court handled the jury question about predisposition. Defendant argues that the court should have modified this Court's model jury instruction on predisposition to require proof that defendant was predisposed to commit the specific crime charged in the indictment. He also claims that the court erred by failing to modify this Court's model instruction, patterned after the Supreme Court's decision in *Jacobson,* that he was an otherwise "innocent" person; instead, he claims that this case raised a "specialized meaning of the term innocent," which necessitated replacement of the word "innocent," with "not otherwise predisposed."

All of these arguments relate to defendant's theory that his predisposition to commit criminal acts of terrorism overseas could not satisfy the government's burden of proving predisposition to attempt to detonate a weapon of mass destruction within

the United States. Because defendant's theory is fatally flawed, his multiple objections to the court's jury instructions should be rejected.

Defendant's theory defines predisposition too narrowly. Although the Supreme Court has stated that simply being predisposed to violate the laws generally will not suffice, neither the Supreme Court nor any circuit has held that predisposition requires proof that a defendant was contemplating the precise crime charged prior to any government involvement. *Jacobson v. United States,* 503 U.S. at 550.

In fact, the Supreme Court has from its first recognition of the entrapment defense acknowledged that it calls for "an appropriate and searching inquiry" into a defendant's conduct and purposes. *Sorrells,* 287 U.S. at 451. A convicted embezzler may not be predisposed to commit murder-for-hire.[15] But a drug dealer may well be predisposed to commit tax evasion or money laundering because those criminal activities share a common goal (generating and preserving income) and purpose (keeping the business under law enforcement's radar).

Jury instructions defining predisposition within this circuit to include crimes with common characteristics have been upheld. This Court has rejected challenges to jury instructions that identified the government's burden as one that requires proof

[15] An embezzler who commits a wholly different crime at the behest of a government agent is not necessarily entrapped. If he enters into criminal activity "with relish," he is not induced, and therefore not entrapped. *See, e.g.*, *United States v. So,* 755 F.2d 1350, 1353 (9th Cir. 1985) (affirming money laundering conviction even absent evidence of predisposition to commit money laundering).

that a defendant was predisposed "to commit crimes such as are charged." *United States v. Makhlouta,* 790 F.2d 1400, 1405 (9th Cir. 1986); *see also United States v. Williams,* 547 F.3d 1187, 1198 (9th Cir. 2008) (upholding finding that defendant was not entrapped into distributing cocaine because his prior bank robbery and illegal gun sales "suggest[ed] that he was predisposed to this type of criminal activity"). *United States v. Varela,* 993 F.2d 686, 688–89 (9th Cir. 1993) (affirming a jury instruction that defined a predisposed person as one who is "ready and willing to commit crimes."). Other circuits agree.

The Sixth Circuit rejected a defense argument that the government had to prove that he was predisposed to commit every element of the offense charged. *United States v. Al-Cholan,* 610 F.3d 945, 950 (6th Cir. 2010). Instead, evidence "near enough in kind to support an inference that [the defendant's] purpose included offenses of the sort charged." *Id.*, *citing United States v. Brand,* 467 F.3d 179, 200 (2d Cir. 2006); *see also United States v. Hackley*, 662 F.3d 671, 682 (4th Cir. 2011) ("Predisposition is not limited only to crimes specifically contemplated by the defendant prior to government suggestion") (internal citations omitted).

So while the government must ultimately convince a jury that a defendant was predisposed to commit the crime charged, evidence that a defendant was predisposed to commit similar or related crimes may satisfy that standard. Thus, proof that defendant intended to travel overseas to commit illegal terrorist acts *is* relevant to the

issue of whether (after he was prevented from traveling) he was predisposed to attempt to detonate a weapon of mass destruction at the Portland tree lighting ceremony in 2010. Both crimes share a common goal to please Allah while physically and psychologically injuring the non-Muslim community. Consequently, the district court's jury instructions on predisposition were correct.

Following these same principles, the court's answer to the jury's mid-deliberation question was also correct, and the court did not abuse its discretion when it refused to clutter its answer with other factors not directly responsive to the question. The jury asked the court to clarify its instruction on predisposition: "Where it states 'the crime,' does that refer strictly to the crime as stated in the indictment, or could it include 'a similar' crime as stated by the prosecution in closing statements." (ER 140; ECF No. 430 at 6).

After discussing the jury's note with counsel, the court answered the jury as follows: "The jury may consider evidence of similar conduct or willingness to engage in similar conduct, along with all the evidence, in deciding if the defendant was predisposed to commit the crime set forth in the indictment. Please review all of Instruction No. 18." (ER 140, ECF No. 430 at 7).[16]

[16] Instruction 18 described the entrapment defense, listed its elements, and reminded the jury that the government bore the burden of disproving entrapment beyond a reasonable doubt. (ER 6218).

Defendant's argument that the court abused its discretion because this statement was legally wrong should be rejected for the reasons just identified. Defendant's further argument that the court abused its discretion because the answer favored the government's view of predisposition and failed to comment upon the kind of predisposition evidence defendant favored should also be rejected. The instruction was a correct statement of the law that favored neither side; its directive to review "all of Instruction No. 18," adequately addressed defendant's concern.

Defendant's other objections to the court's failure to include his additional instructions on wherewithal, claimed "vulnerability," and specific consideration of the influence the government might have had on defendant's predisposition should be rejected because the court's instructions fairly and adequately covered the crime's elements and the defense.

The court told the jury that defendant had raised an entrapment defense (ER 6217) and that the government had "the burden of proving beyond a reasonable doubt that the defendant was not entrapped." (ER 6217–18). The court also provided the jury with Model Instruction 6.2, which directed it to consider five factors including: (1) "the nature of the government's inducement," which necessarily includes the government's contribution to the criminal plan, its admitted critical role in putting the bomb together, and whether and to what extent defendant may have

been influenced or persuaded by the government agents; and (2) "defendant's character and reputation," which encompassed defendant's claimed vulnerability.

When the court's jury instructions required findings that necessarily encompassed defendant's points, the refusal to give additional instructions is not error. *Whittemore,* 776 F.3d at 1080, *citing United States v. Thomas,* 612 F.3d 1107, 1122 (9th Cir. 2010). In addition, no limitation was placed on defendant's ability to argue all of these points to the jury. There was no error and no prejudice to defendant.

Defendant's claim that the court should have included a First Amendment instruction was properly rejected because defendant was not on trial for any of his words or written statements. Instead, his writings and comments were properly introduced as evidence of intent and his predisposition. *Wisconsin v. Mitchell,* 508 U.S. 476, 489 (1993); *United States v. Hassan,* 742 F.3d 104, 127 (4th Cir.), *cert. denied*, 135 S. Ct. 157 (2014). Moreover, the government repeatedly reminded the jury during its closing argument that defendant's First Amendment activity was *not* illegal: "This defendant has an absolute right to write, say, or watch whatever he wants. We are not here because of that." (ER 6227–28). Instead, the government was careful to point out that defendant's writings and other expressions were relevant only to his motive or intent to commit the crime charged, because they "tell you about his willingness and desire to commit an act similar to the one on November 26th of 2010 and tell you much about why that occurred." (ER 6228).

There was also no error or prejudice because defendant countered the government's evidence by relying upon different writings and communications to argue that he lacked motive or intent. Although the First Amendment protected defendant's communications, it did not create a distinct defense to the charge that necessitated a jury instruction. *See, e.g.*, *United States v. Rasheed,* 663 F.2d 843, 848–49 (9th Cir. 1981) (rejecting First Amendment defense to claim that religious beliefs could have shielded fraudulent activity).[17]

Given the nature of the charges and the defense, the district court correctly distinguished *United States v. Freeman,* 761 F.2d 549, 552 (9th Cir. 1985). Freeman was charged with counseling others to violate the tax laws; thus, his speech *was* the crime, and because there was evidence to suggest that defendant's advocacy was too remote from the false returns filed by others, it was error not to instruct the jury that defendant's conduct was protected by the First Amendment. *Id.* at 551.

Because defendant was not on trial for anything that he said or wrote, the district court properly rejected the proffered defense instruction as "irrelevant and confusing." (ER 159). Moreover, the court's instructions adequately covered

[17] In *Hassan,* the trial court included a First Amendment jury instruction in a case involving defendants convicted of conspiring to provide material support to terrorists. That instruction told the jury about the general right of speech and assembly, but it cautioned that the "First Amendment is not a defense to the crimes charged." *Id.* at 128. The Fourth Circuit affirmed the trial court's refusal to give the defense's eleven other proffered instructions on this topic. *Id.*

defendant's concern that he not be convicted based upon his thoughts or words. The court told the jury that defendant was "not on trial for any conduct or offense not charged in the indictment" and he was "not on trial for any opinions or beliefs, whether religious, political, or otherwise, that he may have expressed orally or in writing." (ER 6216). Because the court's instructions adequately and fairly covered defendant's concerns, he fails to establish any error meriting relief.

IV. & IX. The Court Properly Exercised Its Discretion in Discovery Rulings Under the Classified Information Procedures Act.

Standard of Review: A district court's decision to either authorize the government to withhold classified discovery, or to permit the government to substitute unclassified summaries for classified information, is reviewed for abuse of discretion. *United States v. Renzi*, 769 F.3d 731, 750 (9th Cir. 2014) (withholding classified discovery), *cert. denied*, 135 S. Ct. 2889 (2015); *United States v. Dumeisi*, 424 F.3d 566, 578 (7th Cir. 2005) (substitutions). "CIPA vests district courts with wide latitude to deal with thorny problems of national security in the context of criminal proceedings." *United States v. Abu Ali*, 528 F.3d 210, 247 (4th Cir. 2008).

A. Procedural History

The government filed several pleadings concerning classified matters for the court's in camera and ex parte review. Many of the pleadings included requests for orders authorizing the government to withhold classified material from discovery pursuant to Section 4 of the Classified Information Procedures Act, 18 U.S.C. app. 3

(CIPA) and Fed. R. Crim. P. 16(d)(1). These pleadings are all available in the classified record, and much of the government's response to defendant's appellate claims regarding classified materials is addressed in a separately filed classified brief. The manner in which the district court addressed the classified discovery was sound and its substantive rulings on these issues should be affirmed.

The unclassified record includes a series of unclassified orders the district court issued in response to the government's classified submissions. (ER 44–65). In general, the government requested court authorization to withhold from discovery certain classified material that it did not intend to use during the prosecution and which was not both relevant and helpful to the defense. Besides seeking authorization to withhold certain materials from discovery, the government also sought court authorization to give defendant an unclassified substitution for certain classified information that could not be disclosed in its original form without jeopardizing national security. (ER 52–55). The government was separately ordered to provide, and did provide, an unclassified substitution for certain material that the district court had determined was discoverable under the "relevant and helpful" standard. (ER 56–59).

Following an in camera, ex parte review, the district court ultimately granted the government's various motions for CIPA Section 4 orders, providing explanatory orders in both the classified and public records. (ER 52–65). In general, the court

found that (1) disclosure of the classified information could be expected to cause exceptionally grave or serious damage to national security, (2) the materials submitted were not discoverable under either *Brady v. Maryland*, 373 U.S. 83 (1963), or Fed. R. Crim. P. 16, and (3) national security damage from disclosure outweighed defendant's need for the classified information at issue. (ER 52–65).

B. The CIPA Rules

CIPA governs how federal courts address and process pretrial matters concerning the discovery, admissibility, and use of classified information in criminal cases. *See United States v. Sedaghaty*, 728 F.3d 885, 904–05 (9th Cir. 2013). Congress intended that CIPA Section 4 would clarify the court's powers under Fed. R. Crim. P. 16(d)(1) to deny or restrict discovery in order to protect national security. *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988). CIPA's fundamental purpose is to "harmonize a defendant's right to obtain and present exculpatory material" at trial with "the government's right to protect classified material in the national interest." *United States v. Pappas*, 94 F.3d 795, 799 (2d Cir. 1996); *see also Sedaghaty*, 728 F.3d at 904–05 (recognizing CIPA substitution inquiry "arises out of the Constitution's guarantee that all criminal defendants must have a meaningful opportunity to present a complete defense") (internal quotation marks and citations omitted). "The statute was meant to protect and restrict the discovery of classified information in a way that

does not impair the defendant's right to a fair trial." *United States v. Aref*, 533 F.3d 72, 78 (2d Cir. 2008) (internal quotation marks and citation omitted).

1. Classification Is Committed Solely to the Executive Branch

The government has a compelling interest in withholding national security information from unauthorized persons. *Dep't of Navy v. Egan*, 484 U.S. 518, 527 (1988). As the Supreme Court has emphasized, courts should be especially "reluctant to intrude upon the authority of the Executive in . . . national security affairs." *Egan*, 484 U.S. at 530; *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) (protecting the secrecy of our government's foreign intelligence operations is a compelling interest); *CIA v. Sims*, 471 U.S. 159, 168–69 (1985) (the Director of Central Intelligence has very broad authority to protect all sources of intelligence information from disclosure).

2. CIPA Section 4 and Rule 16(d)(1) Permit the Court to Restrict Discovery of Classified Information by the Defense

Section 4 and Rule 16(d)(1) authorize a district court to deny or otherwise restrict defense access to classified information. Section 4 provides, in pertinent part, that a district court, upon a sufficient showing, may authorize the United States to: delete specified classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure; substitute a summary of the information for such classified documents; or substitute a statement admitting relevant facts that the classified information would tend to prove. 18 U.S.C. app. 3, Section 4; *see also* Fed. R. Crim. P. 16(d)(1) (a district court may, for

good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief). While courts have discretion to consider the need for a protective order in any criminal case, CIPA specifically focuses on how courts should exercise that discretion when classified information is at issue. *See, e.g.*, *Sarkissian*, 841 F.2d at 965.

Under Section 4 and Rule 16(d)(1), the court may authorize the Government to withhold entirely from discovery classified materials that are not properly discoverable under the appropriate legal standard. *United States v. Yunis*, 867 F.2d 617, 624–25 (D.C. Cir. 1989). If particular classified materials contain properly discoverable information that should be produced to the defense, Section 4 and Rule 16(d)(1) also permit the court to authorize the government to produce the properly discoverable information in a different form (such as a summary) designed to protect the sensitivity of the national security information. *Sedaghaty*, 728 F.3d at 904–05. So while the Executive Branch may protect classified information from disclosure, CIPA rules give the court discretion to fashion appropriate disclosures when "necessary to the defense and neither merely cumulative, . . . nor speculative." *Abu Ali*, 528 F.3d at 248.

Thus, in cases in which a court has found classified information helpful to the defense, it has permitted production either of redacted versions of the classified documents, *see United States v. Miller*, 874 F.2d 1255, 1277 (9th Cir. 1989), or summaries or substitutions that give the defense the arguably discoverable facts contained in the classified information, without compromising sensitive sources and

methods, *see Dumeisi*, 424 F.3d at 578 (approving substitution of unclassified summary in the place of classified information); *United States v. Moussaoui*, 382 F.3d 453, 479–82 (4th Cir. 2004); *United States v. Rezaq*, 134 F.3d 1121, 1143 (D.C. Cir. 1998).

3. Classified Information that Is Neither Relevant Nor Helpful to the Defense Is Properly Withheld from Discovery.

This Court has held that whether the government must disclose classified information to the defense rests upon the same considerations that govern whether informant identities should be disclosed under *United States v. Roviaro*, 353 U.S. 53 (1957); *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998). In *Roviaro*, the Supreme Court recognized that disclosing a confidential informant's identity involved two fundamental competing interests: (1) the defense's ability to present its case; and (2) the public interest in enabling the government to protect its sources. To address these competing concerns, the Court held that defendant's interest was triggered only when information in the government's possession was relevant and helpful. *Roviaro*, 353 U.S. at 60. If the evidence is relevant and helpful, the court must then balance the public interest in protecting the flow of information against the individual's right to prepare his defense. *Id.* at 62.

Yunis adapted this two-step process to a defendant's bid for access to classified materials as follows: (1) is that information actually relevant and helpful to the defense; and (2) if that threshold is met, is the defendant's desire for the information outweighed by national security interests? *Yunis*, 867 F.2d at 622. The District of

Columbia Circuit recognized that the government had an interest in protecting not only the contents of the conversations but also the sources and methods used to collect them. *Id.* The court noted that the mere fact that certain recordings existed could disclose classified information about the United States intelligence gathering capabilities. *Id.* For example, details revealed in surveillance would make "all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities" from what documents withheld from discovery "revealed about sources and methods." *Id.* at 623.

