**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | **Criminal No.: 13-274 (RC)** |
| | : | |
| **v.** | : | |
| | : | |
| **SHANTIA HASSANSHAHI,** | : | |
| | : | |
| **Defendant.** | : | |
| | : | |

**THE UNITED STATES' OPPOSITION TO**
**DEFENDANT'S MOTION TO SUPPRESS EVIDENCE**

JOHN P. CARLIN
Assistant Attorney General for
National Security

RONALD C. MACHEN JR.
United States Attorney

JEFFREY M. SMITH
CASEY T. ARROWOOD
Attorneys
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

FREDERICK YETTE
Assistant United States Attorney
555 4th Street, N.W.
Washington, D.C. 20530
(202) 252-7733
frederick.yette@usdoj.gov

**TABLE OF CONTENTS**

## TABLE OF AUTHORITIES

**CASES:**

**CONSTITUTION:**

**STATUTES AND REGULATIONS:**



**MISCELLANEOUS:**

On January 12, 2012, upon his arrival back to the United States from a trip to Iran, Defendant Shantia Hassanshahi was selected for secondary border screening, at which time officers took his laptop and sent it to Sterling, Virginia for examination. That search uncovered substantial evidence that Hassanshahi engaged in millions of dollars of unlawful transactions with the government of Iran, as well as evidence that he knew his conduct was unlawful.

He now seeks to suppress that evidence on the basis of a purportedly unlawful law enforcement computer database query, made months earlier, that tipped federal agents to a phone number (subsequently determined to be associated with him) that had been in contact with a suspected Iranian procurer. Hassanshahi's motion fails because the evidence that he seeks to suppress is sufficiently attenuated from the earlier database query such that he is neither entitled to suppression of that evidence nor to discovery into the government's law enforcement databases. Moreover, because seeking admission to the United States from abroad is an intervening event that breaks the causal chain under the fruit-of-the-poisonous-tree doctrine, the exclusionary rule does not apply here.

Hassanshahi's alternative argument that the border search was unlawful because the government lacked reasonable suspicion is similarly without merit. The government has plenary authority to conduct suspicionless searches at the border. And, in any event, the government's months-long investigation had, prior to the border search, uncovered sufficient information to provide reasonable suspicion that Hassanshahi was involved in unlawful commerce with Iran.

## BACKGROUND

On August 16, 2011, Homeland Security Investigations ("HSI") received an unsolicited e-mail from a voluntary source indicating that the source had received an e-mail from an Iranian known as M. Sheikhi who, on behalf of Radyab Bartar Company (an Iranian company), sought

the source's assistance in procuring protection relays for an Iranian power project. Def's Ex. at 4. On September 20, 2011, two HSI agents interviewed the source in person. *Id.* at 5. The e-mail from Sheikhi to the source contained a business phone number. *Id.* After independent investigation to corroborate the information provided by the source, an HSI agent used the business telephone number associated with Sheikhi to "search[] HSI-accessible law enforcement databases, in furtherance of identifying potential U.S.-based targets engaged in the sale or export of protection relays for use in the Iranian electrical power grid." *Id.* at 6; Affidavit of Joshua Akronowitz ¶ 3 (attached) ("Akronowitz Aff."). This search returned a single telephone record indicating a call between Sheikhi's business number and a number with a Los Angeles, California area code. *Id.* ¶ 4.[1] Aside from this single phone number and its one call with Sheikhi's number, the database queries did not return any information relevant to the investigation. *Id.*

Viewing the Los Angeles-area number as a potential investigative lead, an HSI agent searched the number on Google's search engine and learned that the number was assigned to a company called Bandwith. *Id.* ¶ 12. The agent prepared and served on Bandwith an Administrative Export Enforcement Control Subpoena pursuant to 50 U.S.C. App. § 2411(a). *Id.* On October 4, 2011, Bandwith responded that the number was assigned to Google Voice, not Bandwith. *Id.* ¶ 13. On October 6, 2011, HSI prepared and served on Google an Administrative Export Enforcement Control Subpoena. *Id.* ¶ 14; Def's Ex. at 6. On October 18, 2011, Google provided responsive information that identified Hassanshahi as the person to whom the number was registered, and also identified Hassanshahi's e-mail address as shantia34@gmail.com.

[1] The Affidavit in Support of Criminal Complaint states that HSI "discovered telephone call log records indicating that a number of telephone calls between [the two numbers] had occurred within a relatively narrow time frame." Def's Ex. at 6. While this could be read to suggest that the initial database query of Shekihi's number returned multiple call records, in fact it returned only a single call record. Akronowitz Aff. ¶ 4. Additional call records were later acquired through a subpoena to Google. *Id.* ¶ 15.

