No. 15-4111

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

ALI SABOONCHI,

Appellant.

Appeal from the United States District Court for the
District of Maryland, Southern Division
Honorable Paul W. Grimm, District Judge

BRIEF OF APPELLEE
UNITED STATES OF AMERICA

Rod J. Rosenstein
United States Attorney

Christine Manuelian
Assistant United States Attorney

Sujit Raman
Chief of Appeals

36 South Charles Street
Baltimore, Maryland 21201
(410) 209-4800

November 18, 2015

Attorneys for the Appellee

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Regulations

Other Authorities

STATEMENT OF JURISDICTION

The district court (Paul W. Grimm, J.) had jurisdiction over this federal criminal case pursuant to 18 U.S.C. § 3231. This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF THE ISSUES

I. Whether the government's forensic search of the defendant's electronic media detained at the border constituted a valid warrantless border search?

II. Whether the district court properly instructed the jury that in order to find the defendant guilty of unlawfully exporting goods to Iran, it had to find that the defendant acted with knowledge that his conduct was unlawful.

STATEMENT OF THE CASE

On March 4, 2013, following a joint investigation by the Federal Bureau of Investigation (FBI) and United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI), the defendant, a dual citizen of the United States and Iran, was indicted by a federal grand jury on conspiracy and substantive charges relating to his unlawful export of goods and services to Iran. He was arrested on March 7, 2013. JA 7. The indictment was subsequently superseded on August 23, 2013 (JA 12), and again on December 12, 2013 (JA 15). The second

superseding indictment, the operative charging document at trial, alleged the following crimes by the defendant (and his three named co-defendants located in Iran): conspiracy to unlawfully export goods and services to Iran (Count One), six substantive counts of unlawfully exporting goods to Iran (Counts Two through Seven), and one substantive count of attempting to unlawfully export goods to Iran (Count Eight), all in violation of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1702 and 1705, and the Iranian Transactions and Sanctions Regulations (ITSR), 31 C.F.R. §§ 560.203 and 560.204. JA 29-53.

The defendant filed numerous pre-trial motions through multiple counsel, which were the subject of two hearings and extensive briefing. In various oral rulings, written orders, and two subsequently published opinions (referenced below), the district court denied all of the defendant's substantive motions. JA 9-21, 145-209, 334-89, 421-99, 608-15.

Trial commenced on July 28, 2014, and concluded on August 11, 2014, with the return of guilty verdicts on all counts. JA 21-22. The defendant subsequently filed a motion for judgment of acquittal, which the district court denied on January 28, 2015. JA 23-24. Sentencing occurred on February 2, 2015, and the court sentenced the defendant to concurrent 24-month terms of imprisonment on each

count. JA 2774-96. Judgment was entered on February 11, 2015, and the defendant filed a timely notice of appeal on February 24, 2015. JA 25.

STATEMENT OF FACTS

The government's evidence at trial established that during the period from September 2009 through March 2013, the defendant purchased, attempted to purchase, or facilitated the purchase of, various United States-origin industrial parts and components for export to Iran, in violation of the Iran Trade Embargo. This evidence consisted of hundreds of electronic communications, seized pursuant to multiple warrants, between the defendant, his criminal associates, and the United States manufacturers/suppliers from which products were sought or obtained. (Many of the email/chat communications between the defendant and his co-conspirators were in Farsi; the English translations were admitted into evidence through the testimony of a certified FBI linguist). The seized emails, electronic chats, and emailed documents were corroborated by business records from the affected United States companies and the testimony of certain company representatives.

In total, the evidence revealed that upon receiving requests from his Iranian associates, either through email, electronic chat, or other means, the defendant would obtain price-quotes for, order, and purchase the goods sought, and then

either personally export the items, or arrange their export, to Iran by way of Dubai, United Arab Emirates, or China. He ordered and purchased the components under the name of Ace Electric, a company he registered in Maryland for the sole purpose of making it appear as though he were obtaining items for domestic use. He took delivery of the items at various locations in Maryland, where he or his friends resided. In order to acquire the products, he provided false information to the United States manufacturers/suppliers regarding the true end-use and destination of the items sought. He also falsely identified on invoices and shipping documents the true value of the exported goods and their ultimate destination. Once the exported items arrived in Dubai or China, the defendant's co-conspirators arranged for their subsequent shipment to Iran. In a few instances, the defendant's role was limited to providing payment to the relevant United States manufacturer/supplier for the items ordered by his co-conspirators. He was compensated for his time and the cost of the items he obtained for export by the transfer of funds from his associates through money couriers or wire transfers into Iranian or American bank accounts he and his wife maintained.

The products sought or obtained by the defendant for export to Iran were industrial parts and components used in the oil, gas, energy, aerospace, defense, steel, and nuclear industries, and in medical environments. These products

included: an industrial camera system for use in steel processing (attempted purchase for export); industrial electronic components (attempted purchase for export); cyclone separators used in industrial pipelines to separate impurities (exported); thermocouples used to measure liquid temperatures of chemicals and petrochemicals (exported); bypass filters used in industrial filtering systems (exported); flow meters used to measure water, gasses or other liquids (exported); springs for actuators used to control liquid flow rates (exported); hydraulic valves and connectors and other parts used in industrial motion control and fluid handling (exported); industrial gas analyser components (attempted purchase for export); industrial pumps and valves (exported); industrial LCD modules (exported); carbide end mills (exported); a turboexpander used for nitrogen gas processing (attempted purchase for export); and radioiodine air-sampling cartridges (attempted export).

The specific way in which each transaction was undertaken and completed was established through the chronological progression of the defendant's electronic communications with his co-defendants and other co-conspirators, and with each of the relevant United States product manufacturers/suppliers. JA 1312-1533, 1560-1770, 1775-1819, 1845-85 (admission of electronic communications and

business records through testimony of FBI case agent); JA 824-40, 869-89, 902-03, 905-22, 923-50, 972-1003, 1147-65 (testimony of company representatives).

The defendant's willful intent to violate export laws was established not only through direct evidence of his concealment of the true end-destination of the products, but also by his receipt of numerous export warnings on documents provided by the manufacturers/suppliers; his facility navigating the Internet to conduct research to purchase products and register his fake company (thus showing an ability to find out basic information on export restrictions); and most importantly, his statements to his co-conspirators that evinced his knowledge that he was engaging in unlawful conduct, and his conscious avoidance and deliberate disregard of the law. For example:

- On September 1, 2009, Iranian co-conspirator Mohsen Hosseyni asked the defendant to get prices on an industrial camera system to be used in steel processing by Mobarakeh Steel, a company located in Isfahan, Iran. Hosseyni stated that the United States company would not sell to Iran. The defendant made inquiries regarding the product, but the transaction was never completed. In one of his emails to Hosseyni, the defendant advised that his preference would be to ship the equipment through Dubai, which would have concealed the ultimate end-destination of the item. JA 1306-07, 1315-23.

- On October 29, 2009, the defendant told Iranian co-conspirator Mohammad Nemati that he was involved in "trade," and if there was any business to be done, he was available. Nemati asked if he could be the defendant's "partner in Iran," and the defendant replied, "whoever in Iran wants something from here, I can find it for them. Yes, you too, like the rest, can look for customers, whatever they want, we buy it for them, and we send it . . . ." JA 1324-25.

- In November 2009, the defendant struck up a business partnership with co-defendant Arash Rashti Mohammad (Rashti), who was the Sales Manager for Darya Sazeh Aria Zamin Co. (DSAZ) in Tehran, Iran, and had a virtual office in Dubai identified as General DSAZ FZ-LLC. The defendant determined that he could obtain items more easily by creating a Maryland company through which he could order products to make it appear as though he was obtaining them for domestic use. In an electronic chat with Rashti on December 1, 2009, he described restrictions placed on importers/exporters in Maryland and the requirements for registering his business that he had learned from perusing the website for the Maryland Department of State. On December 18, 2009, the defendant registered Ace Electric with the State of Maryland, describing the business as a "residential and commercial electrical low and high voltage and trading (export and import)." There was no indication that he ever used the company for electric work. JA 2092-

96. On March 9, 2010, Rashti sent the defendant a list identifying sixteen of his customers in Iran, including oil refineries, a steel company, petrochemical companies, and shipping companies. Thereafter, any products obtained by the defendant for Rashti were sent to Rashti's virtual office in order to conceal their true end-destination in Iran. JA 1326-44, 1351-53, 1355-57, 1364-70, 1372-75, 1378-79, 1885-1910.

- On December 3, 2009, the defendant received a forwarded email from an employee of Kavoosh Niroo, an Iranian company he had worked for previously. The email contained an exchange in which Kavoosh Niroo was advised by a GE Industrial subsidiary in the Netherlands that it could not provide a quote for a particular industrial part because GE policy precluded doing business with an Iranian entity. It appeared that the email was forwarded to the defendant so he could attempt to obtain the part. On December 9, 2009, the defendant emailed the customer service department at the GE Industrial subsidiary (which had been copied on the forwarded email exchange with Kavoosh Niroo) falsely stating, "the GE department in the U.S. gave me your contact info. They said you can help me. . . . I need quote for this product and shipping to the U.S." JA 1348-51.

- On September 26, 2010, Iranian co-conspirator Hamidreza Dastjerd asked the defendant to obtain multiple units of an industrial-related electronic

component for delivery to Iran either directly or through Turkey. On September 28, 2010, the defendant responded, "As soon as they find out that the goods are for abroad, they don't sell. I had to use gimmicks to get prices." JA 1380-84.