Thus, when a defendant seeks classified information, the government is not required to disclose that information if: "[n]othing in the classified [information] in fact goes to the innocence of the defendant *vel non*, impeaches any evidence of guilt, or makes more or less probable any fact at issue in establishing any defense to the charges." *Id.* at 624. Application of the *Roviaro* standard reflects an important condition of Executive Order 13,526 for access to classified information, namely that the recipient of the information have a need-to-know classified information that is not favorable or helpful: "inculpatory material which the government does not intend to offer at trial need not be disclosed. Such information cannot conceivably help a defendant, and therefore is both unnecessary and useless to him." *United States v. Rahman*, 870 F. Supp. 47, 52 (S.D.N.Y. 1994).

This Court and others have followed *Yunis* and applied the relevant and helpful threshold for discovering classified information. *See, e.g.*, *Klimavicius-Viloria*, 144 F.3d at 1261; *United States v. Mejia*, 448 F.3d 436, 455–56 (D.C. Cir. 2006); *United States v. Varca*, 896 F.2d 900, 905 (5th Cir. 1990). *See also United States v. Smith*, 780 F.2d 1102, 1109–10 (4th Cir. 1985); *United States v. Pringle*, 751 F.2d 419, 426–27 (1st Cir. 1984).

Even if classified information is relevant and helpful, however, courts do not automatically order disclosure. *Roviaro* required a court to "balanc[e] the public interest in protecting the flow of information against the individual's right to prepare his defense." *Roviaro*, 353 U.S. at 62. Nevertheless, in conducting this review, the trial court "places itself in the shoes of defense counsel" and "acts with a view to their interests." *Sedaghaty*, 728 F.3d at 906 (citations omitted).

The government's interest in protecting national security sources and methods is at least as important as the need to protect law enforcement information at issue in *Roviaro*. Thus, this Court has held that even if a defendant is able to show that information is both relevant and helpful to the defense, overriding national security concerns may, on balance, trump the defendant's need for the information. *Sarkissian*, 841 F.2d at 965.

Congress plainly intended to allow the court to take into account national security interests in considering motions filed under Section 4: "in deciding on whether to permit discovery to be denied, restricted or deferred," a district court

should take into account the need to protect "information vital to the national security." S. Rep. No. 96-823 at 6 (1980), *reprinted in*, 1980 U.S.C.C.A.N. 4294, 4299–4300. Thus, if disclosing evidence obtained from classified sources, although potentially helpful, would harm national security, national security may outweigh a defendant's need for such evidence. Accordingly, CIPA and Rule 16 permit the court to consider the jeopardy that disclosure may bring to important government interests in evaluating whether defendant's need for this information should prevail.

C. The District Court Did Not Abuse Its Discretion by Holding Ex Parte Hearings.

Defendant complains that the court examined the government's CIPA filings in camera and occasionally conducted ex parte hearings with government counsel in connection with those filings, both before and during the trial. Section 4 of CIPA specifically authorizes a court to examine the government's filings ex parte. And this Court rejected, based upon long-standing precedent, a similar broadside challenge to CIPA's ex parte procedures in *Sedaghaty*, 728 F.3d at 908; *see also Aref*, 533 F.3d at 81 (rejecting defendant's challenge to ex parte CIPA procedures).

Although ex parte hearings are generally disfavored, "[i]n a case involving classified documents, however, *ex parte*, *in camera* hearings in which government counsel participates to the exclusion of defense counsel are part of the process that the district court may use in order to decide the relevancy of the information."

Klimavicius-Viloria, 144 F.3d at 1261; *see also United States v. Abu-Jihaad*, 630 F.3d 102, 143 (2d Cir. 2010); *United States v. Campa,* 529 F.3d 980, 995 (11th Cir. 2008).

Access to classified information has two requirements: (1) a security clearance; and (2) a need to know the information. Exec. Order No. 13,526, § 4.1(a)(3), 75 Fed. Reg. 707, 720 (Dec. 29, 2009). Defendant claims that his attorneys, who had security clearances, had a need to know simply by virtue of their representation. (D. Br. 85, n.18). Sedaghaty raised this same argument (Brief of Defendant-Appellant at 126 (No. 11-30342), 2012 WL 1667960 (9th Cir. May 3, 2012), and this Court rejected it. *Sedaghaty*, 728 F.3d at 909. Such a need is not established simply because counsel is representing a defendant. The issue is not, as defendant claims, whether national security interests "trump" a defendant's constitutional right to a fair trial. (D. Br. 84). Rather, a defendant only has a need to know if the court determines that the information sought to be withheld is both relevant and helpful to the defense. Other circuits have also recognized that security-cleared defense counsel are not automatically entitled to access to classified information absent a specific need to know the information. *See, e.g.*, *United States v. Amawi*, 695 F.3d 457, 473 (6th Cir. 2012), *cert. denied*, 133 S. Ct. 1474 (2013); *Campa*, 529 F.3d at 995; *United States v. Bin Laden*, 126 F. Supp. 2d 264, 287 n.27 (S.D.N.Y. 2000), *aff'd*, *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008).

Moreover, the district court was well aware of defendant's trial theories, and it was able to place itself in defense counsel's position as this Court requires. Thus, when the trial court considered the government's CIPA submissions, it did so with a comprehensive understanding of the defense. From the outset of the litigation, and throughout the extensive pretrial litigation, defendant made clear that his theory was that he was a vulnerable teen who had been manipulated by government agents and induced to commit the charged crime. Thus, the trial court remained acutely sensitive to those issues throughout its CIPA review process. Because the law specifically allows such protective measures, and because those measures adequately addressed defendant's interests, the ex parte hearings that the court held regarding the classified filings were not an abuse of discretion.

D. The District Court Did Not Abuse Its Discretion in Protecting the Undercover Employees' Identities.

Prior to trial, the government notified defendant that the two undercover employees' (UCEs) identities were classified and moved for the entry of an order under CIPA deleting their true identities from discovery. (ER 1939–58). After careful review, the district court granted the government's motion. (ER 91–94).

At trial, several protections were instituted to prevent the UCEs' true identities from being released. Defendant agreed with many of those protections. At trial, defendant rigorously cross-examined both UCEs, and much of their interaction with defendant was preserved on videotapes shown to the jury. Defendant fails to identify

any actual prejudice from the court's ruling protecting the UCEs' identities. In sum, defendant had the same type of opportunity to effectively cross-examine the UCEs as was available in *United States v. El-Mezain*, 664 F.3d 467, 493 (5th Cir. 2011).

For example, Youssef was cross-examined extensively about his interactions with defendant: why he gave him food when they met (ER 4410), defendant's unfamiliarity with explosives (ER 4425), directions Youssef gave to defendant about making a "good bye" video (ER 4435–43), and defendant's general lack of sophistication relative to renting an apartment and storage shed (ER 4459–606, 4466–67). Much of Hussein's cross-examination focused on his videotaped interactions with defendant. Hussein was questioned about religious or flattering comments he made to defendant and his explanation that he was attempting to build a "rapport" was thoroughly probed. (ER 4588–90). Hussein confirmed that defendant was incapable of executing the planned bombing on his own. (ER 4648). Defendant used all of this information elicited on cross-examination to support his defense that he was induced by the agents because he was unsophisticated and susceptible to their attention and flattery.

It is pure speculation to suggest that any additional information about the UCEs' identities or backgrounds would have altered the outcome at trial because defendant's best pitch for inducement was fully presented to the jury through the videotaped interactions, the absence of a video recording of their first in-person

meeting, and their email exchanges. The agents' actual identities had no bearing on defendant's inducement theory.

Moreover (as explained in greater detail in the classified brief), the government gave defendant relevant background information about the undercover agents' training and experience (GSER 1–8) and defendant explored this subject only briefly during cross-examination. (ER 4578–80). Defendant did, however, make sure that the jury knew that he knew the UCEs only by their aliases and that he received redacted background information about them. (ER 4576, 4580).

The court protected defendant's constitutional rights by ensuring that the government provided sufficient background information about the undercover employees to permit cross-examination, while limiting that background disclosure to prevent the defense from overtly or indirectly revealing the undercovers' identities. The Confrontation Clause gives a defendant the right to confront and cross-examine the government's witnesses. *See Maryland v. Craig*, 497 U.S. 836, 846 (1990); *Smith v. Illinois*, 390 U.S. 129 (1968). "The rule is that once cross-examination reveals sufficient information to appraise the witnesses' veracity, confrontation demands are satisfied." *United States v. Falsia*, 724 F.2d 1339, 1343 (9th Cir. 1983).

Critically, the Confrontation Clause does not require that a jury hear a witness's true name: "trial judges retain wide latitude insofar as the Confrontation Clause is concerned to impose reasonable limits on such cross-examination based on concerns

about, among other things, harassment, prejudice, confusion of the issues, the witness' safety, or interrogation that is repetitive or only marginally relevant." *Delaware v. Van Arsdall*, 475 U.S. 673, 679 (1986).

This Court has joined other circuits in affirming a district court's discretion to protect witnesses' identities when disclosure would serve little purpose to the defense but could threaten the witnesses' security. *United States v. Cosby*, 500 F.2d 405, 407 (9th Cir. 1974); *United States v. Rangel*, 534 F.2d 147 (9th Cir. 1976). *See also United States v. Palermo*, 410 F.2d 468, 472 (7th Cir. 1969) (citing *United States v. Varelli*, 407 F.2d 735 (7th Cir. 1969)); *Siegfriedt v. Fair*, 982 F.2d 14, 18 (1st Cir. 1992).

Courts have approved alias testimony in a variety of contexts, oftentimes without the detailed witness information the government provided defendant in this case. *See, e.g.*, *United States v. Ramos-Cruz*, 667 F.3d 487, 500–01 (4th Cir. 2012) (affirming use of pseudonyms for El Salvadoran witnesses who feared reprisal from defendant or other sources); *El-Mezain*, 664 F.3d at 492 (affirming trial court's order protecting witnesses' true names classified under Israeli and American law). For example, in *United States v. Abu Marzook, et al.*, the court permitted witnesses from the Israel Security Agency to testify for the government outside of public view and using the pseudonyms by which the defendant knew them. *United States v. Abu Marzook, et al.*, No. 03-cr-978 (N.D. Ill. Aug. 29, 2006) (St. Eve, J.), ECF No. 652 at 2. Similar protective orders were granted in other terrorism cases. *See, e.g.*, Order, *United States v.*

Sheikh, No. 5:13-cr-00305-BO (E.D.N.C. Oct. 6, 2014), ECF No. 67; Order, *United States v. Sami Osmakac*, No. 8:12-cr-00045-MSS-AEP (M.D. Fla. Feb. 12, 2014), ECF No. 217; *United States v. Abu Marzook*, 412 F. Supp. 2d 913, 923–24 (N.D. Ill. 2006).

Defendant rigorously cross-examined the undercover agents. Nothing would have been gained by revealing the agents' true identities, while much could have been lost by doing so. The district court properly balanced the government's interest in protecting its undercover agents against any potential benefit to defendant and appropriately struck the balance in favor of non-disclosure.

E. The District Court Did Not Abuse Its Discretion by Refusing to Compel the Government to Disclose Bill Smith.

"Bill Smith" is the pseudonym of an individual the FBI hired to have limited, online contact with defendant beginning in October 2009. (ER 1653). The district court, in response to defendant's request for information regarding Smith, ordered the government to disclose Smith's true name to defendant, as well as "whatever information you'd want if you were investigating this to determine what involvement Bill Smith had." (ER 1566). Thereafter, the court reversed its earlier position and denied defendant's motion to disclose Smith's identity, relying on the informant's privilege described in *United States v. Henderson*, 241 F.3d 638, 645 (9th Cir. 2000). (ER 20). Defendant filed a Motion for Reconsideration challenging the district court's application of the privilege. (ER 1616–30).

Prior to ruling on defendant's Motion for Reconsideration, the court held an in camera, ex parte hearing with Smith present. (ER 32).[18] Although defendant was not given the opportunity to participate at the actual hearing, the court addressed defendant's concerns by permitting him to file an ex parte submission regarding contact between government actors—including Smith—and defendant. (ER 1477). The court also permitted defendant to submit questions for the court to ask Smith in considering the government's motion at the ex parte hearing. (ER 38).

After listening to Smith's testimony, the court denied defendant's motion. The district court balanced the three factors identified in *United States v. Gil*, 58 F.3d 1414, 1421 (9th Cir. 1995): "(1) the degree [of the informant's] involvement in the criminal activity; (2) how helpful the informant's testimony would be to the defendant; and (3) the government's interest in nondisclosure." *Id.* at 1421. (ER 36–40). The court found: "it is undisputed Bill Smith broke off contact with [defendant] in April 2010 and had no part in the scheme to explode a bomb at the tree lighting ceremony. There is no evidence to the contrary." (ER 38–39).

The district court rejected defendant's argument that the law required Bill Smith's testimony at trial: "Since all of Bill Smith's contacts are through email, and the government produced all the emails to the defense, I do not see how Bill

[18] The September 24, 2012, in camera, ex parte hearing remained unclassified because Smith's true identity was never revealed. In the event Smith's identity was revealed at the hearing, it would have been classified by the government.

Smith's identity or testimony at trial would be helpful to Mohamud, including regarding his entrapment defense." (ER 39). Defendant was free to argue that the Smith emails supported entrapment: "Mohamud can argue any meaning to the jury, including the beginning of an entrapment scheme, which he thinks the emails support. (*Id.*). The court concluded, "without going into any detail, the government established a solid and compelling interest in not disclosing Bill Smith's true identity." (*Id.*).

The defense case was premised on his theory that the government—starting with the Bill Smith emails—induced defendant to commit the crime charged. Smith never met defendant in person, and his sole contacts with defendant were contained within the emails admitted at trial through Agent Dodd's testimony. (Ex. 226). And it was Dodd, not Smith, who supervised the emails' composition. (ER 5185). Dodd testified that he was personally involved in drafting all of the Smith emails, and he explained the thinking behind them. For example, he testified that he used purposefully vague terms to discern defendant's thoughts (ER 5186), he used terms from *Jihad Recollections* to gauge defendant's reaction (ER 5193, 5197–98), and he used "common phrases from chat rooms." (ER 5199–200).

Defendant was able to fully explore this aspect of the investigation through cross-examining Agent Dodd. Dodd read all of the emails into the record and they were admitted as exhibits. (Ex. 226). Dodd confirmed that he knew little about defendant during the email exchange (ER 5247), defendant never tried to meet Smith

(ER 5227), and defendant did not always respond to Smith (ER 5250). Bill Smith's presence at trial would have added nothing to the case.

Moreover, in his closing argument, defendant relied upon the emails' content rather than their provenance to urge the jury to find that defendant was unlawfully induced. It was Agent Dodd, not Smith, who was in the best position to explain both the content and intent of the Smith emails, and thus, the district court did not abuse its discretion by refusing to compel the government to disclose anything further about Bill Smith. (This issue is also addressed in the government's classified brief.)

F. There Was No "Selective Declassification."

The district court carefully reviewed each classified submission under CIPA and *United States v. Klimavicius-Viloria,* 144 F.3d 1249, 1261 (9th Cir. 1998). For the reasons more fully addressed in the government's classified brief, there was no "selective declassification" designed to skew the evidence at trial.

G. The District Court Did Not Abuse Its Discretion in Approving the Government's CIPA 4 Summary.

In addition to deleting specific items of classified discovery, CIPA Section 4 permits a court to authorize the government "to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove." 18 U.S.C. app. 3 § 4. Defendant argues that the district court abused its discretion when it authorized the government to produce a CIPA 4 summary relating to the FBI's assessment that

defendant would not attempt to conduct a terrorist attack without specific direction from the UCEs. (SER 51). Defendant principally relies upon *United States v. Sedaghaty*, 728 F.3d 885, 906 (9th Cir. 2013), to support the proposition that the summary contains deficiencies that render it inadequate and incomplete. (D. Br. 101). Whether a summary is adequate under Section 4 is, however, a case and fact-specific inquiry.

In cases where a court finds that classified information is helpful to the defense, it has permitted the government to produce redacted versions of the documents or summaries. The summary the district court authorized was evenhanded and balanced, and does not exclude information helpful to defendant. While defendant complains that the summary omits crucial, exculpatory information, the facts belie this claim. As can be seen from an examination of the classified record, the summary does not omit any exculpatory information or information otherwise helpful to the defense. Rather the summary contains, critically, facts that give defendant "substantially the same ability to make his defense as would disclosure of the specific classified information." 18 U.S.C. app. 3 § 6(c)(1).

Defendant used the summary extensively in cross-examining the lead case agent. (ER 5357). He read the summary into evidence (twice) (ER 5359, 5361–62), and repeated it again during his closing argument to underscore that he lacked the wherewithal to commit the crime on his own. (ER 6285). Defendant confirmed that Agent Dwyer prepared the summary based upon reports he had reviewed and that the

summary was accurate. (*Id.*). The reports Dwyer referenced were hearsay opinions, not subject to any evidentiary exception that would have permitted their introduction, and not amenable to any claim that they could have yielded otherwise admissible evidence. Defendant gained more traction with the summary than he ever could have achieved with the underlying reports themselves.