Akronowitz Aff. ¶ 15; Def's Ex. at 6. Google also provided call log information for the period September 6, 2011 to October 6, 2011, which showed numerous calls between the number registered to Hassanshahi and an Iranian-based number. Akronowitz Aff. ¶ 15; Def's Ex. at 6.

On October 18, 2011, an HSI agent searched the Department of Homeland Security's TECS system for information about Hassanshahi.[2] Akronowitz Aff. ¶ 16. TECS revealed Hassanshahi's involvement in a previous investigation by federal law enforcement. *Id.* In that earlier matter, Hassanshahi and two partners established an American company that sought to enter into an agreement with a Chinese company to build a computer production facility in Iran. *Id.* The American company filed a breach-of-contract claim against the Chinese company in California state court. *Id.* The suit was dismissed, in part because the contract was unenforceable as against public policy, as it involved doing business in Iran. *Id.* The Department of Justice did not file criminal charges in that case. *Id.*

TECS also revealed a number of earlier instances of reentry into the United States by Hassanshahi, including an incident in 2005 when he was questioned by U.S. Customs and Border Protection agents after returning from Dubai with $15,000 in cash; an incident in 2006 when he returned from Tehran with a travel companion; and four other recent returns from Tehran, two in 2008, one in 2010, and one in 2011. *Id.* TECS also showed that on October 14, 2007, Hassanshahi was stopped and interviewed at the United States/Mexico border. *Id.*

On November 29, 2011, HSI augmented the existing TECS information by entering instructions that HSI should be alerted and Hassanshahi should be referred for secondary screening, if and when he returned to the United States. *Id.* ¶ 17. The basis for this instruction was HSI's belief, based on the results of its investigation to that point, that Hassanshahi may

[2] TECS is a database that serves as a data repository to support law enforcement "lookouts," border screening, and reporting for DHS's primary and secondary border inspection processes. *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

have been attempting to assist in the export of protection relays in violation of United States law. *Id.*

On or about December 20, 2011, HSI prepared and served on Google another Administrative Export Enforcement Congrol Subpoena, this one seeking subscriber information and recent Internet protocol logs for shantia34@gmail.com. *Id.* ¶ 18. On January 10, 2012, Google provided information indicating that the e-mail account had been accessed from Iran 24 times between December 8 and December 15, 2011. *Id.*

On January 11, 2012, HSI was alerted that Hassanshahi would be returning to the United States through Los Angeles International Airport ("LAX") the next day. *Id.* ¶ 19; Def's Ex. at 6. When Hassanshahi arrived at LAX on January 12, 2012, he was referred for secondary screening. Akronowitz Aff. ¶ 20; Def's Ex. at 7. U.S. Customs and Border Protection agents took several electronic devices from Hassanshahi, including a laptop computer, and sent them to Sterling, Virginia for analysis. Akronowitz Aff. ¶ 20; Def's Ex. at 7. That review located numerous documents relating to Hassanshahi's business activities in Iran. Def's Ex. at 7-17. For example, the documents showed that in 2009, Hassanshahi, through his company, purchased approximately $6,000,000 in goods that were exported to Armenia and then transshipped to Iran. *Id.* at 9. In a September 5, 2011 letter from Hassanshahi to the Iranian Minister of Energy, Hassansahi asked the Iranian government for payment for "protective relays for transmission lines." *Id.* at 10 (translated from Farsi). He warned that if he was unable to pay his supplier, a lawsuit might be brought in the United States, and "given that I am an Iranian and that these items are subject to sanctions and the fakeness of the end user, the worst will be expected." *Id.* at 11 (translated from Farsi). In another September 5, 2011 letter, this one to the chief executive of an Iranian company, Hassanshahi wrote that if his supplier "is not paid by the said date, that

company will probably begin to look into the address and information of the fake user in the Central Asian countries. This would mean giving away the diverted itineraries of the *High Tech* goods to our country!" *Id.* at 14 (translated from Farsi) (italics and underlining in original). Hassanshahi further warned: "Since I am an Iranian and that [sic] these *High Tech* items are subject to sanctions and that [sic] the address and information of the end user is fake, the worst legal problems will be expected." *Id.* (translated from Farsi) (italics and underlining in original).