- On February 20, 2010, Rashti received a request from an Iranian oil refinery (identified on the client list he had sent to the defendant) to purchase two cyclone separators. He asked the defendant to pursue the request through Geiger Pump in the United States. On November 17, 2010, after the defendant had placed the order, Geiger Pump asked the defendant if the items were for domestic use, and if not, to provide the end-use and destination. The defendant responded falsely, "we do stuck (sic) them and use it for domestic customer." In connection with the purchase, Geiger Pump provided a terms and conditions statement to the defendant that contained an export restriction stating, in pertinent part: "All products sold are for domestic use only, unless specifically documented otherwise by purchaser. Export and reexport sales must comply in all respects with the law and regulations of the United States, [and] the intended use and destination must be documented and approved . . . ." JA 824-40, 1390-1415. The defendant subsequently received similar warnings on documents related to a number of the other transactions established at trial. JA 1359-60, 1363-64, 1381-83, 1398, 1428, 1453-54, 1463-64, 1615-16, 1634, 1770.

- On September 20, 2010, after Rashti had received an order for thermocouples from another of his Iranian oil refinery clients, he asked the defendant to get a quote on the items from a named United States company. The company asked the defendant to identify the end-destination; after separately conferring with Rashti, he falsely identified Spin Control in Turkey as the end-destination. This was another company used by Rashti as a front to conceal shipment of his products to Iran. At the defendant's direction, Rashti subsequently deposited reimbursement for the defendant's shipping costs into a Bank Melli account in Iran held by the defendant's wife. JA 1416-17, 1419-74, 1565-67.

- In May 2011, Rashti caused two separate inquiries to be made for a list of thermoelectric industrial components, including a gas chromatograph – one inquiry by the defendant to the United States distributor, and the other inquiry by one of Rashti's Iranian employees to the manufacturer in the United Kingdom. The distributor's representative testified at trial that his company and the manufacturer became suspicious of the inquiries and denied the purchase. When the defendant was told, in his email exchange with the distributor, that a quote for the parts would not be provided because "it was already quoted by the factory for the customer in Iran," the defendant falsely responded, "Huh, are you sure? I got this order from a company from UAE, that sounds weird. If that's a [*sic*] case don't

worry about it and thanks for letting me know." Shortly thereafter, Rashti and the defendant engaged in an electronic chat about what had happened. The defendant told Rashti, "We screwed up." Rashti told the defendant to falsely state to the distributor that the purchase request came from the "Emirates." The defendant said he had already done so, to which Rashti said, "[I]f anyone asks us, we will say that we got this from client in Iraq. We did not know it was from Iran. Tell them [the distributor] that you asked us and we told you that, we got this from another company in Iraq." The defendant replied, "No, they probably won't even answer my hello." JA 905-22, 1524-33.[1]

- In late July 2012, Iranian co-conspirator Mehdi Mohammadi asked the defendant to obtain various industrial parts, including liquid pumps and check valves. He asked if the defendant would accept payment to family members in Iran. The defendant said he would not ship items directly to Iran, but was willing to ship to "Dubai or somewhere else." The two men discussed using the

[1] In connection with this attempted purchase, the defendant provided a business reference identified as Patrick Gross, a representative for RG Group, an industrial parts supplier from which the defendant had ordered numerous components on Rashti's behalf for unlawful export to Iran. In an email to Gross advising that he had been provided as a reference, the defendant asked that, if contacted, Gross say that the defendant's orders with RG Group were a combination of local and overseas orders, as "it would sound better for me." Gross testified at trial that he neither responded to the defendant, nor acceded to the request to lie on his behalf. JA 996-98, 1526-27.

defendant's "buddy" in Dubai (a reference to Rashti) to ship items to Mohammadi in Iran. The defendant ultimately solicited the assistance of his Iranian co-defendant Ehsan Naghshineh to have the products trans-shipped to Iran through China. Naghshineh subsequently confirmed delivery of the items to Mohammadi in Iran. JA 1657-1725.

- Between February and March 2013, the defendant attempted to obtain a turboexpander from a United States company for export to Mohammadi. When Mohammadi told the defendant to tell the company the product was for use in China, the defendant responded: "[I]f this address in China is the address of an office, rest assured, they will reject us. It has to be a place that if they Google it, it would look like a factory." Mohammadi replied that the address was for a copper tube manufacturing company and that he had coordinated with his contact in case an inquiry was made regarding the order. The defendant subsequently provided false information to the company identifying the end-user as a Chinese entity. JA 1847-61.

After his arrest on March 7, 2013, the defendant gave a *Mirandized* statement in which he attempted to minimize his export-related activities. He admitted to some knowledge of the Iran sanctions and that shipping items to Iran was a problem. He stated that it was not his concern where the items he exported

went or how they were used, as he was not shipping them to Iran. The FBI case agent testified at trial that throughout the interview, the defendant referred to Iran as "home" and reiterated his belief that as a United States citizen, he should be free to sell equipment to whomever he wished. JA 1925-66.

The defendant called a number of character witnesses in his defense, one of whom confirmed that in June 2011, she had sent him an email with a link to an article regarding the United States sanctions against Iran Air that included information about the Office of Foreign Assets Control (OFAC). JA 2170-78. The defendant testified in his own defense (JA 2385-2542), during which he provided nonsensical explanations for many of the damning statements in his emails and chats, and attempted to portray himself as a simple man of limited intellect. This latter point was negated not only by the government's evidence (and the defendant's admission regarding his ability to navigate the internet – JA 2538-42), but also by the defendant's fluency, during his testimony, in reading, understanding, and communicating in English, and his educational background, which, as corroborated by his resumes admitted at trial, included having obtained a Bachelor's degree in Industrial Engineering from a prestigious Iranian university where his father was a professor, and a Masters degree in Systems Engineering

from Morgan State University in Maryland, where he was continuing work on his Ph.D. JA 674-76, 678-80, 2393-96, 2508-09, 2411-14.

Ultimately, the defendant admitted: 1) his knowledge that the items he obtained, paid for, and exported were destined for his co-conspirators in Iran; 2) that he had provided false information to the United States manufacturers/supplier and put false information on invoices and shipping documents; and 3) that he violated the ITSR by not having obtained authorization for his export activity from OFAC. JA 2409-13. However, he asserted that he did not knowingly and intentionally violate the ITSR, as he was unaware that shipment to Iran through a third country was unlawful. JA 2415-18. He claimed his lack of knowledge was due to his lack of facility with the English language. JA 2390-2400. Finally, he attributed his actions to nothing more than doing what was easiest to obtain the items his associates required, and circumventing the type of government corruption with which he was familiar, having grown up in Iran. JA 2414-16, 2472-76, 2514-18, 2528-30. The jury disagreed.

SUMMARY OF ARGUMENT

I. The United States's sovereign interests have long been understood to justify broad authority to conduct warrantless searches at the border. In this context, the Supreme Court repeatedly has struck the balance of "reasonableness"

under the Fourth Amendment in favor of the sovereign, in light of the government's heightened interest in policing its borders and protecting its citizens, and the reduced expectations of privacy of individuals crossing international borders. As a result, travelers and their belongings – including their electronic devices – have long been subject to routine search at the border without a need to show probable cause or to obtain a warrant. This precedent remains unchanged by the Supreme Court's opinion in *Riley v. California*, which held that a warrant is required for searches of electronic media incident to arrest. The rationale of *Riley* does not apply to border searches, which are based on the government's plenary authority to inspect people and items entering and exiting the country. Border searches are treated differently under the law, serve a different purpose, and involve a much reduced expectation of privacy. For these reasons, no court has ever held that a warrant is required for a border search.

The Supreme Court has reserved whether, in certain exceptional cases involving intrusions on bodily integrity, destructive searches, or potentially highly offensive searches, a constitutional requirement of reasonable suspicion might be necessary to satisfy the "reasonableness" requirement of the Fourth Amendment. Some lower courts have also imposed a reasonable suspicion requirement for searches at the "extended border" after persons and property have cleared customs.

Here, the detention and forensic search of the defendant's electronic devices did not fall into any of these exceptional categories. This Court should not recognize a new exception to the government's plenary authority at the border for searches of electronic devices. The government has a compelling interest in ensuring that digital media is not used in international travel to smuggle contraband or materials that evidence or could be used in criminal activity, any more than written materials that could be used for the same purpose. At the border, any privacy expectations are reduced, and the government's sovereign interests remain paramount.

In any event, as the district court correctly found, there *was* reasonable suspicion that the defendant was engaged in criminal wrongdoing at the time agents detained his devices at the border and subjected them to a forensic search. Moreover, any error in the admission of the evidence seized from the defendant's devices was harmless beyond a reasonable doubt. Accordingly, this Court need not and should not decide the constitutional question of whether the search at issue here required reasonable suspicion: that constitutional inquiry would be far broader than what is necessary to resolve this case.

II. The defendant asserts that a willful violation of the IEEPA and the ITSR requires knowledge of the specific regulations and laws prohibiting exports

to Iran. This assertion is contrary to established precedent holding that proof of general knowledge of illegality, rather than knowledge of a specific law or regulation, is all that is required to sustain a conviction for a willful export violation. Because the jury instruction given by the district court was a correct statement of the law, the court did not abuse its discretion in denying the defendant's erroneous instruction on the issue of knowledge and intent.