V. The District Court Did Not Abuse Its Discretion When Addressing the State of Mind Exception.

Standard of Review: This Court reviews *de novo* whether a district court properly construed a hearsay rule and reviews its decision to admit evidence for an abuse of discretion. *United States v. Washington,* 462 F.3d 1124, 1135 (9th Cir. 2006).

Defendant argues that the district court became hopelessly confused in applying the evidence rules when it permitted government witnesses to explain the investigation's progress, but precluded defendant from offering his own exculpatory statements through other witnesses.[19] The record, however, establishes that the court was not confused and did not abuse its discretion in handling these issues.

The court properly determined that testimony regarding the course of the investigation was not hearsay and was relevant given the nature of the defense. Defendant placed the investigation's integrity directly in issue during his opening

[19] While the court expressed frustration about the state-of-mind arguments at one point (ER 4221–22), it nevertheless made clear that it knew the rules governing hearsay quite well. (ER 5472–81).

statement. Defense counsel told the jury that the FBI targeted and influenced a "teenager who they knew to be conflicted and manipulable." (ER 3944). Defense counsel told the jury, twice, that "the FBI simply went too far." (ER 3978, 4003). He also left the jury with two specific false impressions: first, he told the jury that "teams of FBI agents" had followed defendant and tracked all of his phone and electronic communications, "And what did that surveillance produce? He was studying. He was partying. Nothing about weapons of mass destruction, nothing about attacking in the West, nothing about any interest in doing bad things in his hometown." (ER 3983).

The FBI's surveillance had, however, revealed that defendant was communicating with Al-Ali and attempting to connect with Abdul Hadi. To understand the import of this information, and how it undermined defendant's claim about the surveillance revealing "nothing," the government had to explain why defendant's contacts with Al-Ali raised concerns. It did so through testimony from agents who were aware of the Saudi Arabian Red Notice (Ex. 80) and other evidence, and it did so through Evan Kohlmann's expert testimony. Without the agents' testimony about their reliance on the Red Notice—not for its truth, but to explain why the undercover operation commenced—the jury would have been left with a

misleading and false impression that defendant was targeted because he was young, manipulable and conflicted, or worse, because he had expressed unpopular views.[20]

Second, defense counsel also argued in opening that the FBI should have shut down its investigation when Bill Smith was unable to make any headway with defendant: "The FBI's initial plans with Bill Smith hadn't resulted in Mohamed showing any interest in committing violence. Instead of stopping, another plan developed." (ER 3988–89). The district court did not abuse its discretion when it permitted the government to introduce evidence to rebut the suggestion that the undercover operation commenced because the Bill Smith effort failed; to correct this misimpression, the agents had to explain that it was the Al-Ali emails and defendant's attempts to reach Abdul Hadi that prompted the undercover operation.

The district court fully grasped the relevance of this evidence, and it repeatedly provided the jury with limiting instructions (drafted by the defense) to accompany the agents' testimony and restrict the evidence to its proper purpose. (ER 4092–93, 4280, 4298, 4383–84, 5016, 5115).[21] This Court has recognized that an agent's testimony

---

[20] Defendant claims that the government improperly expanded its reliance upon the 2009 Red Notice (Ex. 80) during its closing argument. (D. Br. 117). Not so: "When the FBI ultimately began their investigation they believed Mr. Al-Ali was, in fact, a wanted terrorist, and that affected their decisions." (ER 6234).

[21] Regarding the Red Notice (Ex. 80), the court instructed: "You heard evidence yesterday relating to an Interpol notice and Amro Al Ali. I instruct you that this evidence is admitted only for the limited purpose of what it means regarding the

(continued . . .)

about the course of an investigation is not testimonial for purposes of the Confrontation Clause, or hearsay under Rule 801(c), because it is not offered for the truth of the matter asserted. *United States v. Wahchumwah,* 710 F.3d 862, 871 (9th Cir. 2012); *United States v. Makhlouta*, 790 F.2d 1400, 1402 (9th Cir. 1986); *see also United States v. Munoz*, 412 F.3d 1043, 1050 (9th Cir. 2005) (affirming admission of agent's reasons for referring defendant to secondary inspection, in part, because it permitted the jury to assess defendant's subsequent behavior); *United States v. Ransfer*, 749 F.3d 914, 925 (11th Cir. 2014); *Hassan,* 742 F.3d at 137 (4th Cir. 2014) (affirming admission of agent's testimony about information received that explained the origins of the investigation); *United States v. Becker*, 230 F.3d 1224, 1236 (10th Cir. 2000); *United States v. Paredes-Rodriguez*, 160 F.3d 49, 57 (1st Cir. 1998).

In this case, whether the Saudis were correct about Al-Ali was irrelevant. What was relevant was two-fold: first, the agents decided to move forward with the undercover operation because defendant's repeated contacts with Al-Ali and Abdul Hadi raised security concerns, and second, information about Al-Ali permitted the jury to assess both why defendant was trying to contact Abdul Hadi and why he would have responded to Youssef's initial inquiry as he did. Because the truth of the Saudi's charge within the Red Notice was irrelevant, the exhibit was not hearsay.

(. . . continued)
agents' and the defendant's mental state; and therefore, you must consider it for that purpose and not for any other purpose." (ER 144, 4280).

This Court's rulings in *Makhlouta* and *United States v. Dean,* 980 F.2d 1286, 1288 (9th Cir. 1992), raise a separate question about whether the information the agents relied upon was relevant under Rule 401. While there is no dispute that entrapment focuses upon a defendant's state of mind, and the agents' state of mind may not be relevant where, for example, it is only relevant to establish probable cause for a search, the agents' testimony about the Red Notice rebutted defendant's claims that the FBI targeted him because he was vulnerable (not because he was perceived as a potential threat to national security) and refuted claims that the FBI had no good reason to continue its investigation after the Bill Smith effort fizzled. Thus, even if an investigator's state of mind is not ordinarily relevant in a case involving entrapment, defendant opened the door and *made* it relevant to this case.

The trial court also did not abuse its discretion in rejecting defendant's converse claim that it erred when it precluded him from introducing through other witnesses his own potentially exculpatory statements under Fed. R. Evid. 803(3)'s state-of-mind exception. A defendant cannot introduce through other witnesses his own exculpatory out-of-court statements because they are hearsay and there is no exception to the hearsay rule that permits their admission. *United States v. Sayakhom*, 186 F.3d 928, 937 (9th Cir.), *amended by* 197 F.3d 959 (9th Cir. 1999).

In any event, the exclusion of the few items defendant identifies was harmless because defendant asked the case agent to read many of his own emails into the

record (ER 5447), he introduced other exhibits reflecting his own state of mind (Ex. 1012), and the court permitted defendant to introduce exculpatory statements he made to a registered nurse after his arrest under the medical diagnosis exception. (ER 5980–81). Defense counsel highlighted these remarks in his opening statement. (ER 4002–03).

VI. The District Court Properly Exercised Its Discretion When It Declined to Rule on Defendant's Fourth Amendment Challenges.

Standard of Review: Pretrial rulings governing trial evidence are reviewed for abuse of discretion. *United States v. Bensimon*, 172 F.3d 1121, 1125 (9th Cir. 1999).

In November 2009, defendant was the subject of a rape investigation by the Oregon State Police (OSP). (ER 71, 75). Defendant was never charged in connection with the investigation. By November 2009, the national security investigation of defendant had already begun. (ER 71–75). FBI agents contacted OSP, observed an interview with defendant without his knowledge, and reviewed the contents of defendant's cell phone and laptop computer. (ER 75–76). Notwithstanding their knowledge of the rape investigation, federal investigators learned nothing in the course of that investigation that assisted the national security investigation. After conducting evidentiary hearings on the issues of possible taint and/or independent source (ER 69–70), the district court specifically found that nothing the FBI learned from the OSP investigation "tended significantly to direct the national security

investigation." (ER 80–82). Instead, most of the information gleaned from OSP was either irrelevant or already known to the FBI. (*Id.*).

The trial court also found that nothing learned from the OSP investigation was used to "guide decisions" relative to the undercover operation. (ER 84). Thus, because the court found no factual link between the federal government's knowledge of the unrelated state investigation and the conduct of the separate national security investigation, the trial court denied defendant's motion to suppress evidence. In particular, the court determined that "any taint ha[d] dissipated" and that "evidence obtained through the national security investigation ha[d] an independent source." The court thus reasoned that there was "no need to address the alleged constitutional violation." (ECF No. 224; ER 69).

Defendant does not challenge any of these factual findings. Instead, he claims that the trial court violated his alleged right to a pretrial determination on the constitutionality of the government's actions relative to the state investigation. Defendant, however, has no right to a pretrial ruling. The district court was well within its discretion when it concluded that further rulings on this topic were unnecessary.

Defendant's argument that he was constitutionally entitled to a ruling on his Fourth Amendment allegations regarding the OSP rape investigation finds no support in the law. This Court has held that a trial court may find attenuation or independent

source without reaching the underlying Fourth Amendment question. *United States v. Crawford*, 372 F.3d 1048, 1053–59 (9th Cir. 2004) (en banc). And the Supreme Court has recognized this same principle in the good faith context. *United States v. Leon*, 468 U.S. 897, 925 (1984); *see also United States v. Craig*, 861 F.2d 818, 820 (5th Cir. 1988) ("Principles of judicial restraint and precedent dictate that in most cases, we should not reach the probable cause issue if a decision on the admissibility of evidence under the good faith exception of *Leon* will resolve the matter.").

To the extent defendant claims that a ruling in his favor on his Fourth Amendment issue would have benefitted him at trial or supported his related motion to dismiss, he offers no support for this novel proposition.[22] Additionally, the rules of evidence do not favor it.

Whether material OSP gathered and shared with federal agents was obtained in violation of the Fourth Amendment has no bearing on whether defendant was predisposed to commit the crime charged and whether the undercover agents unlawfully induced defendant into committing the offense. To suggest that a past

[22] Defendant cites only *United States v. Mazzarella*, 784 F.3d 532 (9th Cir. 2015), but that case is factually distinguishable in several material respects: it involved *Brady* claims and several unresolved disputed factual issues, including whether the government's trial evidence was tainted by an employee working at the government's behest. This case, by contrast, involved evidentiary hearings and fact findings unchallenged on appeal. *Mazzarella* does not stand for the broad proposition that a trial court, after finding the government's investigation was entirely unaffected by an unrelated state investigation, must necessarily decide all other claimed Fourth Amendment issues.

alleged constitutional violation by certain agents might tend to show the inclination of *other* agents to violate defendant's rights is too attenuated and runs afoul of the anti-propensity proscription in Fed. R. Evid. 404, strains relevance under Fed. R. Evid. 401, and it not a theory that would have survived an objection under Fed. R. Evid. 403. *See, e.g.*, *United States v. Williams*, 458 F.3d 312, 317–18 (3d Cir. 2006) (holding that anti-propensity rules apply to the defense and affirming trial court's exclusion of evidence of a government witness's prior bad acts); *United States v. McCourt*, 925 F.2d 1229, 1235 (9th Cir. 1991) (affirming exclusion of 404(b) evidence proffered by the defense for impermissible propensity purpose). The probative value of such evidence, if any, was marginal and introducing this subject would have opened the door to the fact that defendant was a suspect in an unrelated rape case—something both parties wanted to avoid.

VII. & VIII. The District Court Correctly Held that FISA Amendment Act Collection was Consistent with the Fourth Amendment and Applicable Statutes.

A. Introduction and Standard of Review

Defendant contends that the district court erred in denying his motion to suppress evidence derived from the FISA Amendments Act (FAA, or, more specifically, Section 702 of FISA), 50 U.S.C. § 1881a, as well as motions for other relief related to Section 702 surveillance, because collection of his communications under Section 702 violated the Fourth Amendment. In doing so, defendant,

supported by amici (ACLU Br. 12–31), challenges the government's authority to conduct critical foreign intelligence surveillance targeting non-U.S. persons outside the United States pursuant to court-approved procedures Congress authorized. Section 702 was specifically intended to address significant challenges the government faced in collecting foreign intelligence information as a result of sweeping changes in communications technology following the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978.

As explained below, Section 702 lawfully targets non-U.S. persons abroad who lack Fourth Amendment rights. No warrant requirement applies—either to the targeted non-U.S. persons abroad or to third-party U.S. persons who communicate with them, because the collection at issue falls within the foreign intelligence exception to the Warrant Clause of the Fourth Amendment. The collection here also was constitutionally reasonable. The government has interests of the utmost importance in obtaining foreign intelligence information under Section 702 to protect national security. And the collection is governed by court-approved procedures to ensure that only non-U.S. persons outside the United States are targeted and to minimize the acquisition, retention, and dissemination of information in order to protect the privacy of U.S. persons whose communications are incidentally collected.

Denial of defendant's motion to suppress Section 702-derived evidence is reviewed *de novo*. *See, e.g.*, *United States v. Cook,* 797 F.3d 713, 717 (9th Cir. 2015).

B. Background

1. Proceedings Below

On November 29, 2010, the government filed a notice advising defendant that it intended to use in the case "information obtained and derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 ('FISA'), as amended, 50 U.S.C. §§ 1801–1812 and 1821–1829. The statutes cited in the notice permit electronic surveillance and physical search, provided that the government establishes to the satisfaction of the Foreign Intelligence Surveillance Court (FISC) that, among other things, there is probable cause to believe that the target is an agent of a foreign power. *See* 50 U.S.C. §§ 1801, 1804–1805, 1821, 1823–1824.[23] Electronic surveillance under these provisions is commonly referred to as Title I collection, while physical search is commonly referred to as Title III collection.

Before trial, the district court denied defendant's challenges to the government's use of evidence obtained or derived from Title I and Title III FISA collection. (ER 3–18). On November 19, 2013, between trial and sentencing, the government filed a supplemental FISA notification based on the government's then-recent determination that certain evidence referenced in the original FISA

[23] The judges on the FISC are United States District Judges who serve by designation of the Chief Justice of the United States. 50 U.S.C. § 1803(a).

notification, obtained or derived from Title I and Title III collection, was itself also derived from Section 702 collection as to which defendant was aggrieved.

Defendant moved to suppress the Section 702-derived evidence used in this case. After reviewing the relevant material in camera and ex parte, the court denied defendant's motion. (ER 172–227) (*United States v. Mohamud*, 2014 WL 2866749 (D. Or. Jun. 24, 2014). The court found that Section 702 collection was constitutionally reasonable. The court relied in particular on *In re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008), in which the FISA Court of Review held that the Protect America Act (PAA)—a statute similar to the FISA Amendments Act (FAA) that expired in 2008—was reasonable under the Fourth Amendment. *Mohamud*, 2014 WL 2866749, at *20.[24] The court weighed "the government's compelling interest in protecting national security" against "the degree to which § 702 surveillance intrudes" on "the privacy of U.S. persons whose communications are incidentally acquired," and held that the "numerous safeguards built into the statute," including FISC-approved "targeting and minimization procedures," satisfied the Fourth Amendment. *Id.* at *27.

2. The Foreign Intelligence Surveillance Act

In 1978, Congress enacted FISA "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." *See* S. Rep. No. 95-604, at

[24] The FISA Court of Review is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

7 (1977). Before the United States may conduct "electronic surveillance," as defined in FISA, to obtain foreign intelligence information, the government generally must obtain an order from a FISC judge. *See* 50 U.S.C. §§ 1805, 1809(a)(1); *see* 50 U.S.C. §§ 1803(a), 1804(a). To obtain such an order, the government must establish, *inter alia*, probable cause to believe that the "target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the surveillance is directed" (inside or outside the United States) "is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2). The electronic surveillance authorized under such an order must be conducted pursuant to procedures that the FISC judge has determined are reasonably designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublic information concerning unconsenting "United States persons," consistent with the government's need to obtain, produce, and disseminate foreign intelligence information. *See* 50 U.S.C. §§ 1801(h), 1805(a)(3) and (c)(2)(A).