Hassanshahi now seeks to suppress the evidence obtained from the border search, arguing that the "HSI-law enforcement accessible database[]" that provided HSI with his phone number (and therefore gave impetus to HSI's investigation of him) "is undoubtedly the so-called Bulk Telephony Metadata Program or some variant thereof, which has been in the news of late." Mot. 1. He contends that this program is unconstitutional or, alternatively, was accessed in violation of "the government's own internal orders and authority." Mot. 3. Hassanshahi also argues that a forensic search of a laptop at the border must be supported by reasonable suspicion and that reasonable suspicion was lacking here. None of Hassanshahi's arguments has merit.

## ARGUMENT

Hassanshahi's speculation that the "HSI-accessible law enforcement databases" referenced in the Affidavit in Support of Criminal Complaint include the National Security Agency's ("NSA") bulk telephony metadata database is incorrect. The NSA's database is not an "HSI-accessible law enforcement database"; it is a foreign intelligence database that can be accessed only by specified personnel within NSA. *See ACLU v. Clapper*, 959 F. Supp. 2d 724, 734 (S.D.N.Y. 2013). The "HSI-accessible law enforcement databases" searched in this case are, as the government's Affidavit in Support of Criminal Complaint indicates, law enforcement databases. And there is no basis for allowing Hassanshahi to delve into the operational details of

these databases because, even assuming that the query that returned a phone number associated with him was for some reason unlawful, there would be no basis for suppressing the evidence uncovered by the border search because the border search was sufficiently attenuated from the query such that it is not the "fruit" of that allegedly "poisonous tree." And, in any event, because arrival from abroad is an intervening act that breaks the causal chain between any prior Fourth Amendment violation and customs inspection, the fruit-of-the-poisonous-tree doctrine does not apply to border searches.

Hassanshahi's further argument that the border search was illegal is also without merit. The government does not need reasonable suspicion to conduct a border search and, in any event, it had reasonable suspicion in this case.

## I. The Evidence Seized During The Border Search Of Hassanshahi's Laptop Should Not Be Suppressed

### A. Because The Border Search Of Hassanshahi's Laptop Was Attenuated From The Query That Generated His Phone Number Several Months Earlier, The Exclusionary Rule Does Not Apply

Even assuming *arguendo* that the query that first produced Hassanshahi's phone number somehow violated his Fourth Amendment rights, suppression is unwarranted because the subsequent laptop search was sufficiently attenuated from that query. Not all evidence that may be causally connected to a challenged search will be deemed "fruits" of that search. Although subsequent evidence may be the result of a "but for" causal chain stemming from the challenged search, there comes a "point at which the . . . deterrent effect of the exclusionary rule no longer justifies its cost." *United States v. Leon*, 468 U.S. 897, 911 (1984) (quotation marks omitted). In determining whether the evidence is sufficiently "attenuated as to dissipate the taint" of the initial search, *Murray v. United States*, 487 U.S. 533, 537 (1988), courts consider three factors: (1) the "temporal proximity" of the search to the acquisition of the evidence; (2) "the presence of

intervening circumstances"; and (3) "the purpose and flagrancy of the official misconduct." *Brown v. Illinois*, 422 U.S. 590, 603-04 (1975). Here, (1) months passed between the query and the computer search, (2) during that time there were substantial intervening events, and (3) any alleged government misconduct was not flagrant. All three *Brown* factors therefore confirm that the results of the border search are not the "fruits" of the challenged query.

**1. The Acquisition Of The Evidence At Issue Was Temporally Remote From The Challenged Query**

Between the time they received the phone number in response to the query and the time of the border search, HSI agents spent more than three months conducting an investigation that turned a minor lead (*i.e.*, a phone number that had been in contact with a previously known target) into a substantial criminal inquiry that ultimately netted extensive evidence of criminal misconduct. This lengthy investigation is sufficient to attenuate the border search from the challenged query. *Compare United States v. Carter*, 573 F.3d 418, 425 (7th Cir. 2009) (finding attenuation based on subsequent investigation even though "very little time," approximately two hours, separated the illegal search from the subsequent investigatory technique). The first *Brown* factor thus weighs against suppression.

**2. Intervening Circumstances Break The Causal Chain**

In this case, two types of intervening circumstances broke the causal chain or dissipated the taint, if any, from the initial query that produced Hassanshahi's phone number: the numerous investigative steps that followed and Hassanshahi's voluntary appearance at the border with his laptop upon returning from foreign travel.