ARGUMENT

I. THE GOVERNMENT'S FORENSIC SEARCH OF THE DEFENDANT'S ELECTRONIC MEDIA DETAINED AT THE BORDER CONSTITUTED A VALID WARRANTLESS BORDER SEARCH.

A. Standard of Review

In evaluating an appeal regarding suppression of evidence, this Court reviews the district court's factual findings for clear error and its legal conclusions de novo. *United States v. Jackson*, 728 F.3d 367 (4th Cir. 2013). Because the district court denied the defendant's suppression motions, this Court views the relevant facts in the light most favorable to the government. *United States v. Kimbrough*, 477 F.3d 144, 147 (4th Cir. 2007).

B. Relevant Facts

On March 31, 2012, at 9:47 p.m., U.S. Customs and Border Protection (CBP) officers stopped the defendant and his wife in their vehicle as they

attempted to enter the United States via the Rainbow Bridge in Niagara Falls, New York. A query of the defendant's name in the TECS database maintained by the Department of Homeland Security (DHS) revealed that the defendant was the subject of two ongoing investigations for export violations relating to the Iran sanctions – one based in Baltimore associated with HSI Special Agent Kelly Baird, and the other associated with HSI agents in Washington, D.C. As a result of the TECS query, the defendant and his wife were referred for a secondary inspection. JA 134, 153-56, 162-66. At 9:52 p.m., CBP Officer Kenneth Burkhardt contacted Agent Baird to advise her that the defendant had been stopped at the border. Agent Baird requested that electronic devices in the defendant's possession be detained for inspection.

At 10:00 p.m., Officer Burkhardt conducted a secondary examination of the defendant and his wife, during which he asked routine questions about their travel and had them remove the contents of their pockets. Among the defendant's possessions were two cell phones and a thumb drive. Per Agent Baird's request, the cell phones and thumb drive were detained and turned over to the HSI duty agent in Buffalo, who subsequently forwarded them to Agent Baird in Baltimore. The defendant and his wife were released from secondary inspection at

approximately 12:25 a.m. and allowed to proceed into the United States. JA 134-35, 166-80, 218-25.

On April 4, 2012, Agent Baird provided the defendant's detained electronic media to a HSI computer forensic agent in Baltimore for forensic imaging and analysis. JA 222-25, 239-40. The thumb drive was found to contain a copy of the defendant's resume, which indicated that he had worked in Iran for an Iranian company named Kavoosh Niroo. One of the detained cell phones, an Apple iPhone, was found to contain contact information for Patrick Gross (with RG Group, *see* Statement of Facts, above). The resume and the contact information were seized as evidence. No other information was seized pursuant to the forensic search of the detained media.[2] JA 231-34, 251.

On April 13, 2012, two weeks after the border crossing, Agent Baird and HSI Special Agent Tonya Matney met with the defendant in Baltimore to return his devices. Agent Baird asked him about his employment in Iran, as reflected on his resume, and whether he was aware of the Iranian sanctions and restrictions regarding conducting business for, or on behalf of, Iranian entities. The defendant responded: that he became aware one to two years earlier that there were restrictions and sanctions in place; that his friends who were students in the United

[2] The second detained phone was determined not to belong to the defendant; he subsequently confirmed it belonged to a friend. JA 233-34, 239-40, 672.

States were having trouble receiving funds from their families in Iran; and that United States persons were not allowed to use Iran Air. JA 232-33, 236-41. Agent Baird told the defendant he would need to seek permission from OFAC, through their website, prior to conducting any business for, or on behalf of, Iranian entities. The meeting lasted approximately ten minutes. JA 237, 242.

Following his arrest in March 2013, the defendant filed motions to suppress his statements to Agent Baird and the evidence obtained from the forensic search. As grounds for suppression of the forensic evidence, he asserted that once the devices were removed for inspection to Baltimore, the search was transformed into an "extended border search" requiring reasonable suspicion. JA 60-61.

At a motions hearing before the district court on September 23, 2013, Agent Baird detailed the information she had gathered on the defendant prior to his border crossing. She was aware that he traveled frequently to Iran. She was aware that in the fall of 2010, a company in Vermont had notified the FBI that the defendant had inquired about purchasing certain specialized technology having industrial, medical, or military applications. In late December 2011/early 2012, HSI agents in another office advised her that the defendant had become a person of interest in a separate investigation involving unlawful exports to Iran. In early March 2012, records she received from FedEx pursuant to subpoena revealed that

the defendant had shipped two cyclone separators valued at $100 to his future co-defendant Arash Rashti at a company in the UAE named General DSAZ. A search of that company through public sources indicated that it was linked to a company in Iran that dealt with industrial parts. JA 226-28, 244-46.

On March 29, 2012, Agent Baird interviewed employees of Geiger Pump, the company that had sold the cyclone separators to the defendant. Through those interviews she learned that the defendant had paid approximately $2,100 for the items, which was far less than the value he declared at the time of shipment. Agent Baird knew from her experience and training, as she testified at the hearing, that undervaluing items for shipment is a method commonly used to evade certain shipping reporting requirements and detection of such activity. Agent Baird also learned from Geiger Pump that the defendant had represented on an end-user statement that the cyclone separators were being obtained for domestic use, which was contrary to the evidence of his subsequent shipment of the items to the UAE. Finally, Agent Baird was told the defendant had sought to obtain another item from Geiger Pump on or about August 1, 2011. When asked to identify the end destination of the item, the defendant told Geiger Pump that he was unsure; a few

days later, however, he indicated that the item was to be sold to a company in Turkey. JA 228, 230-32, 234-36, 244.[3]

On March 30, 2012, RG Group advised Agent Baird that the defendant had purchased a number of items from the company in April 2011 through its customer service representative Patrick Gross. The defendant told the company that the items were being obtained for resale or restocking.[4] Agent Baird's review of subpoenaed credit card records received during the same time period as the interviews of RG Group and Geiger Pump revealed that the defendant also had been making numerous purchases from various other vendors costing thousands of dollars. JA 228-30, 246.

Agent Baird testified at the hearing that she sought detention and inspection of the defendant's electronic media pursuant to the authority she held as a customs officer to search persons and property traversing the border. Given her suspicions regarding his activities, she was seeking to determine if he was violating export laws. She also indicated that as a matter of course, she would be looking for

[3] The seized email communications admitted at trial established that the Turkish company, as well as General DSAZ, the Emirati company, were front companies used by the defendant and co-defendant Rashti to obtain items for export to Iran. *See* Statement of Facts, above.

[4] As noted in the Statement of Facts, above, those items were obtained for, and exported to, individuals and companies in Iran.

evidence of criminality relating to customs, immigration, terrorism, or national security violations. JA 221-26, 239-40, 248-51. She testified that even if she had no knowledge from the forensic search that the defendant had been employed in Iran, she would have given him the same advisement regarding the Iranian sanctions and OFAC restrictions upon returning his property, as she wanted to ensure that, as of the date of their meeting, he was aware of what he needed to do to comply with the sanctions. JA 241.

After the motions hearing, the district court published an opinion concluding that reasonable suspicion is the applicable standard for the type of forensic search conducted here. The court found that that standard was easily met in this case, that the search was therefore lawful, and that the defendant's subsequent statements to Agent Baird were the result of a voluntary, non-custodial encounter. JA 274-80, 289-91. *See United States v. Saboonchi (I)*, 990 F.Supp.2d 536, 539-44 (D.Md. 2014) (findings); JA 335-43.

Approximately one month prior to the start of trial, the Supreme Court issued its opinion in *Riley v. California*, 134 S. Ct. 2473 (2014). The defendant promptly filed a motion seeking reconsideration of the district court's refusal to suppress the results of the forensic search, arguing that *Riley* imposed a blanket requirement that all searches of digital data be conducted pursuant to a warrant

based on probable cause. JA 588. The court denied the motion for reconsideration in a published opinion. *United States v. Saboonchi (II)*, 48 F.Supp.3d 815 (D.Md. 2014); JA 608-15.

At trial, the government called Agent Baird to testify about the resume seized in the border search and her encounter with the defendant on April 13, 2012.[5] She testified that when she met with the defendant to return his property, he told her that six to seven years earlier, Kavoosh Niroo had him work, in an unpaid capacity, on a research project due to his industrial engineering background and English language skills. The defendant also stated that he knew United States persons were not allowed to use Iran Air because of sanctions he thought had been implemented one to two years earlier. Agent Baird testified that she advised the defendant that doing business with, or on behalf of, Iranian entities required a license from OFAC. She wrote out the full name for OFAC and its acronym on the back of the property receipt she gave to the defendant, and told him that OFAC had

[5] Government counsel did not question the agent about the contact information for Patrick Gross seized from the defendant's iPhone. Defense counsel, however, inquired about it on cross-examination. JA 710.

a website he could consult to see what rules and restrictions were in place. JA 671-78.[6]

Agent Baird also testified at trial about the execution of a search warrant at the defendant's residence on the day of his arrest, during which another copy of the defendant's resume was found. JA 678-80. The residential warrant had been preceded by the execution of multiple warrants on email accounts the defendant and his co-conspirators used, the supporting affidavits for which made no reference to any information obtained from the border search of defendant's electronic media, and were premised on information developed wholly independent of the border search. JA 403-07, 465-67, 482-88. The resume found in the residential search (Gov't Trial Exhibit 95) contained the same information regarding the defendant's employment with Kavoosh Niroo that was reflected on the resume obtained through the border search. (Gov't Trial Exhibit 94). JA 674-76, 678-80.