Under FISA as originally enacted, only "electronic surveillance" is subject to the requirement of a judicial order based on probable cause. FISA's original "electronic surveillance" definition did not apply to most of the government's extraterritorial surveillance.[25] This was true even if that surveillance might specifically

[25] In FISA, Congress defined "electronic surveillance" to include four discrete types of domestically focused foreign intelligence collection activities: (1) acquiring *(continued . . .)*

target U.S. persons abroad or incidentally acquire, while targeting third parties abroad, communications to or from U.S. persons or persons located in the United States. *See* S. Rep. No. 95-701, 2d Sess. 7 & n.2, 34-35 & n.16 (1978).[26] At the time of FISA's enactment, the acquisition of international communications did not rely on the four types of "electronic surveillance" defined in the proposed legislation—including wire interceptions executed in the United States—and thus those operations would not be affected by FISA. *See Foreign Intelligence Surveillance Act: Hearing before the Subcomm. on Crim. Laws and Procedures of the S. Judiciary Comm.*, 94th Cong., 2d Sess., at 11 (Mar. 29, 1976 *et seq.*) ("Mar. 29, 1976 FISA Hrg."). Accordingly, Congress understood that most foreign-to-foreign and international communications fell outside the definition of "electronic surveillance." *See* S. Rep. No. 95-701, at 71 ("[T]he legislation does not

---

(. . . continued)
wire or radio communication by "intentionally targeting" a "particular, known United States person who is *in the United States*" in certain circumstances; (2) acquiring wire communication to or from a "person *in the United States*" when the "acquisition occurs in the United States"; (3) intentionally acquiring certain radio communications when the "sender and all intended recipients are located *within the United States*"; and (4) the installation or use of a surveillance device "*in the United States*" for monitoring or to acquire information other than from a wire or radio communication in certain circumstances. 50 U.S.C. § 1801(f) (emphasis added); *cf.* 50 U.S.C. § 1801(i) (defining "United States person" to mean, as to natural persons, a citizen or permanent resident of the United States).

[26] Executive Order No. 12,333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12,333, § 2.2, 3 C.F.R. 210 (1981 Comp.), *reprinted as amended in* 50 U.S.C. § 401 note (Supp. II 2008).

deal with international signals intelligence activities as currently engaged in by the National Security Agency."). Where the government did not intentionally target a particular, known U.S. person in the United States, FISA allowed the government to monitor international communications through radio surveillance, or wire surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework.

3. The FISA Amendments Act

By 2008, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now transmitted principally by fiber optic cables and therefore qualified as wire communications under FISA. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intelligence*, 110th Cong., 1st Sess. 19 (2007) ("FISA Modernization Hrg."), at 19. Once that change occurred, FISA potentially regulated the surveillance of international communications that were previously not covered by the statute, due merely to a change in technology rather than any intentional legislative decision. *Id.*[27]

The government in 2008 thus faced different communications technology and

[27] *Compare* 50 U.S.C. § 1801(f)(2) (defining wire communication as "electronic surveillance" if, *inter alia*, one party is in the United States) *with* 50 U.S.C. § 1801(f)(3) (defining radio communication as "electronic surveillance" only if the sender and all intended recipients are in the United States).

a different terrorist threat and it therefore needed greater flexibility than FISA allowed. The fix needed, as a Department of Justice official stated, was a "technology-neutral" framework for surveilling foreign targets—focused not on "how a communication travels or where it is intercepted," but instead on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." May 1, 2007 FISA Modernization Hrg. at 46 (statement of Asst. Att'y Gen. Kenneth L. Wainstein).

In July 2008, Congress enacted the FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436, which enacted a new Section 702 of FISA.[28] Section 702 (50 U.S.C. § 1881a), "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013).

Under Section 1881a(b), an authorized acquisition must meet each of the following requirements, which are directed at preventing the intentional targeting of U.S. persons or persons located within the United States, or collection of communications known at the time of acquisition to be purely domestic:

(1) The authorized acquisition "may not intentionally target any

[28] In 2012, Congress reauthorized the FAA for an additional five years, until December 31, 2017. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

person known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(1).

(2) It may not intentionally target a person outside the United States "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2).

(3) It "may not intentionally target a United States person reasonably believed to be located outside the United States." 50 U.S.C. § 1881a(b)(3).

(4) It may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. 50 U.S.C. § 1881a(b)(4).

(5) The acquisition must be "conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(5).

Section 702 does not require an individualized court order addressing each non-U.S. person targeted under its provisions. Section 702 instead permits the FISC to approve annual certifications by the Attorney General and Director of National Intelligence (DNI) that authorize the acquisition of certain categories of foreign intelligence information—such as information concerning international terrorism and the acquisition of weapons of mass destruction—through the targeting of non-U.S. persons reasonably believed to be located outside the United States.

4. The Government's Submission to the FISC

Section 702 requires the government to obtain the FISC's approval of (1) the government's certification regarding the proposed collection, and (2) the targeting and minimization procedures to be used in the acquisition. 50 U.S.C. § 1881a(a), (c)(1),

(i)(2), (3); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B). The Attorney General and DNI must certify that

> (1) there are targeting procedures in place, that have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the acquisition is limited to targeting persons reasonably believed to be located outside the United States and to prevent the intentional acquisition of purely domestic communications;
>
> (2) the minimization procedures meet the definition of minimization procedures set forth in Titles I and III of FISA (50 U.S.C. §§ 1801(h), 1821(4)) and have been or will be submitted for approval by the FISC;
>
> (3) guidelines have been adopted by the Attorney General to ensure compliance with the aforementioned limitations set forth in Section 1881a(b) prohibiting, among other things, the targeting of United States persons;
>
> (4) the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment;
>
> (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
>
> (6) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider"; and
>
> (7) the acquisition complies with the limitations in Section 1881a(b).[29]

50 U.S.C. § 1881a(g)(2)(A)(i)–(vii); *see* 50 U.S.C. §§ 1801(h), 1821(4), 1881a(b); *cf.* 50

[29] Those limitations, as described above, generally prevent intentionally targeting United States persons or persons located within the United States or collection of communications known at the time of acquisition to be purely domestic.

U.S.C. §§ 1801(e), 1881(a) (defining "foreign intelligence information").

5. The FISC's Order

The FISC must review the certification, targeting and minimization procedures, and any amendments thereto. 50 U.S.C. § 1881a(i)(1) and (2). If the FISC determines that the certification contains all the required elements and concludes that the targeting and minimization procedures are "consistent with" both the Act and "the [F]ourth [A]mendment," the FISC will issue an order approving the certification and the targeting and minimization procedures. 50 U.S.C. § 1881a(i)(3)(A).

6. Implementing Section 702 Authority

The government acquires communications pursuant to Section 702 through compelled assistance from electronic communications service providers. 50 U.S.C. § 1881a(h). The government identifies to these service providers specific communications facilities, such as email addresses and telephone numbers that the government has assessed, through the application of FISC-approved targeting procedures, are: (1) likely to be used by non-U.S. persons reasonably believed to be located abroad, (2) who possess, communicate, or are likely to receive a type of foreign intelligence information authorized for collection under a FISC-approved certification. The government must identify specific communications facilities, not key words or the names of targeted individuals. *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, ("Section 702

Program Report") 32–33; 41–46 (July 2, 2014).[30]

The FISC has approved authorizations to acquire foreign intelligence information under a series of Section 702 certifications dating back to 2008. The FISC has found that acquisitions under Section 702 fall within the foreign intelligence exception to the Fourth Amendment's warrant requirement because they targeted "persons reasonably believed to be located outside the United States," who are "not protected by the Fourth Amendment," and such targets "will have been assessed by [the government] to possess and/or to be likely to communicate foreign intelligence information." *In re DNI/AG Certification*, No. 702(i)-08-01, Mem. Op. at 35, 37.[31] The FISC has also concluded, after considering in detail the targeting and minimization procedures, that the acquisitions satisfied the Fourth Amendment's reasonableness requirement "in view of the gravity of the government's national security interests and the other safeguards embodied in the targeting and minimization

[30] Available at https://www.pclob.gov/library/702-Report.pdf. The Privacy and Civil Liberties Oversight Board is an independent agency within the Executive Branch. After conducting an in-depth review of the Section 702 program, the Board found that the "core of the Section 702 program—acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court-approved targeting rules and multiple layers of oversight," was reasonable under the Fourth Amendment. Section 702 Program Report at 9.

[31] Available on the DNI's website at http://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

procedures." *Id.* at 38, 41.

7. Oversight

Section 702 requires that the Attorney General and DNI periodically assess the government's compliance with targeting and minimization procedures and relevant compliance guidelines, and that they submit those assessments to the FISC and to Congressional oversight committees. 50 U.S.C. § 1881a(*l*). In addition, at least once every six months, the Attorney General must "fully inform" relevant Congressional oversight committees concerning Section 702's implementation. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.").

C. Acquiring Foreign Intelligence Information Pursuant to Section 702 is Lawful under the Fourth Amendment

1. No Judicial Warrant is Required for Foreign Intelligence Collection Targeted at Foreign Persons Abroad

Defendant argues that collection of his communications under Section 702 required a judicial warrant, either as to the target or as to any third party U.S. persons, such as himself, whose communications were incidentally collected. However, where, as here, the surveillance is lawful as to the target, the fact that others' communications with the target are incidentally collected does not trigger any warrant requirement.

a. The Fourth Amendment Generally Does Not Apply to Non-U.S. Persons Abroad

The Supreme Court has held that the Fourth Amendment does not "apply to activities of the United States directed against aliens in foreign territory." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267, 271 (1990). Based on the Fourth Amendment's text, drafting history, and post-ratification history, *id.* at 265–67, as well as its own precedents, *id.* at 268–71, the Court concluded that the Fourth Amendment was not intended "to restrain the actions of the Federal Government against aliens outside of the United States territory," *id.* at 266. "If there are to be restrictions on searches and seizures which occur incident to such American action," the Court explained, "they must be imposed by the political branches through diplomatic understanding, treaty, or legislation." *Id.* at 275. Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, at least where such persons lack "substantial connections" to this country, the Fourth Amendment does not prevent the government from subjecting them to warrantless surveillance.

Intelligence collection under Section 702 targets non-U.S. persons located outside the United States. Accordingly, under *Verdugo-Urquidez*, the Fourth Amendment generally is inapplicable to persons who are targeted for collection under the statute. Thus, a facial challenge to Section 702 fails because the statute has a "plainly legitimate sweep" in its intended application to persons unprotected by the Fourth Amendment. *See Washington State Grange v. Washington State Republican Party*,

552 U.S. 442, 449 (2008) (citation omitted).

b. Incidental Collection Does Not Require a Warrant

Section 702 does not permit the intentional targeting of U.S. persons or of non-U.S. persons located in the United States. To the extent that the government *incidentally* collects communications of U.S. persons who communicate with Section 702 foreign targets, such "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." *In re Directives*, 551 F.3d at 1015; *see also United States v. White*, 401 U.S. 745, 751–53 (1971) (holding that a conversation recorded with the consent of one participant did not violate another participant's Fourth Amendment rights); *United States v. Kahn*, 415 U.S. 143, 156–57 (1974) (upholding interception of communications of a woman that were incidentally collected pursuant to a criminal wiretap order targeting her husband); *United States v. Martin*, 599 F.2d 880, 884-85 (9th Cir. 1979) (holding that the Fourth Amendment does not require wiretap application to show probable cause that non-targeted individual committed a crime, even where the government expects the wiretap to intercept the individual's conversations with the target), *overruled on other grounds by United States v. De Bright*, 730 F.2d 1255 (9th Cir. 1984) (en banc); *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) (upholding the constitutionality of warrantless surveillance for foreign intelligence purposes even though "conversations . . . of American citizens[] will be overheard"); *United States v. Bin Laden*, 126 F. Supp.

2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").[32]

Under these principles, incidentally capturing a U.S. person's communications during surveillance that lawfully targets non-U.S. persons abroad does not require a judicial warrant or other individualized court order to be reasonable under the Fourth Amendment. *See Bin Laden*, 126 F. Supp. 2d at 281 (noting that "the combination of *Verdugo-Urquidez* and the incidental interception cases" would permit surveillance that collects a U.S. person's communications as an incident to warrantless surveillance targeting a non-U.S. person abroad, so long as the United States person is not a "known and contemplated" surveillance target).

The district court reached the same conclusion in upholding the Section 702 collection in this case. *See Mohamud*, 2014 WL 2866749, at *15.[33] The court's conclusion is particularly appropriate because minimization procedures protect privacy interests of U.S. persons whose communications are incidentally collected. *See In re Directives*, 551 F.3d at 1016 (noting that the minimization procedures under the

---

[32] Amici's contention (ACLU Br. 17) that the incidental collection cases all involved surveillance based on warrants is incorrect—*White* involved surveillance based on consent, *In re Directives* involved warrantless foreign intelligence surveillance pursuant to Section 702's predecessor statute, and *Bin Laden* involved a warrantless search conducted abroad.

[33] Another district court also recently rejected facial and as-applied constitutional challenges to Section 702. *United States v. Muhtorov*, No. 1:12-cr-00033-JLK (D. Colo. Nov. 19, 2015) ECF No. 885.

PAA (FAA's predecessor) "serve[d] . . . as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons").

Defendant and amici do not dispute that incidental collection is lawful in the context of electronic surveillance pursuant to traditional FISA orders or law enforcement wiretaps under Title III of the Wiretap Act, 18 U.S.C. § 2510 *et seq.* ("Title III wiretaps").[34] Rather, they contend that incidentally collecting U.S. persons' communications under Section 702 is unconstitutional because the government expects that some foreign targets will communicate with U.S. persons, and minimization procedures permit the government in certain circumstances to retain those communications. However, the same is true of Title I FISA electronic surveillance and Title III wiretaps. Under those authorities, the government also incidentally collects third party communications, and minimization procedures permit the government to retain those communications in certain circumstances. Moreover, contrary to amici's contention (ACLU Br. 16–17), the fact that one purpose of Section 702 surveillance may be to discover whether the foreign targets are in contact with individuals in the United States does not mean that collection of such communications requires a separate warrant or is constitutionally unreasonable. *See United States v. McKinnon*, 721 F.2d 19, 22–23 (1st Cir. 1983) ("While an interception

[34] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 *et seq.*

that is unanticipated is *a fortiori* incidental, the converse is not true: something does not have to be unanticipated in order to be incidental."). Again, amici's reasoning applies equally to traditional FISA electronic surveillance and to Title III wiretaps, where often one of the goals is to discover the identities, locations, and activities of third parties who may be communicating with the target.

Amici further contend (ACLU Br. 18–19) that because Section 702 incidentally collects more U.S. person communications compared to traditional FISA electronic surveillance or Title III wiretaps, this necessitates an exception to the incidental collection principle. Amici cite no authority suggesting that the lawfulness of incidental collection depends on how extensively the government uses the particular surveillance authority at issue. *See Mohamud*, 2014 WL 2866749, at *15 (holding that, as a "general rule," the "incidental collection of [U.S. person] communications with a [foreign] target" pursuant to Section 702 is "lawful," and rejecting the claim that the potential for incidental collection of large numbers of U.S. person communications warrants an exception to that rule).

Moreover, the premise that traditional FISA surveillance leads to incidental collection of communications of only a "handful" of U.S. persons, compared to Section 702's "tens of thousands or even millions," is unsupported. (ACLU Br. 19).

While there are more targets under Section 702 than under traditional FISA,[35] electronic surveillance, which unlike Section 702 can be used to target U.S. persons and persons in the United States, is likely to capture a significantly larger concentration of non-targeted U.S. persons' communications than Section 702, which targets foreign communications. *See [Caption Redacted]*, 2011 WL 10945618, at *7 (FISC Oct. 3, 2011). Incidentally collecting non-targeted third party communications under Section 702 is reasonable, just as it is under traditional FISA, because the surveillance is lawful as to the target, and no separate warrant is required as to those third parties.

Courts have never recognized a warrant requirement for incidentally intercepted U.S.-person communications during surveillance targeting non-U.S. persons abroad for foreign intelligence purposes. *Cf. In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 169 (2d Cir. 2008) (holding that the warrant requirement does not apply to searches or surveillance of U.S. citizens that occur outside the United States because the original purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters"); *United States v. Barona*, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) (foreign

[35] The government has released information showing that in 2014 there were approximately 90,000 individuals targeted under Section 702, while approximately 1500 individuals were targeted under traditional FISA orders. ODNI's "Statistical Transparency Report Regarding Use of National Security Authorities," available at http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

searches have "neither been historically subject to the warrant procedure, nor could they be as a practical matter").

Moreover, because the government cannot know in advance who the target will communicate with, *see Bin Laden*, 126 F. Supp. 2d at 280 ("[T]he government is often not in a position of omniscience regarding who or what a particular surveillance will record."), requiring a warrant for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection, even though foreign targets lack Fourth Amendment rights and their communications may involve only other foreigners. Such a rule would unduly restrict the government's intelligence collection against foreign targets and degrade its ability to protect against foreign threats.