The challenged query returned only a phone number. In cases where such limited information is obtained, turning such information into actual evidence will necessarily require substantial independent investigative steps. Suppressing evidence obtained in such a scenario

would essentially turn the fruit-of-the-poisonous-tree rule into a but-for rule, in contravention of Supreme Court precedent. *United States v. Ceccolini*, 435 U.S. 268, 276 (1978) (rejecting "per se or 'but for' rule"); *see also United States v. Smith*, 155 F.3d 1051, 1060 (9th Cir. 1998) (noting "the courts' consistent rejection of a 'but for' causation standard in 'fruit of the poisonous tree' doctrine"). For this reason, courts have consistently held that where an unlawful search produces only the identity of a potential suspect, and investigators thereafter choose to focus attention on him, the results of that subsequent investigation are sufficiently attenuated from the initial search such that suppression is unwarranted.

For example, in *United States v. Friedland*, 441 F.2d 855, 856-57 (2d Cir. 1971), officers illegally bugged the offices of an acquaintance of the defendant. The bugging agents informed other officers that the defendant was worth investigating, and this triggered further investigation, which uncovered the defendant's involvement in bond forgery. *Id.* at 857. In refusing to suppress the evidence, Judge Friendly held that it "would stretch the exclusionary rule beyond tolerable bounds" to "grant life-long immunity from investigation and prosecution simply because a violation of the Fourth Amendment first indicated to the police that a man was not the law-abiding citizen he purported to be." *Id.* at 861. Other courts have reached the same conclusion on similar facts. *See Carter*, 573 F.3d at 423 ("Few cases, if any, applying the attenuation exception hold that evidence . . . is inadmissible because an illegal search first made a particular person a suspect in a criminal investigation."); *United States v. Najjar*, 300 F.3d 466, 478-79 (4th Cir. 2002) (documents from illegal search led to a subsequent investigation, but additional and independent investigatory steps sufficiently attenuated evidence from initial search); *Smith*, 155 F.3d at 1063 (Illegally obtained evidence "tipped off the government to the fact that a crime had been committed and to the probable identity of the perpetrator. It was, in

the words of the district court, a 'lead.' A lead, however, is simply not enough to taint an entire investigation."); *United States v. Watson*, 950 F.2d 505, 508 (8th Cir. 1991) ("[W]here a law enforcement officer merely recommends investigation of a particular individual based on suspicions arising serendipitously from an illegal search, the causal connection is sufficiently attenuated so as to purge the later investigation of any taint from the original illegality.").

In this case, the challenged query did not even return Hassanshahi's name. It merely identified a phone number that, through subsequent investigation, HSI was able to determine was associated with him. Over the next three months, HSI served several subpoenas and researched the TECS database to learn about prior government interactions with Hassanshahi. *See United States v. Crews*, 445 U.S. 463, 475 (1980) ("The exclusionary rule . . . does not reach backward to taint information that was in official hands prior to any illegality."). It was this investigation, and not the phone number, that underlay the instruction to refer Hassanshahi for secondary screening. Accordingly, the evidence collected as a result of the border search is attenuated from the query not only by the border search itself, but also by the investigation that preceded it. And, while the query result of Hassanshahi's phone number provided an early investigative lead, "it is not enough [to justify suppression] that the original [search] may have triggered [official] suspicion or gave 'impetus or direction toward what is to be focused on by the government.'" *Najjar*, 300 F.3d at 479 (quoting *Smith*, 155 F.3d at 1061).

Indeed, in a case similar to this one (but where, unlike here, there was a concededly illegal search), the Seventh Circuit observed that "requiring suppression because an illegal search made [the defendant] a target of the [criminal] investigation comes perilously close to Judge Friendly's famous hypothetical of 'grant[ing] life-long immunity from investigation and prosecution simply because a violation of the Fourth Amendment first indicated to the police that

a man was not the law-abiding citizen he purported to be.'" *Carter*, 573 F.3d at 424 (quoting *Friedland*, 441 F.2d at 861). And, indeed, personal immunity is precisely what Hassanshahi's motion seeks. *See* Mot. 2 (arguing that "*but for* the use of [the challenged] database, the government would not have had any interest in Mr. Hassanshahi") (emphasis in original). The law does not permit him to obtain immunity from further investigation.

Furthermore, Hassanshahi's voluntary decision to cross the international border constitutes an independent intervening circumstance that attenuates the laptop search from the initial query. As set forth in substantial detail *infra* Part II.A, the government has plenary authority to search persons and property at the international border to protect the territorial integrity of the United States, and such searches infringe only a minimal reasonable expectation of privacy on the part of travelers.