C. A Border Search Does Not Require a Warrant or Probable Cause.

Searches of persons and their effects at the border constitute a long recognized exception to the probable cause and warrant requirements of the Fourth Amendment. *United States v. Ramsey*, 431 U.S. 606, 619 (1977). Because the

[6] The details of the April 13th meeting were corroborated by Agent Matney, who was called by the government to rebut the defendant's own testimony regarding the encounter. JA 2561-66.

sovereign's interest in protecting its territorial integrity "is at its zenith" at the border, *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), "the expectation of privacy [is] less at the border than in the interior, [and] the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is . . . struck much more favorably to the Government . . . . " *United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985) (internal citations omitted). *See also Ramsey*, 431 U.S. at 623 n.17 (recognizing lack of "statutorily created expectation of privacy" at the border, and the "constitutionally authorized right of customs officials to search incoming persons and goods").

The border search authority granted to customs officers is broad and codified in numerous statutes and regulations. Congress has defined customs officers to include "any officer of the United States Customs Service of the Treasury Department . . . or . . . of the Coast Guard, or any agent or other person, including foreign law enforcement officers, authorized by law or designated by the Secretary of the Treasury to perform any duties of an officer of the Customs Service." 19 U.S.C. § 1401(i). Customs officers' border authority encompasses, among other things, the right to: inspect and search any vehicle or vessel and all persons, packages and cargo therein, *see* 19 U.S.C. §§ 482, 1467, 1581; inspect and search all persons, baggage, and merchandise entering the United States, *see* 19 U.S.C. §§

1496, 1582, and 19 C.F.R. § 162.6; detain and search all persons entering from foreign countries, *see* 19 U.S.C. § 1582; and detain property until inspected, examined, found to comply with the law, and cleared for release, *see* 19 U.S.C. §§ 1461, 1499. Similar broad authority "to conduct routine searches and seizures at the border, without probable cause or a warrant" has existed "[s]ince the founding of our Republic." *Montoya de Hernandez*, 473 U.S. at 537 (citing *Ramsey*, 431 U.S. at 616-17).

The defendant and the amici curiae now seek to have this Court improperly limit the government's statutory and constitutional authority to conduct warrantless searches at the border by extending the holding in *Riley v. California* to border searches of electronic media. The Supreme Court held in *Riley* that a search warrant is generally required to conduct a digital search of a cell phone seized incident to a lawful arrest. *Id*. at 2484-85. As the district court in this case correctly noted, the Court "did not recognize a categorical privilege for electronic data" in *Riley*, but rather expressly stated that "'even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions may still justify a warrantless search of a particular phone[.]" *Saboonchi (II)*, 48 F.Supp.3d at 817 (quoting *Riley*, 134 S. Ct. at 2494); JA 611. Beyond providing an example of how the exigent circumstances exception to the Fourth Amendment

warrant requirement might apply to permit a warrantless search of a cell phone, the *Riley* Court made no effort to address any other well-recognized exceptions to that requirement, such as a border search. *Riley*, 134 S. Ct. at 2486; *Saboonchi (II)*, 48 F.Supp.3d at 818; JA 612-13.

Searches at the border are "not subject to the warrant provisions of the Fourth Amendment," *Ramsey*, 431 U.S. at 617, as they are deemed "reasonable simply by virtue of the fact that they occur at the border . . . . " *Id.* at 616. This Court, in conformity with Supreme Court precedent, also has recognized the broad scope of the government's authority to conduct warrantless border searches of travelers and their belongings. In *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005), for example, the defendant challenged, on both constitutional and statutory grounds, the search of the contents of his laptop and other electronic media by customs officers who had located the items in his van when he presented himself at the border. This Court held that because the items were transported within the defendant's vehicle, the search of their contents was within the statutory border authority conferred upon customs officers by 19 U.S.C. § 1581(a) to inspect and search persons, vehicles, and their cargo. *Id.* at 503-05. The Court also held that the search passed constitutional muster given that border searches conducted without a warrant or a showing of probable cause constitute a "well-recognized

exception to the safeguards of the Fourth Amendment" that derives from the sovereign's right to police its borders and to protect its citizens. *Id.* at 505-06. Finally, the Court refused to extend First Amendment protection to the search, noting that to do so would create "a sanctuary at the border for all expressive material – even for terrorist plans," "undermine the compelling reasons that lie at the very heart of the border search doctrine," and result in the "sorts of legal wrangles at the border" in determining what constitutes protected material that "the Supreme Court wished to avoid by sanctioning expansive border searches." *Id.* at 506.

While the border search of electronic media in *Ickes* was not a forensic search, the decision demonstrates that border searches of electronic devices, like all border searches, do not require a warrant. As the district court correctly noted, *Ickes* also confirms the sovereign's right, as part of a routine border search, to open, inspect, and review files or other items contained in a traveler's electronic media just as it would with other physical items in the traveler's possession. *Ickes*, 393 F.3d at 505-07; *Saboonchi (I)*, 990 F.Supp.2d at 552; JA 356. *Accord United States v. Linarez-Delgado*, 259 Fed.Appx. 506, 508 (3d Cir. 2007) (unpub.) (citing *Ickes* and holding that viewing of video footage on a camcorder detained at border was a reasonable border search not requiring a warrant, consent, or reasonable

suspicion); *United States v. Bunty*, 617 F.Supp.2d 359, 364-65 (E.D.Pa. 2008) (search of computer equipment at border was a routine search not requiring reasonable suspicion); *United States v. Arnold*, 533 F.3d 1003, 1009 (9th Cir. 2008) (reasonable suspicion not required to search laptop or other personal electronic storage devices at the border).[7]

The "longstanding recognition that searches at our borders without probable cause and without a warrant are nonetheless 'reasonable' has a history as old as the Fourth Amendment itself." *Ramsey*, 431 U.S. at 619. *Riley* does not alter this longstanding law. The search-incident-to-arrest exception to the Fourth Amendment's warrant requirement at issue in *Riley* is markedly different in scope and purpose from the border-search exception. The search-incident-to-arrest exception allows for a search of the person and the immediate vicinity of the arrestee. This is fully consistent with the limited purposes of the exception, which are to locate any weapons that might endanger the arresting officer and/or to prevent the destruction of evidence by the arrestee. *See Riley*, 134 S. Ct. at 2483 (quoting *Chimel v. California*, 395 U.S. 752, 762-63 (1969)). As the Court noted

[7] *But see United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc) (discussed in more detail below, where court held reasonable suspicion is required to conduct forensic analysis of a traveler's electronic media).

in *Riley*, "there are no comparable risks [of harm to the officer or destruction of evidence] when the search is of digital data." *Id*. at 2485.

The border search exception, by contrast, serves different and broader purposes: protecting the nation's core sovereign interest in controlling the entry and exit of persons and property to and from the United States in order to safeguard against threats to the citizenry from contraband, smuggling, and illegal activity. *See, e.g.*, *Almeida-Sanchez v. United States*, 413 U.S. 266, 291 (1973) (border search authority is "an incident of every independent nation. It is part of its independence."); *Ickes*, 393 F.3d at 505 ("The realization that important national security interests are at stake 'has resulted in courts giving the broadest interpretation compatible with our constitutional principles in construing the statutory powers of customs officials.'") (quoting *United States v. Stanley*, 545 F.2d 661, 666 (9th Cir. 1976)). *See also United States v. Oriakhi*, 57 F.3d 1290, 1296-1302 (4th Cir. 1995) (holding that rationale for exempting border searches from the Fourth Amendment's probable cause and warrant requirements rests on fundamental principles of national sovereignty, which apply equally to inbound and outbound searches). Unlike the case with searches incident to arrest, the purposes underlying the border search doctrine apply in full force to searches of electronic media, which can contain contraband (such as child pornography) or

material (such as classified information or malware) that, if illicitly transferred beyond our borders, could pose a direct threat to our national security.[8]

There is nothing in *Riley* that suggests, let alone requires, the presence of a warrant to conduct a border search of a cell phone or other electronic device. At the border, the government can search both persons and property, including truck trailers, cargo containers, mobile homes, and more, generally without any requirement of individualized suspicion. Indeed, in its border decisions, the Supreme Court has not only limited any constitutional constraints on that authority, it has never imposed the requirement of a warrant for a border search. Neither has any other court.

---

[8] In *United States v. Kim*, ___ F.Supp.3d ___, 2015 WL 2148070 (D.D.C. 2015), a case the defendant and the amici curiae cite, the district court ruled that *Riley* obviated the need to address the constitutional question of what level of suspicion might be required for a forensic border search of electronic media, reading *Riley* to provide a framework for determining the reasonableness of such a search based on "the totality of the unique circumstances" of the case before it. *Id*., at **18-19. This free-form "reasonableness" balancing test ignores border search precedent and conflicts with the general Fourth Amendment requirement that courts set forth "'workable rules'" established on "'a categorical basis – not in an ad hoc, case-by-case fashion.'" *Riley*, 134 S. Ct. at 2491-92 (noting the Court's "general preference to provide clear guidance to law enforcement through categorical rules," and quoting *Michigan v. Summers*, 452 U.S. 692, 705 n.19 (1981)). Moreover, the *Kim* court's analysis ignores the fact that *Riley*, by its own terms, was limited to an analysis of Fourth Amendment reasonableness in the context of an exception (search incident to arrest) treated differently under the law than border searches. *See United States v. Blue*, 2015 WL 1519159, at *2 (N.D.Ga. April 1, 2015) (unpub.) (finding that *Riley* "has no direct application" to warrantless extraction of data during border search of cell phone).