Defendant's expansive take on the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), is also inapt. (D. Br. 153–55). The Court recognized that an officer's search of a recent arrestee's smartphone bore too little relation to the purposes underpinning the search incident to arrest exception; nothing about the phone's content poses a threat to officer safety and searching the phone does not preserve evidence for later use. By contrast, the government's Section 702 collection involves content that the government already has every right to review, and that content consists of information far more limited than that involved in *Riley* – that is, a non-U.S. person's extraterritorial foreign intelligence communications. And

within that limited scope, the U.S. person's privacy interest is even narrower; only his communications with the foreign target are subject to review under Section 702. Nothing in *Riley* suggests that the government must obtain a warrant as to third-party communicants to retain or access the contents of communications that the government *has already lawfully obtained, accessed, and reviewed* pursuant to surveillance that is lawful as to the target.

Defendants' reliance (D. Br. 152–55) on cases where the government search exceeded the scope of a warrant, consent, or other exception to the warrant requirement is misplaced for the same reason. None of those cases suggest that a search that is otherwise within the scope of a warrant, consent, or other warrant exception becomes unlawful just because it may implicate third party interests.

According to defendant, even if the government lawfully obtained access to the contents of Riley's cell phone (for example through a warrant or consent), it could not access or retain any of the text messages on the phone without obtaining a separate warrant as to each of the third parties who sent or received those messages. Neither *Riley* nor any of the other cases defendant relies on supports such a rule. To the contrary, when communications are lawfully acquired, as they are in the context of Section 702 collection targeting foreigners abroad, the fact that the communications involve third parties (as inevitably they must) does not mean that the government must obtain separate warrants as to each of those third parties.

c. The Search Location Does Not Trigger a Warrant Requirement

Verdugo-Urquidez involved a physical search that was conducted overseas, while collection from service providers under Section 702 takes place within the United States. In the context of electronic communications, however, the fact that the communications of a non-U.S. person outside the United States may be collected from within the United States is not the kind of "significant voluntary connection with the United States" that brings that person within the Fourth Amendment's protection under *Verdugo-Urquidez*. 494 U.S. at 271–72. Otherwise, any foreign person abroad seeking to evade U.S. surveillance could claim Fourth Amendment protection simply by communicating through the facilities of service providers located in the United States. That result would be plainly contrary to the Supreme Court's recognition that the Fourth Amendment protects "the people of the United States" rather than "aliens outside of the United States territory." *Id.* at 266–67.

Moreover, contrary to amici's contention (ACLU Br. 21), when the government collects the communications of a non-U.S. person located abroad, where the collection takes place has no bearing on the person's privacy interests and should not affect the constitutional analysis. When it comes to the content of communications, "the Fourth Amendment protects people, not places." *Katz v. United States*, 389 U.S. 347, 351 (1967)). Accordingly, there is no "constitutional distinction which depends upon the location of the recording apparatus." *United States*

v. Yonn, 702 F.2d 1341, 1347 (11th Cir. 1983).

2. The Foreign Intelligence Exception Applies

Even if the Fourth Amendment were to require, at least in some circumstances, a warrant covering incidentally collected third-party communications, no warrant would be required under Section 702 because surveillance under Section 702 falls within the well-recognized foreign intelligence exception to the warrant requirement.

a. The "Special Needs" Doctrine

The touchstone of the Fourth Amendment is reasonableness, which is assessed by balancing the degree to which a search is needed to promote legitimate governmental interests against the search's intrusion on a person's privacy interests. *See United States v. Knights*, 534 U.S. 112, 118–19 (2001). "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652–53 (1995). But that procedure is by no means inflexibly required. *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (The Fourth Amendment "imposes no irreducible requirement" of individualized suspicion.).

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable,"

Griffin v. Wisconsin, 483 U.S. 868, 873 (1987), such as where the governmental need is especially compelling or especially likely to be frustrated by a warrant requirement, where expectations of privacy are diminished, and where alternative safeguards restrain the government within reasonable limits. *See King*, 133 S. Ct. at 1969. In evaluating whether the "special needs" doctrine applies, the Court distinguishes searches designed to uncover evidence "of ordinary criminal wrongdoing" from those motivated "at [a] programmatic level" by other governmental objectives. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37–40, 48 (2000) (reviewing cases).

b. The Foreign Intelligence Exception

Several appellate courts, including this one, have held by analogy to the "special needs" doctrine, that the government's "special need" for foreign intelligence information justifies an exception to the warrant requirement. *See, e.g., United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); *United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) ("important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement."); *In re Directives*, 551 F.3d at 1010–11 (recognizing "a foreign intelligence exception" to the warrant requirement); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912–13 (4th Cir. 1980); *Butenko*, 494 F.2d at

605; *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973);[36] *but see Zweibon v. Mitchell*, 516 F.2d 594, 618–20 (D.C. Cir. 1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation).[37] Foreign intelligence collection justifies an exception because the "programmatic purpose" of obtaining foreign intelligence information goes "beyond any garden-variety law enforcement objective," and "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011.

Defendant's reliance (Br. 156–57) on *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), is misplaced. The Court in *Keith* expressly reserved the issue of a warrant requirement for foreign intelligence collection. Moreover, *Keith* "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013); *see also In re Sealed Case,* 310 F.3d at 738. The same rationale "applies *a fortiori* to foreign threats," a fact that Congress necessarily recognized in enacting

---

[36] Except for *In re Directives*, these cases involved collection of foreign intelligence information from persons inside the United States. Their reasoning applies *a fortiori* to Section 702 collection, which targets non-U.S. person(s) reasonably believed to be outside the United States.

[37] The plurality in *Zweibon* specifically noted that the surveillance at issue targeted a domestic organization and suggested that its analysis might be different if a foreign power were targeted. *See* 516 F.2d at 651.

FISA. *In re Sealed Case*, 310 F.3d at 738; *see also Truong*, 629 F.2d at 913 ("For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities.").

In addition, unlike Section 702 intelligence collection, the surveillance in *Keith* was targeted at domestic persons with no foreign power connection without a warrant or any judicial or congressional oversight of any kind. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635–37 (1952) (Jackson, J. concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum."). The courts that have addressed the issue of whether foreign intelligence collection is subject to a warrant requirement have expressly distinguished *Keith* in holding that it is not. *In re Directives*, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d at 744; *Truong*, 629 F.2d at 913; *Butenko*, 494 F.2d at 602 n.32; *Brown*, 484 F.2d at 425.

c. The Government's Purpose in Section 702 Collection Goes Beyond Ordinary Crime Control

The government's programmatic purpose in obtaining foreign intelligence information pursuant to Section 702 is not routine law enforcement. *See In re Sealed Case*, 310 F.3d at 717 (holding that the government's "programmatic purpose" in obtaining foreign intelligence information is "to protect the nation against terrorist and espionage threats directed by foreign powers" – "a special need" that

fundamentally differs from "ordinary crime control."); *see also Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (upholding warrantless searches of ferry passengers because "[p]reventing or deterring large-scale terrorist attacks present[s] problems that are distinct from standard law enforcement needs and indeed go well beyond them"). Acquisitions under Section 702 must be conducted with a "significant purpose" to "obtain foreign intelligence information." As the FISA Court of Review found in the context of the PAA (FAA's predecessor), the "stated purpose" of the collection "centers on garnering foreign intelligence," and "[t]here is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes." *In re Directives*, 551 F.3d at 1011.

d. A Warrant or Probable Cause Requirement Would Be Impracticable

As the FISA Court of Review found with respect to the PAA, "there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011. "[A]ttempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" and, therefore, "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations." *Truong*, 629 F.2d at 913. Changes in

technology and the manner of collecting foreign intelligence make timing concerns even more acute; requiring a warrant as to targets or third-party communicants would undermine the vital national security purposes of the collection.

When the government has reason to believe that a non-U.S. person overseas is connected to international terrorist activities, but the government lacks sufficient evidence to establish probable cause that the target is an agent of a foreign power, a warrant requirement could prevent the government from obtaining significant information. Even in circumstances where the government succeeded in eventually gathering enough information to establish probable cause under traditional FISA, the need to develop such information and to obtain FISC approval could result in delays that would hinder the government's ability to monitor fast-moving threats. *See In re Directives*, 551 F.3d at 1011–12 ("[c]ompulsory compliance with the warrant requirement would frustrat[e] the government's ability to collect information in a timely manner"); *cf. Verdugo-Urquidez*, 494 U.S. at 273–74 ("Application of the Fourth Amendment" to aliens abroad could "significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest.").

In short, a warrant requirement would significantly undermine the government's ability to obtain foreign intelligence information vital to the Nation's security. *See Bin Laden*, 126 F. Supp. 2d at 273 ("[T]he imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden" on the

government's ability to obtain foreign intelligence information). That would be a particularly unnecessary result because Section 702 collection does not target persons protected by the Fourth Amendment and the law contains robust safeguards that protect the interests of U.S. persons whose communications are incidentally collected. *See United States v. Abu-Jihaad*, 630 F.3d 102, 121–22 (2d Cir. 2010) ("[T]he Constitution's warrant requirement is flexible, so that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations at issue.") (internal quotation marks and citation omitted).

Finally, although the Fourth Amendment's warrant requirement is based in part on the interest in "interpos[ing] a judicial officer between the zealous police officer ferreting out crime and the subject of the search," *In re Terrorist Bombings*, 552 F.3d at 170 n.7, that concern is considerably diminished in this context because of "the acknowledged wide discretion afforded the executive branch in foreign affairs." *Id.,* as well as the FISC's role in ensuring that Section 702 collection complies with both statutory and Fourth Amendment requirements. *Id.* Contrary to defendant's contention (D. Br. 157), the Fourth Amendment does not require that courts interpose themselves in the Executive Branch's collection of foreign intelligence beyond the procedures provided for by Congress.

e. Section 702 Collection Falls Within the Scope of the Foreign Intelligence Exception

Amici contend (ACLU Br. 21–23) that the foreign intelligence exception is

limited to circumstances where the surveillance was directed at a specific foreign agent or foreign power and was personally approved by the Attorney General. This argument should be rejected.

While *In re Directives* recognized the requirement that surveillance *targeting U.S. persons* under the PAA had to be directed at a specific foreign power or its agent and certified by the Attorney General, the court did not suggest that those requirements are necessary for surveillance targeting *non-U.S. persons* abroad. *See In re Directives*, 551 F.3d at 1012. Indeed, the court specifically upheld the PAA, even though it lacked those requirements for surveillance targeting non-U.S. persons abroad. *See id.* at 1015. Amici's reliance on *Duka*, *In re Sealed Case*, and *Bin Laden*, is equally unavailing because those cases addressed traditional FISA collection or collection targeting a U.S. person.

Although the Attorney General does not personally approve each individual acquisition under Section 702, the Attorney General and DNI jointly authorize the certifications and procedures that govern the acquisition. *See* 50 U.S.C. § 1881a(a). In addition, unlike the unilateral executive branch surveillance in *Truong*, Section 702 collection is governed by stringent, court-approved procedural safeguards and extensive oversight by the FISC and by Congress. *See Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment."). Those requirements provide for extensive authorization and oversight, by all three branches

of government, to fit easily within the foreign intelligence exception.

3. Foreign Intelligence Collection Pursuant to Section 702 Is Reasonable

In circumstances where a warrant and probable cause are not required, searches and seizures are generally subject to the Fourth Amendment's "traditional standards of reasonableness." *Maryland v. King*, 133 S. Ct. at 1970. In assessing whether a search is reasonable, the court must weigh "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Id.* (internal quotation marks and citation omitted). Reasonableness and what safeguards may be necessary in a particular context is determined by balancing the interests at stake in light of "the totality of the circumstances." *Samson v. California*, 547 U.S. 843, 848 (2006); *see also Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 665, 668 (1989) ("neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance" and that "the traditional probable-cause standard may be unhelpful" when the government "seeks to *prevent*" dangers to public safety).

Under the general reasonableness balancing test, searches without a warrant or individualized finding of probable cause are particularly likely to be found reasonable when the governmental need is especially great or especially likely to be frustrated by a warrant requirement, where the search involves modest intrusions on the individual's privacy, and where alternative safeguards restrain the government within reasonable

limits. *See King*, 133 S. Ct. at 1969

In *In re Directives*, the FISA Court of Review upheld the PAA under the general reasonableness test. 551 F.3d at 1012–15. The FISA Court of Review recognized that the government's interest in national security was of such a "high[] order of magnitude" that it would justify significant intrusions on individual privacy. *Id.* at 1012. The court noted further that the PAA, the certifications, and the directives contained a "matrix of safeguards," *id.* at 1013, including "effective minimization procedures" that were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," *id.* at 1015, as well as "targeting procedures" that were "designed to prevent errors" and Executive Branch and congressional oversight of "compliance with the targeting procedures," *id.* The court concluded, based on the panoply of safeguards in the statutory provisions and implementing procedures, that "the surveillances at issue satisfy the Fourth Amendment's reasonableness requirement." *Id.* at 1016.

The FAA provisions, certifications, and procedures at issue in this case, with respect to collection targeting non-U.S. persons overseas, are as protective as, and in some respects significantly more robust than, the comparable PAA procedures that the FISA Court of Review found constitutional. In addition, the FAA goes beyond the PAA by requiring a prior FISC finding that the targeting and minimization procedures are reasonable under the Fourth Amendment. 50 U.S.C. § 1881a(i). The

FAA, unlike the PAA, also expressly prohibits "reverse targeting" of U.S. persons. 50 U.S.C. § 1881a(b)(2). The FAA thus stands on an even firmer constitutional foundation than the PAA, and the FISA Court of Review's analysis upholding the latter applies also to the former.

In addition, the FISC has repeatedly reviewed the targeting and minimization procedures governing the government's acquisition of foreign intelligence information under Section 702 and held that acquisitions pursuant to those procedures satisfy the Fourth Amendment reasonableness standard. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (FISC Oct. 3, 2011).

a. Acquisitions Under Section 702 Advance the Government's Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security

The government's national security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude." *In re Directives*, 551 F.3d at 1012; *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.") (citation omitted). The terrorist threat the United States is facing today "may well involve the most serious threat our country faces." *In re Sealed Case*, 310 F.3d at 746; *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order."). Courts have recognized that the government's compelling interest in collecting foreign intelligence

information to protect the Nation against terrorist groups and other foreign threats may outweigh individual privacy interests. *See, e.g., In re Terrorist Bombings*, 552 F.3d at 172–76 (upholding search and surveillance targeting U.S. person abroad because the intrusion on the individual's privacy was outweighed by the government's "compelling" interest in conducting "sustained and intense" surveillance of foreign terrorist organization).

The collection authorized by Section 702 is crucial to the government's efforts against terrorism and other threats to the United States and its interests abroad. *See* National Security Agency, *The National Security Agency: Missions Authorities, Oversight and Partnerships* 4 (August 9, 2013) ("[C]ollection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."). As the Senate Select Committee on Intelligence found in recommending the FAA's re-authorization in 2012, "the authorities provided under the [FAA] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets." S. Rep. No. 112-174, 112th Cong., 2d Sess. 2 (June 7, 2012); *see also* H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess. 3 (August 2, 2012) ("The importance of the collection of foreign intelligence under the [FAA] . . . cannot be underscored enough. . . . The information collected under this authority is often unique, unavailable from any other source, and regularly provides critically important

insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world.").

Section 702 is a uniquely valuable tool in enabling the government to discover and monitor terrorist networks despite the terrorists' efforts to conceal their activities and communications. Section 702 Program Report at 104–08. Information obtained through Section 702 has played a key role in "the discovery of previously unknown terrorist plots" and has "directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries." *Id.* at 108–09. Thus, as the Executive Branch, Congress, the FISC, and the Section 702 Program Report have all recognized, the government has an extraordinarily compelling interest in collecting information under Section 702.

Amici contend (ACLU Br. 29–31) that Section 702 is unreasonable because the government has "reasonable alternatives" that would achieve the same goals, including obtaining a court order before "accessing Americans' communications" incidentally collected under Section 702. However, the Supreme Court has "repeatedly refus[ed] to declare that only the 'least intrusive' search practicable can be reasonable." *City of Ontario v. Quon*, 560 U.S. 746, 763 (2010). Moreover, the "greater degree of flexibility" Section 702 affords is important because it allows the government to collect foreign intelligence information from foreign targets abroad "without the delay occasioned by the requirement to secure approval from the FISA

court" for accessing a foreign targets specific communications that might also involve U.S. persons. *See* Section 702 Program Report at 106. The warrant requirement suggested by amici would hinder that flexibility and make more difficult the "sustained and intense surveillance" of foreign terrorist groups that is of vital interest to the Nation's safety. *See In re Terrorist Bombings*, 552 F.3d at 175.

b. U.S. Persons Have Limited Privacy Expectations in Electronic Communications With Non-U.S. Persons Outside the United States

The other side of the Fourth Amendment reasonableness balance is the degree to which the search "intrudes upon an individual's privacy." *Knights*, 534 U.S. at 118–19 (citation omitted). In the context of incidental collection, U.S. persons generally have reduced expectations of privacy in information contained within communications that are collected pursuant to surveillance targeting foreigners abroad. Such U.S. persons have no cognizable Fourth Amendment interest in the communications facilities used by the foreign targets of the collection. *See Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (Fourth Amendment rights are personal and may not be asserted vicariously). Moreover, those U.S. persons assume some risk that the foreign intelligence targets with whom they communicate might give the information to others, leave the information freely accessible to others, or that the U.S. government (or a foreign government) will obtain the information. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007).

c. Stringent Safeguards and Procedures Protect U.S. Persons' Privacy Interests

The government employs multiple safeguards to ensure that Section 702 surveillance is targeted at non-U.S. persons located outside the United States for foreign intelligence purposes and to protect the privacy interests of U.S. persons whose communications are incidentally collected.