The search of Hassanshahi's laptop was conducted pursuant to this border search authority. And even if the initial query that ultimately led HSI to investigate Hassanshahi was unlawful, that query was not the proximate cause of the search of his laptop; the border crossing broke the proximate causal chain (even if not the but-for chain). *See, e.g.*, *Smith*, 155 F.3d at 1060 ("[T]he taint inquiry is more akin to a proximate causation analysis. That is, at *some* point, even in the event of a direct and unbroken causal chain, the relationship between the unlawful search or seizure and the challenged evidence becomes sufficiently weak to dissipate any taint resulting from the original illegality."). The border search of the laptop — a permissible exercise of the government's border search authority triggered by Hassanshahi when he voluntarily crossed the international border — is not a "fruit" of the initial query, and suppression is therefore unwarranted.

This principle reflects an application of the analogous line of cases holding that law enforcement officers' authority to stop and arrest a suspect (and to conduct a search incident to arrest) when they have probable cause to believe that they have witnessed a crime is not diminished because a prior illegal search or seizure first brought them into contact with the defendant. *See, e.g.*, *United States v. Allen*, 619 F.3d 518, 526 (6th Cir. 2010) ("Here, there was an initial attempt at a traffic stop, which Allen claims to have been illegal, followed by an attempt to escape from the police by leading the officers on a high-speed chase. . . . [T]he act of fleeing from police officers constituted a new, distinct crime that rendered evidence subsequently seized admissible."); *United States v. Sprinkle*, 106 F.3d 613, 615 (4th Cir. 1997) ("We hold that although no reasonable, articulable suspicion justified the stop, Sprinkle's use of the gun to commit a new, distinct crime after the stop made the gun subject to lawful seizure."); *id.* at 619 n.4 (citing cases from the First, Fifth, Eighth, Tenth, and Eleventh Circuits); *id.* at 619 ("[T]he new crime purged the taint of the prior illegal stop."). In those cases, as Hassanshahi argues here, the government became aware of the defendant by virtue of some prior unlawful search or seizure, yet a voluntary act on the part of the defendant — in those cases, committing a new crime; here, crossing the international border — attenuates the prior unlawful act and renders the exclusionary rule inapplicable. And just as officers do not have to turn a blind eye to the commission of a new crime, border agents do not have to turn a blind eye to the fact that a suspect is crossing the border.

Finally, the attenuation doctrine is premised on the notion that although evidence can be traced in a strict causal sense to a particular search, there comes a "'point at which the detrimental consequences of illegal police action become so attenuated that the deterrent effect of the exclusionary rule no longer justifies its cost.'" *Leon*, 468 U.S. at 911 (quoting *Brown*, 422

U.S. at 609 (Powell, J., concurring in part)). *Leon*'s analysis therefore implies that the attenuation inquiry will take account of the deterrence benefits of suppression as weighed against the costs of excluding often significantly inculpatory evidence. In the border search context, this balance weighs in favor of attenuation because the government's plenary search authority protects critical national security interests while infringing only a minimal reasonable expectation of privacy on the part of individuals crossing the border. *See infra* Part II.A.

**3. Any Alleged Government Misconduct Was Not Flagrant**

The final factor in assessing attenuation is the "flagrancy" of any initial government misconduct. *Brown*, 422 U.S. at 604. Here, any alleged misconduct could not have been "flagrant." The only information relating to Hassanshahi that was retrieved from the challenged query was a single telephone call record. In collecting and utilizing this call record, the government could reasonably rely on binding Supreme Court precedent that holds that call records do not give rise to constitutional protection. *See Smith v. Maryland*, 442 U.S. 735, 742-44 (1979).[3] Indeed, in *Smith*, the Supreme Court unambiguously recognized that "telephone numbers [obtained via call records] are not protected by the Fourth Amendment." *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 454 (D.C. Cir. 2000)) (citing *Smith*); *accord Reporters Comm. for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1042-46 (D.C. Cir. 1978); *United States v. Baxter*, 492 F.2d 150, 167 (9th Cir. 1973); *United States v. Fithian*, 452 F.2d 505, 506 (9th Cir. 1971); *United States v. Doe*, 537 F. Supp. 838, 839-40 (E.D.N.Y. 1982); *see also United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009) (holding that "there is no Fourth

[3] Even apart from the *Smith* line of cases, Hassanshahi's claim to Fourth Amendment protection in the record of a single *international* telephone call would be dubious in light of the Supreme Court's holding that the government may conduct suspicionless searches of the contents of international letters. *See United States v. Ramsey*, 431 U.S. 606, 607-08 (1977); *see also id.* at 623 n.17 ("There are limited justifiable expectations of privacy for incoming material crossing United States borders.").