In *Montoya de Hernandez*, for example, the Court held that officers needed reasonable suspicion that a traveler was smuggling contraband in her alimentary canal in order to detain her for a monitored bowel movement, in light of the impact on the traveler's personal dignity and physical privacy. 473 U.S. at 540-41. The Court specifically refrained from defining further "what level of suspicion, if any, [would be] required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches." *Id.* at 541 n.4. Nine years later in *Flores-Montano*, the Court upheld the suspicionless border search of the gas tank in a traveler's vehicle that was removed and dismantled as part of the search. There, the Court cautioned against "[c]omplex balancing tests" to categorize items crossing the border that might require individualized suspicion. 541 U.S. at 152. Both of these decisions reflect the Court's hesitance to unduly constrain the sovereign's border authority by arbitrarily assigning higher levels of privacy at the border to particular categories of items, or to particular types of searches.[9]

[9] A divided panel of this Court, relying in part on *Riley*, recently held that cell phone users have a reasonable expectation of privacy in their historical cell site location information, and thus, any inspection of that data constitutes a search requiring a warrant. *United States v. Graham*, 796 F.3d 332, 342-61 (4th Cir. 2015). On October 28, 2015, this Court granted the government's petition for rehearing en banc and vacated the panel opinion, tentatively scheduling oral argument before the en banc court for March 2016. *See* 2015 WL 6531272 (Mem. Order). The defendant and the amici curiae rely heavily in their briefs on the *Graham* panel opinion, which no longer has any precedential value. In any event,

In the context of his argument regarding *Riley*'s implications, the defendant recharacterizes the nature of the border search of his electronic devices in unjustified ways. First, the fact that officers took his devices to a secondary location for analysis did not alter the character of the search; it still was a border search requiring neither probable cause nor a warrant for its execution. In *Cotterman, supra*, the defendant's laptop was seized at the border and forensically examined 170 miles away. The Ninth Circuit found that this was still a border search because the laptop had never been "cleared" for entry by customs. 709 F.3d at 961-62. The Sixth Circuit employed similar reasoning in *United States v. Stewart*, 729 F.3d 517 (6th Cir. 2013), where it found that an offsite examination of the defendant's computers fell within the border search exception. "[T]here was no attenuation between Stewart's border crossing and the search of his computers; the government conducted the search *before* clearing them for entry and *before* he could regain an expectation of privacy in that property." *Id.* at 526 (emphasis in original).[10]

---

the issue in *Graham* is entirely distinct from the issue here, where a search is justified by compelling governmental interests at the border, coupled with the sharply diminished expectations of privacy of international travelers.

[10] As *Stewart* and *Cotterman* explain, an offsite examination does not transform a search into an extended border search. Even if it did, however, it would make no difference to the outcome of this case, because extended border searches may be

Second, the subjective intent of the officers initiating or conducting a border search "does not make otherwise lawful conduct illegal or unconstitutional." *Scott v. United States*, 436 U.S. 128, 138 (1978). *See also United States v. Villamonte-Marquez*, 462 U.S. 579, 584 n.3 (1983) (holding that the suspicionless boarding of a vessel to inspect its documents was valid even though customs officers were accompanied by state policeman investigating drug smuggling, citing and reaffirming same principle set forth in *Scott*). Neither is a border search rendered unlawful if it uncovers evidence of a crime rather than contraband, or is undertaken at the request of, or based upon information from, another law enforcement agency. *See United States v. Gurr*, 471 F.3d 144, 148-51 (D.C. Cir. 2006) (upholding border search even though made at request of FBI pursuant to a criminal investigation, where evidence of criminal activity was seized). "The important factor for a court to consider is whether the search was conducted under the proper authority, not the 'underlying intent or motivation of the officers involved.'" *Id*. at 149 (quoting *Scott*). *See also United States v. Smasal*, 2015 WL 4622246, at **2-4 and 10 (D.Minn. June 19, 2015) (unpub.) (in case where forensic analysis of defendant's electronic devices detained at border revealed evidence of crimes, district court rejected claim that border search was conducted

---

justified by reasonable suspicion, which, as described below, was clearly present here.

for general law enforcement rather than customs enforcement, citing Supreme Court's admonitions against subjective inquiries into improper motives or pretext in order to determine Fourth Amendment issues, and noting validity of a border search "does not depend on whether it is prompted by a criminal investigative motive") (quoting *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006)).

Export violations, by their very nature, are customs-related offenses affecting the national security and economy of the United States. Such violations are part and parcel of what customs officers investigate. The fact that Agent Baird had an ongoing investigation of the defendant's export activities, and had entered his information in the TECS database as a result, did not vitiate the validity of her authority to subject him and his property to a border search. *See United States v. Martinez*, 2014 WL 3671271, at **3-4 (S.D.Cal. July 22, 2014) (unpub.) (HSI agent's entry of defendant into TECS system was to further his investigation of defendant's alien smuggling activities; resulting border search of defendant's cell phone, which included extraction of data, upheld based on reasonable suspicion of criminal conduct developed from informant tips; court declined to address whether such suspicion was required).

There is no dispute that Agent Baird was well within her authority as a customs officer to initiate a border search of the defendant. More importantly, she

did so based on information suggesting that the defendant had engaged in, and was possibly continuing to engage in, export violations. "Whether a Customs official's reasonable suspicion arises entirely from her own investigation or is prompted by another federal agency is irrelevant to the validity of a border search, which . . . does not depend on whether it [was] prompted by a criminal investigative motive." *United States v. Levy*, ___ F.3d ___, 2015 WL 5692332, at *3 (2d Cir. Sept. 29, 2015) (and cases cited therein) (internal citation and quotation marks omitted).

D. Because Reasonable Suspicion of Criminal Activity Was Present in This Case, This Court Need Not Determine If It Was Required.

By virtue of its decision in *Cotterman*, the Ninth Circuit became the first and only federal appellate court to hold that a forensic examination of electronic media detained at the border for inspection requires the presence of reasonable suspicion of criminal wrongdoing. 709 F.3d at 962-68. The court's decision was accompanied by a powerful dissent criticizing the majority for flouting border search jurisprudence in its effort to elevate electronic devices to a special category carrying with it heightened Fourth Amendment protections at the border. 709 F.3d at 971-81 (Callahan, J., dissenting in part).

The *Cotterman* Court determined that because forensic analysis could enable greater access to the large quantity of information capable of being stored in

electronic devices, such analysis was analogous in invasiveness and intrusiveness to a strip search and thus required greater Fourth Amendment protections at the border. *Id*. at 964-66. As the dissent pointed out, however, this holding does not square with Supreme Court precedent that, to date, has made clear the Court's disinclination to determine the intrusiveness of a border search based upon the categories of objects involved, or the quantity of items searched. 790 F.3d at 975-76 (Callahan, J., dissenting); *Flores-Montano*, 541 U.S. at 142.

Though the district court in this case reached the same conclusion as in *Cotterman* – that a forensic search of electronic devices detained at the border requires the presence of reasonable suspicion – it took issue with the Ninth Circuit's failure adequately to define what constitutes a "forensic" search, and how such a search differs from a conventional search of such devices. *Saboonchi (I)*, 990 F.Supp.2d at 553-54; JA 359-61. Recognizing this Court's controlling precedent in *Ickes* regarding the broad scope of the sovereign's border search authority, the district court limited its requirement of reasonable suspicion to a forensic search that involves the creation of "a bitstream copy" of the hard drive of a computer or digital device that is then analyzed "by means of specialized

software." 990 F.Supp.2d at 569; JA 386.[11] The district court made clear that as to any *conventional* search of a computer or digital device, which may include booting up and/or operating the device to review its contents, reasonable suspicion is *not* required, because such searches are a routine exercise of the sovereign's border search authority. 990 F.Supp.2d at 560-61, 568-70; JA 371-72, 384-87.

Forensic examinations of computers and other electronic devices are important tools for identifying national security threats. There will be cases in which a customs officer suspects illegal activity based on information that would fall short of reasonable suspicion, or where the government has a reasonable suspicion of illegal activity but cannot disclose the basis for it (because, for example, the investigation is classified). Imbuing a traveler with a heightened privacy interest in information maintained in electronic form essentially provides a

[11] Other district courts have disagreed with the notion that electronic devices should be afforded heightened protection from search at the border. *See, e.g.*, *House v. Napolitano*, 2012 WL 1038816, at **7-8 (D.Mass. Mar. 28, 2012) (unpub.) (forensic border search of computer does not involve dignity and privacy interests associated with highly intrusive searches of the person, and requiring higher level of suspicion for such searches would arbitrarily "provide travelers carrying such devices with greater privacy protection than others who chose to carry the same type of personal information in hard copy form"); *United States v. Verma*, 2010 WL 1427261, at *4 (S.D.Tex. Apr. 8, 2010) (unpub.) (forensic border search of traveler's computer and external drives, regardless of how exhaustive, constitutes routine search, does not threaten the traveler's dignity nor inflict damage to his property, and is far less intrusive than dismantling of traveler's gas tank upheld as routine border search in *Flores-Montano*).

free pass to those who would do harm to this country – be it violent or economic – by intentionally concealing, obfuscating, and/or encrypting information that, once past the border, can be accessed with impunity to the detriment of our national interests. The information criminal actors (or others) could render undetectable in a non-forensic search could include not only tools that would further terrorist-related activity once within our borders, but also items such as malware, malicious code, or other tools of cyberespionage. This result flies in the face of the underlying basis for the broad border search authority granted to the sovereign. *See Ramsey*, 431 U.S. at 621.