(1) *Senior officials certify that the government's procedures satisfy statutory requirements*

Section 702 requires the DNI and the Attorney General to certify *inter alia* that a significant purpose of the acquisition is to obtain foreign intelligence information, that the Attorney General and DNI have adopted guidelines to ensure compliance with the statutory limitations in Section 702(b), and that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A). The requirement that these senior executive branch officials certify that the procedures comply with statutory and Constitutional requirements represents an important "internal check" on Executive Branch actions. *See In re Sealed Case*, 310 F.3d at 739.

(2) *Prior Judicial review*

Under Section 702, the government's certification, targeting procedures, and minimization procedures are all subject to FISC review. Section 702 requires the FISC to approve a certification if the court finds that it contains all the required

elements and that the targeting and minimization procedures are consistent with 50 U.S.C. § 1881a(d) and (e) and with the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A). Prior FISC approval, and in particular the required judicial finding that the government's targeting and minimization procedures are consistent with the Fourth Amendment, supports the conclusion that Section 702 collection conducted pursuant to such procedures is constitutional. *See Clapper*, 133 S. Ct. at 1150 (noting the importance of the requirement that the FISC "assess whether the Government's targeting and minimization procedures comport with the Fourth Amendment"). The FISC's declassified opinions make clear that the FISC subjects those procedures to exacting scrutiny. *See, e.g., In re DNI/AG Certification,* No. 702(i)-08-01, Mem. Op. at 32–40; *[Caption Redacted],* 2011 WL 10945618 (FISC Oct. 3, 2011). Moreover, "FISC review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather the Court also examines how the procedures have been and will be implemented." *[Caption Redacted]*, Mem. Op. at 3 (FISC Aug. 26, 2014); *see also id.* at 25 ("[T]he FISC has a continuing role in determining and enforcing compliance with these procedures.").[38]

[38] Available at http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

(3) *Targeting procedures ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States*

Section 702 provides that targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *See* 50 U.S.C. § 1881a(d)(1). The FISC has repeatedly held that collection pursuant to the Section 702 targeting procedures meets these requirements and is reasonable under the Fourth Amendment. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (FISC Oct. 3, 2011); *In re DNI/AG Certification*, No. 702(i)-08-01, Mem. Op. at 39–40 (noting that targeting procedures afford a "reasonable" degree of particularity).

Targeting procedures generally[39] require the government to assess whether the potential target (1) is a non-U.S. person; (2) reasonably believed to be located outside the United States (the "foreignness determination"); and (3) possesses and/or is likely to communicate or receive foreign intelligence information (the "foreign intelligence purpose determination"). Section 702 Program Report at 43. The foreignness

[39] The specific targeting procedures governing collection in this case are classified for reasons of national security. These procedures are part of the classified record available for this Court's review.

determination is based on the totality of the circumstances. *Id.* If there is conflicting information regarding foreignness, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting. *Id.* at 44.

In making the foreign intelligence purpose determination, the government must identify the specific foreign power or foreign territory concerning which the foreign intelligence is being sought. *Id.* at 45. Targeting procedures require documentation of the government's foreignness and foreign intelligence purpose determinations. *Id.* Targeting determinations by government analysts are subject to an internal approval process before the communications facility may be "tasked" for acquisition, and the tasking requests are also subject to oversight review by the Justice Department and the Office of the DNI.

Thus, under targeting procedures, the government must specifically determine that the target is a non-U.S. person reasonably believed to be located outside the United States, the government may obtain communications only relating to specific identifiers, such as an email address or telephone number, and only if the government determines that those identifiers are being used to communicate foreign intelligence information. *Id.* at 41; *see also In re DNI/AG Certification*, No. 702(i)-08-01, Mem. Op. at 41 (holding that "the NSA's assessment under its targeting procedures of the likelihood of obtaining foreign intelligence information provides a reasonable factual

predicate for conducting the acquisitions"). These requirements limit the scope of the acquisition and support the reasonableness of collection under Section 702.

(4) *A significant purpose of the acquisition must be to obtain foreign intelligence information*

Section 702 only authorizes collection when a "significant purpose" of the collection is to "obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). That requirement precludes the government from using directives issued under Section 702 "as a device to investigate wholly unrelated ordinary crimes." *In re Sealed Case*, 310 F.3d at 736. The targeting procedures ensure that any surveillance satisfies this purpose by requiring an assessment that the individual or facility targeted for collection is likely to communicate foreign intelligence information. *See* Section 702 Program Report at 45; *see also In re Directives*, 551 F.3d at 1013 (finding that "procedure[s] t[hat] ensure that a significant purpose of a surveillance is to obtain foreign intelligence information" supported the constitutional reasonableness of the PAA); *Mohamud*, 2014 WL 2866749, at *27 (same as to Section 702).

(5) *Minimization procedures protect a U.S. person's privacy*

The government also employs minimization procedures, as defined in FISA, to limit the acquisition, retention, and dissemination of information concerning U.S.

persons, consistent with the government's foreign intelligence needs.[40] *See* 50 U.S.C. § 1801(h)(1); Section 702 Program Report at 50 ("Minimization procedures are best understood as a set of controls on data to balance privacy and national security interests") Section 702 further requires that the FISC review those procedures and determine that acquisitions in accordance with such procedures are consistent with the statute and the Fourth Amendment. 50 U.S.C. § 1881a(i)(1) and (2). All Section 702-acquired information is subject to the FISC-approved minimization procedures.

Minimization procedures limit how long information concerning U.S. persons can be retained and how it can be disseminated. The procedures require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. *See* Section 702 Program Report at 64–65. As the FISC has held, the minimization procedures ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against the government's intelligence needs. *See In re DNI/AG Certification*, No. 702(i)-08-01, Mem. Op. at 40.

Procedures governing Section 702 collection generally parallel procedures

[40] Declassified minimization procedures used by the NSA, FBI, and CIA are available on the DNI's website at http://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of. The specific minimization procedures governing the Section 702 collection in this case are available in the classified record.

employed for FISA Title I and III collection, as well as the PAA procedures. The FISA Court of Review has found that these procedures sufficiently protect the privacy interests of U.S. persons whose communications are incidentally acquired and that such procedures are an important factor in upholding the constitutional reasonableness of traditional FISA surveillance and the PAA. *In re Sealed Case*, 310 F.3d at 740–41; *see In re Directives*, 551 F.3d at 1015 (finding it "significant" that "effective minimization procedures are in place" to "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.").

The FISC has authority to supervise the government's compliance with minimization procedures. Section 702's oversight provisions require regular reporting to the FISC concerning the government's implementation of minimization procedures. 50 U.S.C. § 1881a(*l*). In addition, Rule 13(b) of the FISC's Rules of Procedures requires the government to report, in writing, all instances of non-compliance. In response to such reports, the FISC has authority to disapprove or to require amendments to the minimization procedures, as, indeed, the FISC has done.[41]

---

[41] In *[Caption Redacted]*, 2011 WL 10945618, at *1 (FISC Oct. 3, 2011), the FISC found that the government's minimization procedures, as applied to certain electronic communications acquired at "upstream" points on the internet backbone networks, did not comply with Section 702 or the Constitution, due to technical limits on the government's ability to isolate targeted communications that were transmitted as part of a multi-communication batch. The government revised its procedures, and

(continued . . .)

The claim by defendant and amici (Def. Br. 154–55; ACLU Br. 27–28) that minimization procedures are inadequate because they permit the government to access and query information already collected pursuant to Section 702 using terms associated with U.S. persons ignores settled case law. Courts have held in various contexts that when the government queries information lawfully obtained, it does not implicate any reasonable expectation of privacy beyond that implicated in the initial collection; running queries or accessing a database does not infringe on any significant privacy interest or trigger any fresh constitutional analysis.

Thus, for example, when the Supreme Court concluded that the State of Maryland had lawfully collected DNA from persons arrested for serious offenses, the state's subsequent analysis of the DNA "did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment. *King,* 133 S. Ct. at 1980; *see also United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151–53 (9th Cir. 2007) (running computer query of lawfully obtained license plate and driver's license identification numbers in government databases, which revealed information about subject's car ownership, driver status, and criminal record, was not a search under the Fourth Amendment); *see also Johnson v. Quander*, 440 F.3d

---

(. . . continued)
the FISC held the amended procedures were consistent with the statute and the Fourth Amendment. *[Caption Redacted]*, 2011 WL 10947772, at *1 (FISC Nov. 30, 2011).

489, 498–99 (D.C. Cir. 2006) (holding that "accessing the records stored in the [DNA] database is not a 'search' for Fourth Amendment purposes"). Notably, the Sixth Circuit has applied this principle in the foreign intelligence context. *Jabara v. Webster*, 691 F.2d 272, 277–79 (6th Cir. 1982) (holding, where plaintiff did not challenge the lawfulness of warrantless NSA interception of his foreign communications, that subsequent dissemination of that information to the FBI "after the messages had lawfully come into the possession of the NSA" did not implicate any reasonable expectation of privacy).

The same reasoning applies here. Where, as here, the government has lawfully collected foreign intelligence information pursuant to statutory requirements and FISC-approved procedures that meet Fourth Amendment standards, the government's subsequent querying of that information does not amount to a significant further intrusion on privacy that implicates the Fourth Amendment. Accordingly, when the government queries (whether using U.S. person identifiers or otherwise) and accesses information lawfully obtained pursuant to Section 702, it is not a separate search under the Fourth Amendment and does not require separate or additional judicial process, as the court below correctly held. *See Mohamud*, 2014 WL 2866749, at *24–26 (holding that, although it is a "close question," the "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth

Amendment"); *Muhtorov*, No. 1:12-cr-00033-JLK, slip. op. at 31 (D. Colo. Nov. 19, 2015) (rejecting defendant's contention that U.S. person queries amounted to a "backdoor search" that required a warrant or rendered Section 702 unconstitutional).

Moreover, U.S.-person information is, by necessity, already subject to review (and use) under the court-approved minimization procedures. Querying lawfully collected information using U.S.-person identifiers does not involve a significant additional intrusion on a person's privacy, beyond that already occasioned by the government's review and use of information lawfully collected under Section 702 pursuant to its need to analyze whether the information should be retained or disseminated.

A U.S. person query, whether for foreign intelligence or a criminal investigation, is not a search that exceeds the original foreign intelligence justification for the collection. Foreign intelligence must be a "signficiant" purpose under Section 702, but it need not be the exclusive purpose. *In re Sealed,* 310 F.3d at 742-43. All of the information queried using a U.S. person identifier falls within the scope of FISC approved foreign intelligence certification. By analogy, if a DEA agent lawfully seizes a drug ledger that also reveals evidence of tax evasion, there is no legal requirement that the IRS obtain a separate warrant to examine the properly seized drug ledger; moreover, the fact that more than one person used the drug ledger also creates no additional requirement that the government seek a warrant or other legal justification

to examine the document. *See, e.g.*, *Maryland v. Garrison,* 480 U.S. 79, 86 (1987) (recognizing that police executing a warrant at a home with multiple residents may search common areas suspect shares with others). In any event, this case involves an investigation of criminal conduct that is closely related to international terrorism, and evidence of such crimes falls squarely within FISA's definition of "foreign intelligence information." *In re Sealed,* 310 F.3d at 724.

On the other side of the balance, the government has a compelling interest in conducting such queries for appropriate purposes. Specifically, the ability to use query terms to more quickly identify foreign intelligence information contained in section 702-acquired information—including, for instance, to learn about the activities of a U.S. person terrorist suspect, to help identify a U.S. person in contact with a foreign intelligence officer, or to search for communications concerning a U.S. person who is the planned victim of an assassination or kidnapping plot—is a critical tool to ensure that the government can effectively "obtain, produce, and disseminate foreign intelligence information." H.R. Rep. No. 95-1283, pt. 1, at 56 (1978). Similarly, the government's interest in preventing crime is "paramount." *Branzburg v. Hayes,* 408 U.S. 665, 700 (1972); *see also* 50 U.S.C. § 1801(h)(3) (requiring minimization procedures to allow retention and dissemination of information that is evidence of a crime); *In re Directives*, 551 F.3d at 1011 ("A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose" because, for example,

the "apprehension of terrorism suspects . . . is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection.").

The FISC has also repeatedly approved minimization procedures that permit queries using U.S. person identifiers. *See [Caption Redacted]*, 2011 WL 10945618, at *7 (FISC Oct. 3, 2011). In approving such queries, the FISC has noted that the minimization procedures the court has approved in connection with other FISA authorities also permit queries using U.S.-person identifiers, even though that information was likely to include a higher concentration of U.S. person information than Section 702 collection. *Id.* The FISC concluded, "[i]t follows that the substantially-similar querying provision found [in] the [Section 702] minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons." *Id.* Likewise, for decades the Federal Wiretap Act's minimization procedures have specifically allowed the government to use evidence from a wiretap to prove a crime unrelated to the original purpose for the wiretap. *See* 18 U.S.C. § 2517(5); *see also, e.g.*, *United States v. Goffer*, 721 F.3d 113, 123 (2d Cir. 2013), *cert. denied*, 135 S. Ct. 63 (2014). In sum, querying information lawfully acquired under Section 702 pursuant to court-approved minimization procedures is reasonable under the Fourth Amendment, as the FISC has repeatedly found.

(6) *Executive Branch, Congressional, and Judicial Oversight*

Section 702 requires the Attorney General and DNI to periodically assess whether the government is complying with the FISC-approved targeting and minimization procedures and relevant compliance guidelines. *See* 50 U.S.C. § 1881a(*l*). They must submit those assessments both to the FISC and to congressional oversight committees. *Id.*; *see also Clapper*, 133 S. Ct. at 1144.

In 2012, the Senate Select Committee on Intelligence, following four years of such oversight, found that

> the government implements the FAA surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied. Through four years of oversight, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law.

S. Rep. No. 174, 112th Cong. 2d Sess. 7 (June 7, 2012); *see also* Section 702 Program Report at 11 ("The Board has seen no trace" of any attempted "exploitation of information acquired under [Section 702] for illegitimate purposes" nor "any attempt to intentionally circumvent legal limits."). Under the FAA, as in traditional FISA, the "in-depth oversight of FISA surveillance by all three branches of government" helps to "ensure[]" the "privacy rights of individuals" and to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent

with both national security and individual rights." *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982).

d. Collection Under Section 702 Has Sufficient Particularity

Defendant's claims that Section 702 collection fails the Fourth Amendment's general reasonableness test because U.S. persons' information may be collected in the absence of a particularized court order or probable cause finding as to either the foreign target or the U.S.-person communicant. In making this argument, defendant and amici describe Section 702-authorized collection as "dragnet" surveillance that collects communications in "bulk." *See, e.g.*, D. Br. 153; ACLU Br. 20. However, collection under Section 702 is *not* bulk collection. *See* Section 702 Program Report at 111 ("[T]he Section 702 program is not based on the indiscriminate collection of information in bulk" because "the program consists entirely of targeting specific persons about whom an individualized determination has been made.").

Section 702 collection is focused and reasonable because FISC-approved procedures require the government to determine (1) that the particular "user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States," *[Caption Redacted],* 2011 WL 10945618, at *7 (FISC Oct. 3, 2011); and (2) the collection is designed to obtain foreign intelligence information within the scope of the certification approved by the court. *See In re DNI/AG Certification*, No. 702(i)-08-01, Mem. Op. at 39 n.47 (finding it "obvious"

that "communications to and from targets identified under these [targeting] procedures would be expected to contain foreign intelligence information"); *[Caption Redacted]*, Mem. Op. at 26 (FISC Aug. 26, 2014) ("While in absolute terms, the scope of acquisitions under Section 702 is substantial, the acquisitions are not conducted in a bulk or indiscriminate manner.").[42]

Moreover, defendant's argument conflates the test for constitutional reasonableness with the *different* requirements for a warrant under the Fourth Amendment. In *In re Directives*, the FISA Court of Review rejected the petitioner's "invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable." 551 F.3d at 1013. Although particularity may be considered as one factor among many in assessing a particular search's reasonableness, the Fourth Amendment "imposes no irreducible requirement" of individualized suspicion where the search is otherwise reasonable, as it is here. *See King*, 133 S. Ct. at 1969. Moreover, the "matrix of safeguards," including robust, court-approved targeting and minimization procedures, protect the same interests that would be served by more exacting particularity or prior judicial review of individual targets. *In re Directives*, 551 F.3d at 1013.