Amendment 'expectation of privacy'" in "data about the 'call origination, length, and time of call'") (citation omitted).[4]

For his contrary view, defendant relies entirely on Judge Leon's opinion in *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *appeal pending*, No. 14-5004 (D.C. Cir.). Respectfully, "Judge Leon's analysis in *Klayman* [is] unpersuasive." *In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things*, Dkt. No. BR14-01, at 9 (For. Intel. Surv. Ct. Mar. 20, 2014) (Collyer, J.).[5] But, in any event, the query at issue predated *Klayman* and was undertaken in reasonable reliance on existing appellate caselaw. Thus, even if

[4] Courts have also applied *Smith* to find no reasonable expectation of privacy in e-mail metadata such as "to/from" and Internet protocol ("IP") information, *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008), and in text message addressing information, *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd on other grounds*, 560 U.S. 746 (2010). *See also United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (no reasonable "expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient"); *Guest v. Leis*, 255 F.3d 325, 335-36 (6th Cir. 2001) (no Fourth Amendment interest in subscriber information such as names, addresses, birthdates, and passwords communicated to Internet service providers).

[5] Every other Article III judge that has reviewed the program at issue in *Klayman* has upheld it as constitutional on the ground that individuals have no Fourth Amendment right to the privacy of their telephone call records. *See id.*; *Smith v. Obama*, __ F. Supp. 2d __, 2014 WL 2506421, at *4 (D. Idaho June 3, 2014) (Winmill, J.) ("But *Smith* [*v. Maryland*] was not overruled, and it continues . . . to bind this Court. This authority constrains the Court from joining *Klayman*."); *ACLU v. Clapper*, 959 F. Supp. 2d 724, 741 (S.D.N.Y. 2013) (Pauley, J.) (Call "records are created and maintained by the telecommunications provider, not the [caller or recipient of the call]. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information.") (citing *Smith*), *appeal pending*, No. 14-42 (2d Cir.); *United States v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518, at *7 (S.D. Cal. Nov. 18, 2013) (Miller, J.) ("Here, when Defendant Moalin used his telephone to communicate with third parties, whether in Somalia or the United States, he had no legitimate expectation of privacy in the telephone numbers dialed."), *appeal pending*, No. 13-50572 (9th Cir.); *In re Application of the F.B.I. for an Order Requiring Production of Tangible Things*, Dkt. No. BR13-158, at 4 (For. Intel. Surv. Ct. Oct. 11, 2013) (McLaughlin, J.) (holding that "under *Smith v. Maryland*, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment"); *In re Application of the F.B.I. for an Order Requiring Production of Tangible Things*, No. BR13-09, 2013 WL 5741573, at *2 (For. Intelligence Surv. Ct. Aug. 29, 2013) (Eagan, J.) ("The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*."); *cf. United States v. Dennis*, No. 3:13-cr-10-TCB, 2014 WL 1908734, at *12 (N.D. Ga. May 12, 2014) ("Defendant's reliance on *Klayman* is misplaced . . . and in any event, the Court finds the reasoning of [the Southern District of New York in *ACLU v. Clapper*] persuasive in concluding that there was no Fourth Amendment violation by the [government's] logging of IP addresses that were subsequently queried by the agents.").

the Supreme Court were to overrule *Smith*, the query could not be considered to be a "flagrant" violation. *See Davis v. United States*, 131 S. Ct. 2419, 2429 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.").[6] Thus, the third *Brown* factor, like the first two, weighs heavily against suppression.

* * *

In sum, the border search occurred months after the challenged query, was based on information gathered through subsequent investigative steps, and resulted from no "flagrant" misconduct. All three *Brown v. Illinois* factors therefore compel the conclusion that the border search was sufficiently attenuated from the query that the evidence Hassanshahi seeks to suppress is not the "fruit" of the query he challenges. He is therefore entitled neither to suppression nor to discovery.