This Court, however, need not reach the constitutional question of whether border searches of electronic media also require reasonable suspicion because it is clear, as the district court held, that the search in this case was based on reasonable suspicion. *See United States v. Molina-Gomez*, 781 F.3d 13, 19-20 (1st Cir. 2015) (declining to determine whether border search of defendant's laptop, gaming system, and cell phones required reasonable suspicion where such suspicion was present, and noting Supreme Court's caution against "complex balancing tests"); *United States v. Hassanshahi*, 75 F.Supp.3d 101, 119 n.11 (D.D.C. 2014) (holding that the doctrine of constitutional avoidance counseled against reaching question of whether reasonable suspicion was required for forensic computer search because

reasonable suspicion was present). *See also Irving*, 452 F.3d at 124 (reasonable suspicion was present, so court declined to reach the issue of whether developing and inspecting undeveloped film found in traveler's camera required reasonable suspicion); *United States v. Furukawa*, 2006 WL 3330726 (D. Minn. Nov. 16, 2006) (unpub.) (reasonable suspicion existed to search electronic devices and disks, so court declined to determine if border search was routine).[12]

Reasonable suspicion means a "minimal level of objective justification." *INS v. Delgado*, 466 U.S. 210, 217 (1984). It "is 'considerably less than proof of wrongdoing by a preponderance of the evidence,' and 'obviously less demanding than that for probable cause.'" *United States v. Jones*, 584 F.3d 1083, 1086 (D.C. Cir. 2009) (quoting *United States v. Sokolow*, 490 U.S. 1, 7 (1989)). As the district court correctly found, this standard was easily met here.

[12] Judicial restraint is a long-standing principle oft-repeated by the Supreme Court and enshrined in our jurisprudence. *See Ashwander v. TVA*, 297 U.S. 288, 346-47 (1936) (Brandeis, J., concurring); *Lyng v. Northwest Indian Cemetery Protective Ass'n*, 485 U.S. 439, 445 (1988). That principle counsels that courts should refrain from "'anticipat[ing] a question of constitutional law in advance of the necessity of deciding it,' or 'formulat[ing] a rule of constitutional law broader than is required by the precise facts to which it is to be applied.'" *United States v. Chappell*, 691 F.3d 388, 392 (4th Cir. 2012) (quoting, in part, *Ashwander*, 297 U.S. at 346-47). Before addressing a constitutional issue, it is incumbent upon a court to determine whether a decision on that issue would affect the ultimate outcome of the case. If not, a constitutional decision would be "unnecessary" and therefore "inappropriate." *Lyng*, 485 U.S. at 446.

Indeed, by the time the defendant arrived at the Rainbow Bridge border crossing on March 31, 2012, he was the subject of two investigations involving unlawful exports to Iran, a country in which he grew up and to which he traveled frequently. Documentary evidence and witness interviews had confirmed that the defendant previously had shipped industrial equipment to a company in the UAE linked to a company in Iran; that he had provided false information regarding the end-use/destination of the equipment to the company from whom the products were obtained; and that he had undervalued the items on shipping documents in a manner consistent with avoiding scrutiny. Other witness interviews had confirmed that the defendant had purchased numerous industrial items from another company, claiming they were for resale or restocking. In addition, the defendant's subpoenaed credit card records confirmed other purchases from various vendors costing thousands of dollars. JA 226-32, 234-36, 244-46. As the district court correctly concluded, this information was "sufficient to give rise to reasonable particularized suspicion – if not probable cause – that Saboonchi was involved in violations of export restrictions on Iran." *Saboonchi (I)*, 990 F.Supp.2d at 571; JA 389.[13]

[13] In this regard, the district court opinion in *Kim*, *supra*, is entirely distinguishable from this case. In fact, the judge in *Kim* specifically addressed the facts in this case, acknowledging that the information supporting reasonable

Moreover, the facts known to Agent Baird at the time of the border search, and the rational inferences that could be drawn from those facts, supported her reasonable suspicion that the defendant was engaging in ongoing export-related activities potentially in violation of export, customs, and national security-related laws and regulations. *See Montoya de Hernandez*, 473 U.S. at 541-42. Based on what she knew at the time of the border stop, Agent Baird's suspicion clearly was a "common-sense conclusio[n] about human behavior upon which practical people, including government officials, are entitled to rely." *Id.* at 542 (internal quotation marks and citation omitted).

"The essence of border search doctrine is a reliance upon the trained observations and judgments of customs officials, rather than upon constitutional requirements . . . . " *Ickes*, 393 F.3d at 507. "As a practical matter, computer searches are most likely to occur where . . . the traveler's conduct or the presence of other items in his possession suggest the need to search further." *Id.* Given the existence of reasonable suspicion; a record devoid of specifics regarding the forensic analysis of the defendant's electronic media; and the fact that (as discussed below) any admission of the relevant evidence at trial was in any event

---

suspicion of criminal wrongdoing by Saboonchi was more extensive, and involved an investigation "much further along," than the one presented to her. 2015 WL 2148070, at *13 n.10.

harmless beyond a reasonable doubt, this Court should decline to reach the constitutional issue of whether reasonable suspicion was required.

E. Suppression of the Evidence is Not Warranted Because the Agents Acted in Good Faith Reliance on Binding Appellate Authority, and If the Evidence Was Admitted in Error, the Error Was Harmless Beyond a Reasonable Doubt.

If this Court were to determine that a warrant was required for the forensic search of the defendant's devices (which it should not), or that the district court clearly erred in its factual finding that reasonable suspicion was present prior to the search (which it did not), neither ruling would require the exclusion of the minimal evidence resulting from the search (or otherwise justify reversal). *See Davis v. United States*, ___ U.S. ___, 131 S. Ct. 2419, 2427 (2011) (holding that the deterrence of exclusion varies with the culpability of the relevant law enforcement conduct; when actions are taken with "an objectively 'reasonable good-faith belief'" that the conduct is lawful, exclusion is unwarranted) (quoting *United States v. Leon*, 468 U.S. 897, 909 (1984)). Here, agents plainly acted in an objectively reasonable good faith belief on the Supreme Court's long-established border search precedents (discussed above), as well as this Court's precedent (including *Ickes*), in concluding that they did not need a warrant in order to search the defendant's devices.

Moreover, even if this Court were to determine that the district court erred in admitting the minimal forensic evidence obtained from the border search (which it did not), "[this Court] must 'review[ ] the remainder of the evidence against [the defendant] to determine whether the admission of the [challenged evidence] was harmless beyond a reasonable doubt.'" *United States v. Johnson*, 400 F.3d 187, 197 (4th Cir. 2005) (quoting *Arizona v. Fulminante*, 499 U.S. 279, 310 (1991)). Specifically, this Court "ask[s] 'whether, viewing the record as a whole, it is clear beyond a reasonable doubt that the jury would have returned a verdict of guilty'" absent the improperly admitted evidence. *Id.* (quoting *United States v. Jones*, 913 F.2d 174, 177 (4th Cir. 1990)); *United States v. Holness*, 706 F.3d 579, 598 (4th Cir. 2013) (reviewing court must determine based on the entire record that the error "did not contribute" to the defendant's convictions).

Nothing that emanated from the border search of the defendant's devices was critical to the government's proof. The resume that was seized contained the same information subsequently found in another resume seized in a separate search of the defendant's residence pursuant to a warrant. Moreover, as set forth in more detail in the Statement of Facts above, the evidence against the defendant that established his knowledge of, and intent to violate, the Iran sanctions was comprised almost entirely of evidence essentially generated by the defendant,

either through his extensive emails and chats with his coconspirators, and/or through the business records created in response to his purchases of the items he unlawfully exported, or attempted to export, to Iran. This evidence demonstrated not only the defendant's knowledge of the sanctions (by virtue of his extensive efforts to conceal the true nature and end-destination of his and his coconspirators' purchases), but also his ability to access information about the sanctions if he so desired, thus establishing (at the very least) his deliberate ignorance.

Indeed, one of the defendant's own character witnesses established that in or about June 2011, she had emailed an article to the defendant that contained information regarding the Iran Air sanctions and the website address for OFAC. The article, which was admitted into evidence during the government's rebuttal case, clearly reflected information regarding how to contact OFAC to address questions regarding the Iran sanctions. JA 2170-75, 2575-78, 2583-85. That information alone rendered Agent Baird's admonitions to the defendant about the sanctions approximately one year later in April 2012 somewhat insignificant when considered against the overwhelming documentary evidence of the defendant's ongoing and knowing evasion of export laws. *See United States v. Reed*, 780 F.3d 260, 269 (4th Cir. 2015) (declining to address constitutional issue where, even

assuming error, without so deciding, the error was harmless beyond a reasonable doubt).