[42] Available at http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf

In enacting Section 702, Congress and the Executive Branch developed a balanced framework of procedures to facilitate foreign intelligence collection vital to the nation's security while protecting constitutionally protected privacy interests. That framework is entitled to the utmost constitutional respect by this Court. *See Sawyer*, 343 U.S. at 635–37 (Jackson, J., concurring); *In re Directives*, 551 F.3d at 1016 ("[W]here the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."). Safeguards built into the statute ensured that the collection in this case targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the privacy of U.S. persons. Evaluating the totality of the circumstances and weighing the compelling governmental interests at stake in combination with the extensive safeguards the government employed to protect the privacy interests of U.S. persons, this Court should hold that the government's Section 702 acquisition of foreign intelligence information in this case is reasonable under the Fourth Amendment.

D. Defendant's Statutory Claims Lack Merit

Defendant also contends (D. Br. 147–51) that the Section 702-derived evidence should be suppressed because the statute prohibits the "retention" or "accessing" of communications of U.S. persons that the government incidentally collects while

targeting foreign persons outside the United States, unless the government obtains a specific court order analogous to a warrant. Defendant does not (and cannot) point to any provision in the statute containing this purported limitation. Rather, he asks this Court to read such a limitation into the statute for two reasons: (1) Congress could not have intended to authorize a departure from the traditional warrant requirement for obtaining U.S.-person communications; and (2) a limiting construction is necessary to avoid serious constitutional problems. Both of those contentions are wrong.

Defendant is incorrect when he asserts (D. Br. 148–50) that it would represent a drastic break with the original FISA statute and the Fourth Amendment to permit the government to collect, retain, and "access" (subject to minimization) incidentally collected third-party communications. Courts have held in a variety of contexts that the Fourth Amendment permits incidental collection of third-party communications without a warrant or probable cause as to the third parties when the surveillance is lawful as to the target. *See In re Directives*, 551 F.3d at 1015; *Kahn*, 415 U.S. at 156–57; *White*, 401 U.S. at 751–53. And that principle applies to surveillance of U.S. persons under the original FISA statute, which contains no prohibition on collection or retention (beyond the applicable minimization procedures) of third-party communications.

Defendant attempts (D. Br. 148) to elide the distinction between surveillance targets and third parties whose communications are incidentally collected by stating that FISA requires a warrant for communications where a U.S. person is "involved." But FISA requires a FISC order only as to the target, not the other persons—whether U.S. persons or foreigners—with whom the target communicates. Defendant cites no authority—whether statute or case law—that has ever imposed a warrant requirement to retain or "access" communications of third parties incidentally collected in the course of foreign intelligence surveillance.

In addition, as noted above (*see infra* Part VIII.B.2), Congress in drafting FISA specifically defined "electronic surveillance" to exclude the vast majority of surveillance the government conducted outside the United States, even if that surveillance might incidentally acquire, while targeting third parties abroad, communications to or from U.S. persons in the United States. *See* S. Rep. No. 95-701, at 7 & n.2, 34–35 & n.16. Defendant's suggestion that the warrant requirement applies in these circumstances is inconsistent with decades of foreign-intelligence collection practice, Congress's intent in enacting FISA and the FAA, and Fourth Amendment case law.

If Congress had intended to impose the limitation defendant proposes, it would have done so explicitly. Section 702 enumerates several specific limitations on collection, *see* 50 U.S.C. § 1881a(b), and defendant's proposed limitation does not

appear in these exclusions. The well-settled principle of statutory construction *expressio unius est exclusio alterius* rebuts defendant's proposed statutory gloss.

More to the point, Section 702 addresses the likelihood that surveillance targeting non-U.S. persons abroad would incidentally acquire the communications of U.S. persons through the requirement that acquisition be conducted in accordance with FISC-approved minimization procedures. Congress could have specified that those procedures impose the warrant requirement that defendant insists Congress intended. Instead, Congress adopted the minimization definition from the original FISA statute, which did not require a warrant but generally required the government to adopt procedures to "minimize" the acquisition and retention of nonpublicly available information about unconsenting U.S. persons, "consistent with the need of the United States to obtain, produce, and disseminate foreign-intelligence information." 50 U.S.C. §§ 1801(h)(1), 1821(4)(A); *see* 50 U.S.C. § 1881a(e)(1). Because Congress adopted that specific, detailed framework for incidentally collected information concerning U.S. persons, rather than the warrant requirement defendant advocates, defendant's contention is flatly inconsistent with congressional intent.

E. The District Court Did Not Abuse Its Discretion in Denying Defendant's Motions for Sanctions and Discovery Related to the Timing of the Section 702 Notice

Defendant contends (D. Br. 137–45) that the district court should have suppressed evidence derived from Section 702, regardless of whether that evidence

was lawfully obtained, to punish the government for not providing notice of Section 702 surveillance until after the trial. At the least, defendant argues, the district court should have granted defendant's requests for discovery and a hearing to support his prosecutorial misconduct allegations. Both of defendant's contentions lack merit.

As the district court recognized, a trial judge may exercise its supervisory power to dismiss an indictment or to suppress evidence in order to "remedy a constitutional or statutory violation; to protect judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; or to deter future illegal conduct." *Mohamud*, 2014 WL 2866749, at *4 (quoting *United States v. Stinson*, 647 F.3d 1196, 1210 (9th Cir. 2011)). Suppression of lawfully obtained evidence is generally a disfavored remedy that should not be imposed in the absence of flagrant misconduct and substantial prejudice to the defendant. *See United States v. Haynes*, 216 F.3d 789, 802 (9th Cir. 2000).

The district court correctly rejected defendant's motion to dismiss the indictment or to suppress evidence. First, the district court correctly found that there was no evidence of prosecutorial misconduct, let alone flagrant misconduct in this case. *Mohamud*, 2014 WL 2866749, at *4. Contrary to defendant's claims, the post-trial filing of the notice did not reflect any bad faith or willful misconduct. Rather, it was the result of a careful review of the range of circumstances in which information obtained or derived from FISA Title I or Title III collection should also be considered

as a matter of law to be derived from prior Section 702 collection, such that the government should give notice of both Title I/III and Section 702 surveillance in those cases. This type of internal review and implementation of remedial measures is not indicative of misconduct.

The district court accordingly found that the circumstances of the government's filing of the notice, including the fact that the government provided notice "without prodding from the court or the defense," amounted to "strong evidence of the lack of prosecutorial misconduct." *Id.* at *4; *see also United States v. Dreyer*, 804 F.3d 1266, 1280 (9th Cir. 2015) (en banc) (rejecting suppression for systemic violation of posse comitatus principles because "the Government should have the opportunity to self-correct before we resort to the exclusionary rule"). The court's conclusion that there was no prosecutorial misconduct alone justified its decision to deny sanctions or further discovery. *See United States v. Armstrong*, 517 U.S. 456, 464, 468–89 (1996) (holding that, because "courts presume that [prosecutors] have properly discharged their official duties," defendants seeking discovery in support of a selective prosecution claim must make a "threshold showing"); *United States v. Arenas-Ortiz*, 339 F.3d 1066, 1069 (9th Cir. 2003) (describing *Armstrong* standard as "rigorous").

In addition, as the district court found, defendant was not substantially prejudiced because the notice enabled him to bring post-trial the same challenges to

the Section 702-derived evidence as he could have raised before trial. *See Mohamud*, 2014 WL 2866749, at *4 (noting that the opportunity to move for suppression after trial "put defendant in the same position he would have been in if the government notified him of the § 702 surveillance at the start of the case").

Moreover, as the district court noted, there is no basis in FISA for automatic suppression of *lawfully acquired* information as a remedy for untimely notice. *See id.* at *3. Rather, the statute contemplates a post-trial motion to suppress "unlawfully acquired" information in circumstances where the defendant lacked the opportunity to make such a motion before the trial. 50 U.S.C. § 1806(e). The automatic suppression rule defendant advocates is not only contrary to the statute but also contravenes the settled principle that, in the Fourth Amendment context, society's interest in deterring unlawful conduct and the jury's interest in receiving all probative evidence are properly balanced "by putting the police in the same, not a worse, position than they would have been in if no police error or misconduct had occurred." *Murray v. United States*, 487 U.S. 533, 537 (1988); *see also Hudson v. Michigan*, 547 U.S. 586, 591 (2006) ("Suppression of evidence, however, has always been our last resort, not our first impulse."); *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) ("For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs."). Nothing in the circumstances of this case suggests that automatic suppression of the Section 702-derived evidence would be necessary or

appropriate. *See Mohamud*, 2014 WL 2866749, at *4 (holding that dismissal of the indictment or suppression of evidence was "not needed as a deterrence" against misconduct related to the Section 702 notice).

Cases defendant cites do not support his position. Although the Fourth Circuit has suggested in *dicta* that exclusion of evidence might be an appropriate remedy when the government provides an outright denial that it has conducted electronic surveillance pursuant to FISA or a law enforcement Title III wiretap, *see In re Grand Jury Subpoena (T-112)*, 597 F.3d 189, 201 (4th Cir. 2010), that remedy is inappropriate here because the government did not deny the existence of FISA collection in this case. The government provided notice of FISA Title I and III collection before trial, and the fact that the Section 702-specific notice for the same evidence was not provided until after trial does not justify the automatic exclusion remedy suggested in *T-112*. *See United States v. Donovan*, 429 U.S. 413, 434 (1977) (failure to comply with Wiretap Act's notice requirement did not warrant suppression in the absence of congressional intent to impose suppression as a sanction for noncompliance).

Defendant's reliance (D. Br. 144) on *United States v. Hernandez-Meza*, 720 F.3d 760 (9th Cir. 2013), is likewise misplaced. In that case, the Court remanded for a determination of whether the government acted willfully in light of the Court's concerns that the government may have deliberately withheld material information from the defendant in order to induce him into presenting a particular defense theory

that the government could then refute using the withheld information. *Id.* at 769. Here, by contrast, the untimely notice of Section 702 collection had no bearing on the fairness or reliability of the trial as a vehicle for adjudicating the defendant's guilt or innocence, because it affected only the defendant's ability to raise a challenge to Section 702 as an additional basis for suppression of FISA evidence. *See Good v. Berghuis*, 729 F.3d 636, 640–41 (6th Cir. 2013), *cert. denied*, 135 S. Ct. 1174 (2015). Because defendant was ultimately not deprived of his opportunity to raise that challenge there is no reason for additional remedies or further discovery.

Nor does this Court's recent decision in *United States v. Mazzarella*, 784 F.3d 532 (9th Cir. 2015), support defendant's request for remand and further discovery. The Court in that case remanded for discovery related to the *merits* of the defendant's Fourth Amendment and *Brady* claims. *See id.* at 542. Nothing in *Mazzarella* suggests that the district court was required to grant defendant's speculative motion for discovery of information that related only to his request for sanctions and had nothing to do with the merits of his challenge to the Section 702-derived evidence.

F. The District Court Properly Withheld the FISA Materials from Defense Counsel

Contrary to defendant's claim (D. Br. 162–64), the district court did not abuse its discretion in denying defendant's motion for disclosure of FISA materials. When a defendant moves to suppress FISA evidence or for disclosure of the FISA applications and orders that produced the evidence, the government may respond by

filing a declaration from the Attorney General stating that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). If the Attorney General files such a declaration, as he did in this case, the district court must review the FISA materials ex parte and in camera and may order disclosure of "portions" of the FISA materials "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance." *Id.* (emphasis added); *see also id.* § 1881e(a) (providing that this same procedure also applies to motions to suppress or disclose Section 702-related material);*United States v. Daoud*, 755 F.3d 479, 481–82 (7th Cir. 2014), *cert. denied*, 135 S. Ct. 1456 (2015); *United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010). A court may order disclosure of portions of the FISA materials only if the court finds that it is incapable of accurately resolving the lawfulness of the collection. *See Daoud*, 755 F.3d at 483.

In light of these requirements, courts have consistently held that "[d]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule." *El-Mezain*, 664 F.3d at 567 (citing *Abu-Jihaad*, 630 F.3d at 129); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) ("The language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary.").

Under these principles, the in camera, ex parte review the district court conducted in this case was the appropriate method to determine whether the Section 702 collection was lawful. The court reasoned that defendant's argument—that disclosure was warranted whenever it would be "helpful" or "appropriate"—was inconsistent with FISA's "necessary" standard. *Mohamud*, 2014 WL 2866749, at *32 (noting that "necessary" in this context is "much closer to 'essential' than to 'helpful'"). The court then specifically found that disclosure was not "necessary" for it "to make an accurate determination of the legality of the surveillance." *Id.* The court noted further that it found "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure." *Id.* (quoting *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987)). This Court should likewise review the classified materials and reach the same conclusion. *See Daoud*, 755 F.3d at 485 ("[o]ur own study of the classified materials has convinced us . . . that their disclosure to the defendant's lawyers is . . . not 'necessary'").

Defendant's contention (D. Br. 164) that this Court should order disclosure of the FISA materials, followed by additional briefing, due to the novelty and complexity of the issues he has raised is inconsistent with the statutory standard. When FISA was enacted, every FISA suppression motion would have raised "novel" issues, yet

Congress mandated that FISA litigation be handled ex parte and in camera, with disclosure being the exception. Courts have been following that procedure for decades. *E.g.*, *El-Mezain*, 664 F.3d at 567. Moreover, the statute requires that courts review FISA applications and orders in camera and ex parte first, before even contemplating disclosure. A court's decision to disclose should arise from that review, rooted in facts from the FISA materials, and not from a defendant's assertion that the issues he raises are novel and complex. *See Daoud*, 755 F.3d at 481-82.

In *Belfield*, the D.C. Circuit squarely rejected a similar attempt to compel disclosure on the ground that the legality of FISA surveillance was "too complex" to be resolved without disclosure and adversary proceedings. 692 F.2d at 147. But the court recognized that arguments relying on the complexity of FISA issues would apply in most cases, and would therefore almost always require disclosure. *Id.* That view, the court held, "cannot be correct" because "[t]he language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary." *Id.*; *see also* Kris & Wilson, *National Security Investigations* § 29:3 n.1 (2d ed. 2012) (noting that "necessary" in this context "means 'essential' or 'required,' and therefore the plain language of that provision makes clear that a court may not disclose . . . unless it cannot determine whether the surveillance was unlawful without the assistance of defense counsel"). Thus, defendant's argument that the alleged novelty and

complexity of his claims requires disclosure conflicts with the plain meaning of the statutory standard governing disclosure, as well as the applicable case law.

G. Section 702 Does Not Violate the First Amendment or Separation of Powers

Defendant contends (D. Br. 156–57) that Section 702 violates the First Amendment and Separation of Powers. Both contentions lack merit.

The Supreme Court and this Court have held that when the government's investigative activities affect individuals' First Amendment interests, those interests are safeguarded by adherence to Fourth Amendment standards. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (requiring only that the Fourth Amendment be applied with "scrupulous exactitude" where First Amendment interests are implicated by a search); *United States v. Mayer*, 503 F.3d 740, 747 (9th Cir. 2007) (The "*Fourth Amendment* provides the relevant benchmark" for a challenge to a criminal investigation on First Amendment grounds.). Accordingly, "surveillance consistent with Fourth Amendment protections in connection with a good faith law enforcement investigation does not violate First Amendment rights, even though it may be directed at communicative or associative activities." *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983); *see Mayer*, 503 F.3d at 750 (explaining that lawful surveillance under the Fourth Amendment does not violate First Amendment rights); *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457, 471 (D.C. Cir. 1991) (same in context of FISA surveillance); *United States v. Aguilar*,

883 F.2d 662, 697 (9th Cir. 1989) (noting that defendant's claim that evidence should be suppressed "is a *Fourth* Amendment claim, rather than a First") (citation omitted); *Abell v. Raines*, 640 F.2d 1085, 1088 (9th Cir. 1981) (rejecting suppression claim based on the First Amendment because "the Fourth Amendment (and the exclusionary rule) provide the only basis" upon which evidence could have been excluded). As explained above, Section 702 collection is reasonable under the Fourth Amendment. And because defendant does not, and cannot, claim that the government has conducted such collection for the purpose of suppressing speech, the collection at issue is also lawful under the First Amendment.