## II. The Search of Hassanshahi's Laptop Was A Permissible Exercise Of The Government's Plenary Authority To Conduct Suspicionless Searches At The Border And Was, In Any Event, Supported By Reasonable Suspicion

Hassanshahi argues (Mot. 28-38) that the evidence recovered from his laptop should be suppressed because the government lacked reasonable suspicion to conduct the search. But the government has plenary authority to conduct suspicionless searches at the international border, and that authority plainly applies to the examination of Hassanshahi's laptop. In any event, the search was supported by reasonable suspicion. Hassanshahi's arguments are therefore without merit.

[6] Indeed, even if the Supreme Court were to rule that the warrantless acquisition of call detail records violated the Fourth Amendment, the rule of *Davis* would still mean that call records collected while *Smith* was still in effect would not be subject to suppression. If the call records themselves would not be suppressed, it follows *a fortiori* that evidence further down the causal chain should not be subject to exclusion.

### A. Homeland Security Did Not Need Reasonable Suspicion To Search Hassanshahi's Laptop

#### 1. The Border Search Doctrine Authorizes The Government To Conduct Suspicionless Searches At The Border

"The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004); *see also id.* at 153 ("It is axiomatic that the United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity."). Accordingly, the Supreme Court has "[t]ime and again . . . stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'" *Id.* at 152-53 (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)); *see also, e.g., Ramsey*, 431 U.S. at 616-19 (discussing the deep historical roots of the border search doctrine and explaining that "[b]order searches, . . . from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside").

Border searches are therefore permissible under the Fourth Amendment regardless of whether they are supported by any individualized suspicion of wrongdoing. *See Flores-Montano*, 541 U.S. at 152-53; *see also, e.g., United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985) ("Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant . . . ."); [7] *United States v.*

[7] In *Flores-Montano*, the Supreme Court rejected the Ninth Circuit's over-reliance on *Montoya de Hernandez*'s use of the term "[r]outine." *See* 541 U.S. at 152 ("The Court of Appeals took the term 'routine,' fashioned a new balancing test, and extended it to searches of vehicles. But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person — dignity and privacy interests of the person being searched — simply do not carry over to vehicles. Complex balancing tests to determine what is a 'routine' search of a vehicle, as opposed to a

*Stewart*, 729 F.3d 517, 524 (6th Cir. 2013) ("[S]earches of people and their property at the borders are per se reasonable, meaning that they typically do not require a warrant, probable cause, or even reasonable suspicion."); *United States v. Alfaro-Moncada*, 607 F.3d 720, 728-29 (11th Cir. 2010) (border searches of people and property are generally permissible "without any level of suspicion"); *Nicholas v. Goord*, 430 F.3d 652, 660-61 (2d Cir. 2005). This bedrock principle of Fourth Amendment jurisprudence reflects that one's "expectation of privacy [is] less at the border than in the interior" and that "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 at the border." *Montoya de Hernandez*, 473 U.S. at 539-40; *see also United States v. Gurr*, 471 F.3d 144, 148 (D.C. Cir. 2006); *United States v. Sanders*, 663 F.2d 1, 3 (2d Cir. 1981) ("The entry in and of itself constitutes consent to a routine search of one's belongings and effects, as to which, at the border, no subjective expectation of privacy is recognized."); *Zweibon v. Mitchell*, 516 F.2d 594, 631 n.93 (D.C. Cir. 1975) (en banc) ("In effect, a reasonable border search is 'consented' to in order to obtain a benefit that is only to be accorded those who can show that they should gain admittance and who can demonstrate that they are only transporting goods which can lawfully be brought into the country. . . . [T]here is a minimal invasion of privacy since there is an expectation on the part of those entering that they and their possessions will in all probability be searched to at least some extent.").[8]

---

more 'intrusive' search of a person, have no place in border searches of vehicles."). Moreover, the Supreme Court has been clear that non-routine searches include things like "strip, body-cavity, or involuntary x-ray searches," *id.* (quoting *Montoya de Hernandez*, 473 U.S. at 541 n.4) — not non-destructive searches of property.

[8] This reduced expectation of privacy stems in part from "the longstanding, constitutionally authorized right of customs officials to search incoming persons and goods." *Ramsey*, 431 U.S. at 623 n.17.

Under these well-established principles, the search of Hassanshahi's laptop was reasonable simply by virtue of the fact that he attempted to bring the laptop into the United States.

**2. None Of The Exceptions To The Border Search Doctrine Apply To The Search Of Hassanshahi's Laptop**

Notwithstanding the government's expansive authority to conduct suspicionless searches of persons and property at the international border, searches that are sufficiently "destructive" of property, or "highly intrusive searches of . . . person[s]," might need to be supported by reasonable suspicion; similarly, the Supreme Court has left open the possibility that "particularly offensive" searches might also require some level of particularized suspicion. *Flores-Montano*, 541 U.S. at 152-56 & n.2.[9] The first exception obviously does not apply here, as there is no claim that the search damaged Hassanshahi's laptop. And as set forth below, the second and third exceptions are also inapplicable.