* * *

There is no dispute that the advancement of technology brings with it the ability to store large amounts of information beyond what might be contained in traditional storage devices such as bags, containers, notebooks, and paper documents. That same technology, however, allows for ever-more sophisticated means to hide and obfuscate information that, if discovered, could adversely affect our economy and national interests. Using a broad brush to grant a higher level of protection to the search of electronic media would not only provide an obvious path to criminals and other malevolent actors to conceal evidence of their wrongdoing, but also undermine the very authority that Congress has deemed essential to protecting nation's security and economy.

In any event, for the reasons described above, this Court need not (and should not) decide the constitutional question of whether the search at issue here required reasonable suspicion, because that inquiry would be broader than what is necessary to resolve this case.

II. THE DISTRICT COURT PROPERLY INSTRUCTED THE JURY THAT IN ORDER TO FIND THE DEFENDANT GUILTY OF UNLAWFULLY EXPORTING GOODS TO IRAN, IT HAD TO FIND THAT THE DEFENDANT ACTED WITH KNOWLEDGE THAT HIS CONDUCT WAS UNLAWFUL.

A. Standard of Review

A district court's denial of a defendant's requested jury instruction is reviewed for abuse of discretion. *United States v. McFadden*, 753 F.3d 432, 443 (4th Cir. 2014), *reversed on other grounds*, 135 S. Ct. 2298 (2015). To show an abuse of discretion, a defendant must establish that the proffered instruction: "(1) was correct, (2) was not substantially covered by the charge that the district court actually gave to the jury, and (3) involved some point so important that the failure to give the instruction seriously impaired the defendant's defense." *United States v. Bartko*, 728 F.3d 327, 343 (4th Cir. 2013). "Even if these factors are met, however, failure to give the defendant's requested instruction is not reversible error unless the defendant can show that the record as a whole demonstrates prejudice." *Id.*

Here, the defendant has failed to establish error in light of the simple fact that his requested instruction was an incorrect statement of the law. *See McFadden*, 753 F.3d at 444.

B. Proof of Knowledge of General Illegality is Sufficient to Establish Willful Intent to Violate Export Laws.

In *Bryan v. United States*, 524 U.S. 184 (1998), the Supreme Court addressed the willfulness requirement of 18 U.S.C. § 924(a)(1)(D), which penalizes a willful violation of the statute that prohibits dealing in firearms without a license. The defendant argued that the government had to prove he had specific knowledge of the federal licensing requirement in order to establish his willful intent to violate the law. In support of his argument, he pointed to cases such as *Cheek v. United States*, 498 U.S. 192 (1991), in which the Court held that certain tax laws "carv[e] out an exception to the traditional rule that ignorance of the law is no excuse and require that the defendant have knowledge of the law" in order to prove willfulness. 524 U.S. at 194-95 (internal quotations omitted).

In rejecting the defendant's argument, the *Bryan* Court found that the federal licensing requirement did not raise the same concerns that motivated the Court's prior decisions regarding "highly technical" tax laws that "presented the danger of ensnaring individuals engaged in apparently innocent conduct." *Id.* at 194-95. Noting that "[e]ven in tax cases, we have not always required [a] heightened *mens rea*," *id.* at 194 n.17 (citing *United States v. Pomponio*, 429 U.S. 10 (1976) (upholding instruction similar to that given here)), the Court held that the willfulness requirement of § 924(a)(1)(D) did not carve out an exception to the

maxim that ignorance of the law is no excuse. Rather, all that was required to establish willfulness was proof of knowledge that the charged conduct was unlawful. *Id.* at 196. "[W]hile disregard of a known legal obligation is certainly sufficient to establish a willful violation [of offenses covered by 18 U.S.C. § 924(a)(1)(D)], it is not necessary." *Id.* at 198-99.

This Court has joined the majority of the other circuit courts in applying the definition of willful conduct set forth in *Bryan* to violations of the laws and regulations controlling the export of goods, munitions, services, and technology. In *United States v. Bishop*, 740 F.3d 927 (4th Cir. 2014), for example, this Court addressed the willfulness requirement underlying a violation of the Arms Export Control Act (AECA), which, through its attendant regulations, sets forth a regulatory scheme that controls the export of munitions and related defense technology and services identified on the United States Munitions List. *See* 22 U.S.C. § 2778; 22 C.F.R. Parts 120-130.

Relying on *Bryan*, this Court held that general knowledge of illegality, rather than knowledge of a specific prohibition, was sufficient to establish a willful intent to violate AECA. 740 F.3d at 932-35. In support of its analysis, the Court cited to similar conclusions reached by the Sixth Circuit post-*Bryan*, and the Third and First Circuits pre-*Bryan*. *Id.* at 934 (citing *United States v. Roth*, 628 F.3d 827,

835 (6th Cir. 2011) (knowledge that exported item on Munitions List not required, only "knowledge that underlying action is unlawful"), *United States v. Tsai*, 954 F.2d 155, 162 (3d Cir. 1992) (affirming court's instruction that defendant did not have to read or know details of AECA or Munitions List and could convict so long as it found defendant knew export was unlawful), and *United States v. Murphy*, 852 F.2d 1, 7 (1st Cir. 1988) (upholding jury instruction that government not required to show defendants aware of, or consulted, Munitions List or specific AECA licensing provisions)).

Similar to AECA, IEEPA sets forth a regulatory scheme that controls the export of goods and services and punishes willful violations of its provisions. These provisions include regulations such as the ITSR and others relevant to trade- and national security-related embargos. As is the case with AECA violations, various federal courts have relied on *Bryan* to define what constitutes a willful violation of IEEPA and its related regulations, including the ITSR. *See United States v. Mousavi*, 604 F.3d 1084, 1091-94 (9th Cir. 2010) (applying *Bryan* standard to IEEPA/ITSR violation for providing services to Iran); *United States v. Homa International Trading Corp.*, 387 F.3d 144, 146-47 (2d Cir. 2004) (applying *Bryan* standard to IEEPA/ITSR violation for unlawful money transfers to Iran); *United States v. Elashyi*, 554 F.3d 480, 504-05 (5th Cir. 2008) (applying *Bryan*

standard to violations of IEEPA and Libyan Sanctions Regulations for unlicensed exports to Libya and Syria); *United States v. Brodie*, 403 F.3d 123, 147 (3d Cir. 2005) (citing *Bryan*, among other cases, to support holding that specific intent requirement underlying violation of Cuban Embargo and Trading With the Enemy Act did not require government to prove defendant had knowledge of specific regulation governing the charged conduct; proof of general knowledge of unlawfulness of conduct was sufficient).

In *United States v. Quinn*, 403 F.Supp.2d 57 (D.D.C. 2005), the district court, relying on *Bryan* and *Bishop*, rejected the same argument made in this case that in order to prove willfulness, the government must produce evidence that the defendant possessed specific knowledge of the OFAC licensing requirement relevant to the charged unlawful exports to Iran. In holding that such specific knowledge was not required, the court noted:

> Surely neither Congress in passing IEEPA nor the Executive Branch in promulgating the [ITSR] intended to foreclose prosecution of persons who knew the gist, but not the exact details, of the law they are accused of violating. A defendant's assertion, no matter how credible, that he "had not brushed up on the law" has never been deemed a sufficient defense to a crime requiring knowledge of illegality. In fact, that is precisely the result that the Supreme Court sought to avoid [in *Bryan*].

Id. at 61. *Accord Mousavi*, 604 F.3d at 1093 ("[T]here is no basis for requiring the government to prove that a person charged with violating IEEPA and the [ITSR]

was aware of a specific licensing requirement" as "the danger of ensnaring individuals engaged in apparently innocent conduct is no greater under IEEPA than under the statute analyzed in *Bryan* . . . " (internal quotation marks and citations omitted)).

Here, the defendant appears to argue that the type of heightened *mens rea* the Supreme Court applied in *Cheek*, *supra*, is the level of scienter required by IEEPA and the ITSR in order to rescue its charged regulatory prohibitions from unconstitutional vagueness. In so doing, he conflates two wholly separate and distinct issues and advances an argument he never raised in the district court.

At trial, the defendant's attempt to obtain an instruction elevating the government's burden of proof of willful intent was premised on avoiding *Bryan*'s dictates and misconstruing applicable caselaw; he never raised an argument that tied a heightened *mens rea* to the alleged vagueness of the ITSR. JA 570-73, 580-84, 2351-73, 2380-82. The defendant did file a pre-trial motion seeking to dismiss the indictment on grounds that the ITSR is unconstitutionally vague, *see* JA 397-400, 410-19, but the district court denied that motion prior to trial based on judicial precedent to the contrary. JA 496-99. The defendant never raised the issue again and certainly never asserted it in the context of a challenge to the willful intent instruction. Generally, failure to raise an argument below waives the ability to

argue it on appeal. *United States v. Benton*, 523 F.3d 424, 428-29 (4th Cir. 2008). *See also United States v. Olano*, 507 U.S. 725, 732 (1993) (constitutional claim not raised below reviewed only for plain error that affected defendant's substantial rights). That said, the defendant's claim is simply a misstatement of the law.

Indeed, his assertion that specialized and technical knowledge is required to comprehend what may or may not be subject to the Iran Trade Embargo is puzzling, to say the least. First, this Court has previously held that the very provisions of the ITSR charged in this case, and its related Executive Orders, are unambiguous in barring "all 'exportation . . . to Iran.'" *United States v. Ehsan*, 163 F.3d 855, 860 (4th Cir. 1998). On that basis alone, the defendant's argument is without merit.