Even if defendant could bring an independent First Amendment claim in this context, defendant's unsupported "chilling effect" argument is foreclosed by the Supreme Court's decision in *Clapper*. In that case, the Supreme Court made clear that individuals cannot establish an unconstitutional "chilling effect" based on allegations that fear of government surveillance under Section 702 deters people from communicating. *See Clapper*, 133 S. Ct. at 1152. As the Court explained, although a regulation need not directly prohibit speech to create a cognizable chilling effect, the Supreme Court has not recognized constitutional violations that allegedly "aris[e] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action

detrimental to that individual." *Id.* Because Section 702 does not "regulate, constrain, or compel any action" by an individual, *id.* at 1153, the mere subjective fear of surveillance under that statute does not amount to a constitutionally significant burden on the exercise of First Amendment rights.

Defendant's contention (D. Br. 156–57) that Section 702 authorizes a "law-making role for judges" that violates the separation-of-powers principle is likewise without merit. As the district court correctly held, "[r]eview of § 702 surveillance applications is as central to the mission of the judiciary as the review of search warrants and wiretap applications." *Mohamud*, 2014 WL 2866749, at *10. And even if the FISC's role was somehow improper, defendant has not explained how the FISC's participation violated *his* rights or would provide a basis for excluding evidence. *See id.* at *11 (explaining that "FISC review of § 702 surveillance submissions provides prior review by a neutral and detached magistrate [which] strengthens, not undermines, Fourth Amendment rights").

H. The Good Faith Exception Applies

The good-faith exception to the exclusionary rule set forth in *United States v. Leon*, 468 U.S. 897 (1984), provides an independent basis for this Court to affirm the district court's denial of defendant's suppression motion. *See, e.g.*, *United States v. Ning Wen*, 477 F.3d 896, 897–98 (7th Cir. 2007) (applying good-faith exception to a claim that FISA surveillance violated the Fourth Amendment). That exception applies

when government agents act in "objectively reasonable reliance on a statute" authorizing warrantless searches that is later deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 349–50 (1987), when law enforcement officers reasonably rely on the probable-cause determination of a neutral magistrate, *see Leon*, 468 U.S. at 920, and when law enforcement officers reasonably rely on then-binding appellate precedent that is subsequently overturned, *see Davis v. United States*, 131 S. Ct. 2419, 2434 (2011).

As the district court held, *see Mohamud*, 2014 WL 2866749, at *30, the good-faith exception applies here because the collection at issue was authorized by a duly enacted statute, an order issued by a neutral magistrate, and court of appeals precedent. First, government agents conducted the collection at issue pursuant to Section 702 and procedures adopted by the Attorney General pursuant to the statute. *See Krull*, 480 U.S. at 349; *Duka*, 671 F.3d at 346 (the good-faith rule applies because the search "was conducted in objectively reasonable reliance on a duly authorized statute [FISA]"). Second, government agents also reasonably relied on orders issued by neutral magistrates—the FISC judges—who have repeatedly held that the applicable Section 702 targeting and minimization procedures implemented pursuant to Section 702 are reasonable under the Fourth Amendment. *See Leon*, 468 U.S. at 920; *Duka*, 671 F.3d at 347 n.12. Finally, the agents reasonably relied on FISA Court of Review precedent that upheld similar directives issued under the PAA. *See Davis*, 131 S. Ct. at 2433-34; *In re Directives*, 551 F.3d at 1016.

Defendant advances (D. Br. 165–66) three reasons that, in his view, prevent application of the good-faith exception here. Not one of those reasons is a valid basis to disregard the good faith exception. First, defendant's argument (D. Br. 165) that the Court should not apply the good-faith rule in order to ensure that criminal defendants have an incentive to challenge Section 702 is foreclosed by the Supreme Court's decision in *Davis*. *See* 131 S. Ct. at 2432-33 (holding that providing incentives for criminal defendants to advance novel Fourth Amendment claims is "not a relevant consideration" in determining whether to apply the exclusionary rule).

Second, defendant argues that the exception does not apply here because Section 702 does not explicitly authorize the retention of incidentally collected communications of U.S. persons. Defendant's interpretation of the statute is wrong, *see* Part [VIII-D above]). Even if it were correct, however, defendant cannot show that the contrary construction of Section 702 by the FISC, which has repeatedly found that minimization procedures that authorize retention of such communications in certain circumstances were consistent with Section 702 and the Fourth Amendment, was so manifestly wrong that a reasonable officer should have known that collection pursuant to the court-approved procedures was unlawful. *See Krull*, 480 U.S. at 349.

Finally, defendant argues that FISA's statutory suppression remedy does not incorporate good-faith principles. However, in the related context of Title III of the

Wiretap Act, the weight of the precedent establishes that Title III's statutory suppression remedy for criminal wiretap orders incorporates the good-faith exception. *See United States v. Moore*, 41 F.3d 370, 374, 376 (8th Cir. 1994) (applying good-faith exception to Title III violation); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988)(same); *United States v. Brewer*, 204 F. App'x 205 (4th Cir. 2006)(unpublished) (same); *United States v. Solomonyan*, 451 F. Supp. 2d 626, 637–38 (S.D.N.Y. 2006) (collecting cases). Although two federal appellate courts have reached the opposite conclusion, both courts also questioned in those cases whether the government's actions were actually taken in "good faith," either because the affiant recklessly misled the court, *see United States v. Rice*, 478 F.3d 704, 709–11 (6th Cir. 2007), or because the wiretap order, in the court's view, plainly violated the applicable rule, *see United States v. Glover*, 736 F.3d 509, 515–16 (D.C. Cir. 2013).

In this case, even if defendant could demonstrate (and he cannot) that the collection did not comply with Section 702, there is no deliberate, reckless, or systemically negligent conduct by the agents who conducted the collection. The district court's denial of defendant's motion to suppress should be affirmed.

X. The District Court did not Abuse its Discretion or Err in Imposing Defendant's Sentence.

Standard of Review: Whether a district court adequately explained its reasoning in imposing a sentence, in the absence of a timely objection, is reviewed for plain error. *United States v. Valencia-Barragan*, 608 F.3d 1103, 1108 (9th Cir. 2010).

Review of all federal sentences is under a deferential abuse of discretion standard. *Gall v. United States*, 552 U.S. 38, 49 (2007); *United States v. Carty*, 520 F.3d 984, 988 (9th Cir. 2008) (en banc). Because of this deferential standard of review, reversals will be warranted only in "rare cases." *United States v. Ressam*, 679 F.3d 1069, 1087–88 (9th Cir. 2012) (en banc).

There was no dispute at sentencing that the applicable Guideline range before any departures was correctly calculated in the Presentence Investigation Report (PSR) to be life in prison. (ER 3637, SER 381). The government nevertheless recommended a 40-year sentence (ER 3638), while defendant sought a prison term of no more than 10 years.

At sentencing, the judge said that he had reviewed the parties' written submissions, adopted the uncontested Guidelines calculation in the PSR, and announced his intention to vary from the Guideline sentence under 18 U.S.C. § 3553. (ER 3636–38; SER 475–76). The court then heard a brief statement from a prosecutor, followed by arguments from three different lawyers for defendant and statements from both defendant's parents and his sister. (ER 3664–72).

The court next identified factors favoring a lower sentence than life, including defendant's letter, "renouncing his actions and past belief in violent extremism," and imperfect entrapment: "The Court realizes the agents often reminded the defendant he could back out of the plan if he had a change of heart, but that is balanced by the

Government's inducement through the agent's use of praise and religious references." (ER 3684–85). The district court also considered as mitigating factors defendant's age, his lack of criminal history, and testimony by defense psychologists. (ER 3685).

Tracking the sentencing statute (18 U.S.C. § 3553(a)), the court considered the need to avoid unwarranted sentencing disparities with similar cases, and it highlighted several aggravating factors. First was the contemplated crime's "horrific" nature: "The defendant expected at least 10,000 people, including many children, in the square. He wanted everyone to leave either dead or injured." (ER 3686–87). Next, the court cited defendant's resolve despite warnings about the consequences of his plan: "He expressed his goal of causing as much damage as he could. He pushed the buttons actuating the bomb twice. He had a commitment to his plan and never once expressed any change of heart, even though the agents gave him many opportunities to back out." (ER 3686).

The court also emphasized that defendant was the plan's architect: "The Christmas tree bombing was the defendant's idea. The Government agents were not familiar with the—with this community event prior to defendant's suggestion." Moreover, defendant developed his proposal quickly: "Only 13 minutes into the first meeting, Youssef asked the defendant what he would do, quote, for the cause, end quote. When the defendant said he could do anything, Youssef presented five choices, which included two innocuous ones, and the defendant chose becoming

operational and explained he wanted to put an explosion together and had heard of brothers building and detonating car bombs." (ER 3686).

Finally, the court recognized defendant's long-standing commitment to his cause and the particular concerns associated with terrorism and recidivism:

> The defendant became radicalized at age 15. He began e-mailing Samir Khan extensively and writing for *Jihad Recollections* at age 17, while he was a high school senior.
>
> The Ninth Circuit recognizes—this is the next point. *The Ninth Circuit recognizes that terrorists, even those with no prior criminal behavior, are unique among criminals in the likelihood of recidivism, the difficulty of rehabilitation, and the need for incapacitation.*

(ER 3687)(emphases added). After hearing from defendant, the judge commented, "this is a sad case." (ER 3688). He then sentenced defendant to 30 years, followed by a life term of supervised release. (ER 3689). Defendant raised no contemporaneous objection to the manner in which his sentence was imposed. (ER 3693).

Nevertheless, defendant now accuses the government of tempering its recommendation for a downward variance on an "improper basis" and complains the district court failed both to "resolve controverted issues" and adequately to explain the sentence it ultimately imposed. These claims are meritless.

A. & B. See Sealed Supplement Answering Brief

/////

C. The District Court Properly Selected and Adequately Explained Defendant's Below-Guideline Sentence.

Defendant argues that the district court procedurally erred in imposing his sentence because it failed to resolve the issue of his future dangerousness on an individualized basis and failed to adequately explain its reasons for rejecting his demand for a departure from the terrorism guideline's criminal-history enhancement under USSG § 4A1.3. (D. Br. 172–78). As recounted above, however, the record confirms that the court thoroughly considered all of the parties' arguments and clearly explained its reasoning in selecting the 30-year sentence.

1. The Court Expressly Considered the Evidence Bearing on Defendant's Individualized Risk of Future Dangerousness.

Defendant faults the district court first for failing to afford "individualized consideration" to the evidence he presented pertaining to his "sincere remorse, his post-offense rehabilitation, his . . . renunciation of violence, and the psychiatric reports [indicating] he was a low risk for future dangerousness." (D. Br. 172–73). According to defendant, the court effectively disregarded that evidence in favor of "an almost irrebuttable presumption of a high risk of future dangerousness" (D. Br. 173–74) by misapplying this Court's decision in *Ressam*.

The record compels the opposite conclusion. The district court, both at the sentencing hearing and in its written statement of reasons, made clear that it considered defendant's evidence about his purported lack of future dangerousness.

(ER 3684–87; SER 476). In fact, the court credited most of this evidence at the sentencing hearing, specifically highlighting that defendant had:

(1) Written a letter shortly after his arrest "renouncing his actions and past belief in violent extremism";

(2) Written another letter of remorse in anticipation of sentencing, which the court noted might "reflect[] a true change of heart";

(3) Established factors favoring mitigation by way of "imperfect entrapment" in light of the FBI "agents' use of praise and religious references";

(4) Demonstrated that his "young age made him more vulnerable to suggestion"; and

(5) Introduced competent evidence from "[t]wo psychologists [who] believed that he present[ed] a low risk of future crimes."

(ER 3684–85). The court also noted that defendant's lack of prior criminal conduct "weigh[ed] in his favor," despite the terrorism enhancement's Criminal History Category VI. (ER 3685).

Defendant protests that the court should have given these factors more weight—a supposed error defendant attributes to the district court's alleged misunderstanding of *Ressam*. In that case, this Court adopted the Second Circuit's oft-cited holding that: "'Terrorists, *even those with no prior criminal behavior*, are unique among criminals in the likelihood of recidivism, the difficulty of rehabilitation, and the need for incapacitation." *Ressam*, 679 F.3d at 1091 (quoting *United States v. Jayyousi*, 657 F.3d 1085, 1117 (11th Cir. 2011) (quoting *United States v. Meskini*, 319 F.3d 88, 92 (2d Cir.

2003) (rejecting challenge to USSG Terrorism enhancement)) (emphasis added); *cf.* *United States v. Ali*, 799 F.3d 1008, 1031 (8th Cir. 2015) (quoting *Meskini*).

Not even defendant disputes this uncontroversial proposition as a general matter. He claims, however, that it blinded the district court to the specifics of his individual case: that it was taken to create an "irrebuttable presumption" about all terrorism defendants. (D. Br. 174). The record clearly belies this characterization of the district court's reasoning, which weighed defendant's mitigating facts and arguments along with the case's aggravating facts. The court thus emphasized that defendant:

> (1) had been radicalized at age 15 (years before any contact with government agents);
>
> (2) began e-mailing Samir Khan and writing for *Jihad Recollections* at age 17;
>
> (3) came up with the "horrific" plan to slaughter civilians at the Christmas Tree lighting ceremony all on his own;
>
> (4) attempted to wreak "a great deal of death and mutilation," hoping that "at least 10,000 people, including many children," would "leave either dead or injured";
>
> (5) tried to detonate the bomb not once but twice; and
>
> (6) "never once expressed any change of heart, even though the agents gave him many opportunities to back out."

(ER 3686–87). It was only after recounting these *individualized* factors that the court finally noted this Court's cautionary observation about the need to incapacitate

convicted terrorists in *Ressam*. (ER 3687). Defendant cannot credibly maintain that the district court's weighing of a dozen distinct, individualized factors was really nothing more than blind application of an "irrebuttable presumption" derived from *Ressam*. It self-evidently was not.

2. The District Court Explicitly Resolved Defendant's Request for a Departure from the Terrorism Enhancement.

Defendant also complains that the district court did not "provide a sufficient record regarding the reasons for rejecting the claim that the terrorism enhancement was over-representative under USSG § 4A1.3." (D. Br. 176). This contention must fail for the same reason as the last. It simply ignores all of the factors that the district court expressly considered in determining that there was a "likelihood that the defendant w[ould] commit other crimes" that was not "substantially over-represented," USSG § 4A1.3(b)(1), by his placement in Criminal History Category VI.

This Court has repeatedly held that a sentencing court need not discuss the parties' arguments and the § 3553(a) factors at length in imposing a sentence. *See, e.g.*, *United States v. Chhun*, 744 F.3d 1110, 1123 (9th Cir.), *cert. denied*, 135 S. Ct. 131 (2014). It will suffice if the court only "implicitly addresse[s]" a defendant's arguments by "noting" countervailing considerations. *See id.* 1123–24. "If the record 'makes clear that the sentencing judge listened to each argument' and 'considered the supporting evidence,' the district court's statement of reasons for the sentence, although brief,

will be 'legally sufficient.'" *United States v. Sandoval-Orellana*, 714 F.3d 1174, 1181 (9th Cir. 2013) (quoting *Rita v. United States*, 551 U.S. 338, 358 (2007)).

The district court discussed the factors exacerbating defendant's risk of future dangerousness in substantial detail. In the context of this discussion, the court's statement that it was "not persuaded by defendant's argument to reject the terrorism enhancement" was no error at all—much less plain error.

CONCLUSION

The district court's judgment should be affirmed.

DATED this 7th day of December 2015.

Respectfully submitted,

BILLY J. WILLIAMS
Acting United States Attorney
District of Oregon

s/ Kelly A. Zusman
KELLY A. ZUSMAN

s/ Ethan K. Knight
ETHAN D. KNIGHT

s/Pamala R. Holsinger
PAMALA R. HOLSINGER

s/Ryan W. Bounds
RYAN W. BOUNDS
Assistant U.S. Attorneys

JOHN P. CARLIN
Assistant Attorney General
National Security Division

s/Joseph F. Palmer
JOSEPH F. PALMER
Attorney, Appellate Unit
National Security Division
U.S. Department Of Justice

STATEMENT OF RELATED CASES

Pursuant to 9th Cir. R. 28-2.6, the United States represents that it knows of no cases related to this appeal.

CERTIFICATE OF COMPLIANCE
Circuit Rule 32(a)(7)(C)

Pursuant to Ninth Circuit Rule 32(a)(7)(C), I certify that the government's brief is submitted with an amended motion for leave to file an oversized brief pursuant to Circuit Rule 32-2. The unsealed public brief is 164 pages in length, excluding the portions exempted by Fed. R. App. P. 32(a)(7)(B)(iii). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

s/ Kelly A. Zusman
KELLY A. ZUSMAN
Assistant U.S. Attorney