Second, contrary to the defendant's claim, the prohibitions of the ITSR are much more straightforward than those set forth in the AECA. The Munitions List contains a broad listing of categories of defense articles and services that cannot be exported absent a validated license from the Department of State. In some instances, the determination of whether a specific item falls within a particular category requiring an export license is dependent upon further analysis of the technical specifications of the relevant item or technology by the Department of State's Directorate of Defense Trade Controls. In comparison, the ITSR sets forth

an outright ban on exports to Iran absent some limited exceptions such as humanitarian aid. *See* 31 C.F.R. § 560.210. It strains credulity to say that while proof of knowledge of specific prohibitions is not required for a willful AECA violation, proof of knowledge of the limited exemptions to the Iran Trade Embargo is required to support a willful IEEPA/ITSR violation. This is precisely what the defendant would have this Court hold by imposing the heightened *mens rea* requirement rejected in *Bryan*.

Finally, though the defendant is correct that an intent requirement may mitigate a law's vagueness, *see Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982), he is incorrect in asserting that the required level of scienter for an IEEPA/ITSR violation is one in which the government must prove knowledge of the specific regulations. Those cases that have rejected vagueness challenges to both the AECA and IEEPA have done so while defining the requisite statutory scienter consistent with that set forth in *Bryan*. *See*, *e.g.*, *United States v. Hsu*, 364 F.3d 192, 196-98 and n.2 (4th Cir. 2004) (rejecting vagueness challenge to AECA given that criminal statute regulating economic activity is generally subject to a "less strict vagueness test," and noting evidence of knowledge that conduct was unlawful sufficient for scienter requirement – knowledge of specific regulation not required); *United States v. Lindh*, 212

F.Supp.2d 541, 574 (E.D.Va. 2002) (citing *Bryan* in dismissal of vagueness challenge to IEEPA charge for providing unlicensed services to specially designated persons or terrorists, and noting "[a] mind intent on willful evasion is inconsistent with surprised innocence") (internal citation omitted); *United States v. Amirnazmi*, 645 F.3d 564, 588-91 (3d Cir. 2011) (rejecting vagueness challenge to IEEPA charges for violating Iran Trade Embargo, noting not only nature of statutory scienter requirement, but also availability of guidance from the OFAC).[14]

C. The District Court's Jury Instruction on Willfulness Properly Defined the Government's Burden of Proof Regarding the Defendant's Willful Intent.

In instructing the jury on the conspiracy charged in Count One, the district court recited a combination of the standard instructions on knowledge (including conscious avoidance and deliberate ignorance), intent, and willfulness found in

[14] The defendant cites to two pre-*Bryan* export-related cases out of the Eleventh Circuit – *United States v. Macko*, 994 F.2d 1526 (11th Cir. 1993), and *United States v. Frade*, 709 F.2d 1387 (11th Cir. 1983) – to support his assertion that knowledge of a specific licensing regulation is required to establish a willful violation of export laws. In *United States v. Starks*, 157 F.3d 833 (11th Cir. 1998), a post-*Bryan* opinion in which the Eleventh Circuit applied *Bryan*'s definition of willfulness to a violation of the Social Security Act's anti-kickback provision, the court noted that *Bryan* "explicitly rejected" its prior expansive definition of willfulness as set forth in *United States v. Sanchez-Corcino*, 85 F.3d 549, 553-54 n.2 (11th Cir. 1996), which relied on, and followed, the definition of willful conduct outlined in *Macko* and *Frade* — the very cases upon which the defendant here rests his claim. Indeed, the *Starks* court upheld a definition of willfulness almost identical to that given in this case. *See* 157 F.3d 838; JA 2631.

Sand & Siffert's *Modern Federal Jury Instructions*. JA 586-87, 2629-32. The court defined willfulness as follows:

> You have been instructed that in order to sustain [its] burden of proof, the government also must prove that the defendant acted willfully. Willfully means to act with knowledge that one's conduct is unlawful and with the intent to do something the law forbids; that is to say, [with] the bad purpose to disobey or disregard the law.[15] The defendant's conduct is not willful if it was due to negligence, inadvertence, or mistake or was the result of a good faith misunderstanding of the requirements of the law. In this connection, it is for you to decide whether the defendant acted in good faith, that is, whether he sincerely misunderstood the requirements of the law or whether he knew what he was required to do and deliberately did not do so.
>
> To find that the defendant acted willfully, you must find beyond a reasonable doubt that he acted with the knowledge that his conduct was unlawful. While the government must show that the defendant knew that his conduct was unlawful, it is not necessary for the government to prove that the defendant had read or was aware of the contents of the IEEPA or the ITSR.
>
> Knowledge, willfulness, intent involve a person's state of mind. . . . This may be inferred from what he says or does, his words, his actions and his conduct as of the time of the occurrence of certain events . . . . Accordingly, intent, willfulness and knowledge are usually established by surrounding facts and circumstances as of the time the acts in question occurred or the events took place and the reasonable inferences to be drawn from them. Willful intent or guilty knowledge may also be inferred from the secretive or irregular manner in which a transaction is carried out.

[15] The judge read from his written instructions, which he provided to the jury. The bracketed word "with" was in the written instructions and appears to have been left out of the transcript. JA 2598.

JA 2631-32.

The district court subsequently instructed the jury on the substantive charges contained in Counts Two through Eight, which named certain items the defendant unlawfully exported or attempted to export in violation of the ITSR. JA 2634-37. The jury was instructed that as to each substantive count, the government had to prove that he violated, attempted to violate, or caused a violation of the ITSR (specifically, 31 C.F.R. § 560.204), and that he did so knowingly and willfully. JA 2637-38. After reiterating its previous instruction on § 560.204, *see* JA 2624, and the definitions of the terms "export" and "services," the court instructed the jurors to apply its prior instructions on "knowingly" and "willfully" in their consideration of the substantive charges. JA 2638-39.

As set forth in more detail in the Statement of Facts above, the evidence of the defendant's willful intent was extensive. Through admission of the defendant's email and chat communications, the government was able to establish his course of conduct over a period of four years during which he obtained goods for, and provided services to, Iranian nationals. This evidence revealed not only the defendant's knowledge that the items he obtained for his co-conspirators were destined for their use and/or their customers' use in Iran, but also the extent of his efforts to conceal the true destination of the items he obtained for export. These

efforts included: transshipping the items through Dubai and China; creating and using a Maryland company to make it appear as though the purchased items were for domestic use; providing false information to manufacturers/suppliers in order to avoid revealing that the goods were being obtained for, and on behalf of, Iranian nationals; and providing false information on shipping documents so as not to arouse the suspicions of law enforcement authorities who might scrutinize the exports.

The defendant's own background of growing up in Iran during the pendency of the Iran Trade Embargo, and his admissions to law enforcement regarding the sanctions, further undercut his claim at trial that he had no knowledge of the prohibitions against conducting business with, or providing services to, Iranian nationals. The evidence of the defendant's desire to "evade and avoid" the ITSR could not have been more clear. Despite being specifically admonished in April 2012 by Agents Baird and Matney about the prohibitions against doing business with Iran, the defendant continued to engage in unlawful exports with his co-defendants. Moreover, he admitted in his post-arrest *Mirandized* statement that he did not care if he was violating the law by obtaining goods for Iranian nationals that were likely going to Iran because he felt it was his right to sell goods to whomever he wished.

Finally, the defendant reiterates on appeal his claim, oft-repeated in pre-trial motions and at trial, that the ITSR is a complex and confusing labyrinth of legislative mumbo-jumbo beyond the understanding and comprehension of the average lay person absent the assistance of highly paid legal experts. What private lawyers do to market their services is not dispositive of the level of willful intent required to prove an export violation. Neither is the size of the OFAC staff that administers the ITSR. What is dispositive is the caselaw emanating from the Supreme Court, this Court, and other federal courts, both before and after *Bryan*, that confirms the propriety of the willfulness instruction given in this case.

CONCLUSION

For the reasons set forth above, this Court should affirm the district court's judgment.

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

By: /s/
Christine Manuelian
Assistant United States Attorney

36 South Charles Street, Fourth Floor
Baltimore, Maryland 21201
(410) 209-4800

November 18, 2015

STATEMENT WITH RESPECT TO ORAL ARGUMENT

While the United States respectfully suggests that oral argument is not necessary in this case, it does not dispute that oral argument may aid the Court in reaching its decision.

CERTIFICATE OF COMPLIANCE

1. This brief has been prepared using:

   Microsoft Word, Times New Roman, 14 Point.

2. EXCLUSIVE of the corporate disclosure statement; table of contents; table of citations; statement with respect to oral argument; any addendum containing statutes, rules, or regulations, and the certificate of service, the brief contains **13,970** words. I understand that a material misrepresentation can result in the Court's striking the brief and imposing sanctions. If the Court so directs, I will provide an electronic version of the brief and/or a copy of the word or line print-out.

/s/
Christine Manuelian
Assistant United States Attorney

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on November 18, 2015, I electronically filed the foregoing with the Clerk of Court using the ECF System, which will send notice of such filing to the following registered ECF users:

Meghan S. Skelton, Esq.
Office of the Federal Public Defender
6411 Ivy Lane, Suite 710
Greenbelt, Maryland 20770
Counsel for Ali Saboonchi

Nathan Freed Wessler, Esq.
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, New York 10004
Counsel for Amicus Curiae

Sophia Cope, Esq.
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
Counsel for Amicus Curiae

/s/
Christine Manuelian
Assistant United States Attorney