The forensic examination of petitioner's laptop, however intrusive, was not intrusive "of [a] . . . person." Just as "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person — dignity and privacy interests of the person being searched — simply do not carry over to vehicles," *Flores-Montano*, 541 U.S. at 152, they also do not carry over to computers. As such, the concern animating this exception is inapposite. *See United States v. Cotterman*, 709 F.3d 952, 973 (9th Cir. 2013) (en banc)

[9] Thus, in *Montoya de Hernandez*, 473 U.S. at 535-36, 541-42, the Supreme Court required a showing of reasonable suspicion to support the lengthy detention of a defendant suspected of smuggling drugs in her alimentary canal. But that is the only time the Supreme Court has required any level of individualized suspicion in the border search context. *See United States v. Cotterman*, 709 F.3d 952, 971-72 (9th Cir. 2013) (en banc) (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). Aside from that decision, the Supreme Court has overturned lower court holdings cabining the government's expansive border search authority. *See, e.g.*, *Flores-Montano*, 541 U.S. at 150 (overturning Ninth Circuit decision requiring reasonable suspicion to conduct a border search of an automobile gas tank); *Ramsey*, 431 U.S. at 620-24 (overturning D.C. Circuit decision requiring probable cause and a warrant before opening international mail).

(Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) ("[T]he exception for 'highly intrusive searches of the person' cannot apply here; 'papers,' even private ones in electronic format, are not a 'person.'" (internal citation omitted)). Nor, finally, has Hassanshahi pointed to anything so "particularly offensive" about the search that would warrant applying an exception to the government's expansive authority to conduct suspicionless searches at the border.

### 3. Hassanshahi's Reliance On The Ninth Circuit's En Banc Decision In *Cotterman* Is Misplaced

In support of his argument that the government needed reasonable suspicion before searching his laptop, Hassanshahi relies heavily on the Ninth Circuit's decision in *Cotterman*. There, a majority of the en banc court held that, notwithstanding the government's broad authority to conduct suspicionless searches at the border, the government needed reasonable suspicion to conduct a forensic computer examination at the border. 709 F.3d at 962-68. The decision was motivated in substantial part by the court's determination that forensic searches of computers are different from searches of other types of personal property insofar as such computer searches are more intrusive and invasive of one's personal privacy interests. *See, e.g.*, *id.* at 962-63 (describing the search there as "akin to reading a diary line by line looking for mention of criminal activity — plus looking at everything the writer may have erased"); *id.* at 964 ("The private information individuals store on digital devices . . . stands in stark contrast to the generic and impersonal contents of a gas tank."); *id.* ("We rest our analysis on the reasonableness of this search, paying particular heed to the nature of the electronic devices and the attendant expectation of privacy."); *id.* ("The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or

automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information.").

But *Cotterman*'s view "that electronic devices deserve special consideration because they are ubiquitous and can store vast quantities of personal information . . . has no place in the border search context." *Cotterman*, 709 F.3d at 975 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment).[10] Although the Supreme Court has suggested that it might be appropriate in some cases to distinguish between border searches of people and border searches of property, *see Flores-Montano*, 541 U.S. at 152, the Court has not distinguished between different types of property in the border search context. Indeed, in *Flores-Montano*, the Supreme Court rejected the Ninth Circuit's approach of requiring reasonable suspicion for intrusive searches of property but not for more "routine" searches. *Id.* at 152-56 (rejecting rule that "to conduct a search that goes beyond the routine, an inspector must have reasonable suspicion, and the critical factor in determining whether a search is routine is the degree of intrusiveness") (internal quotation marks and citation omitted).

Rather, "electronic devices are like any other container that the Supreme Court has held may be searched at the border without reasonable suspicion." *Cotterman*, 709 F.3d at 976 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). *See also United States v. Ickes*, 393 F.3d 501, 507 (4th Cir. 2005); *United States v. Linarez-Delgado*, 259 Fed. Appx. 506, 508 (3d Cir. 2007) (unpublished) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."); *United States v. Irving*, No. 03 Cr. 0633 (LAK), 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003).

[10] We explain below why the Supreme Court's recent decision in *Riley v. California*, __ S. Ct. __, 2014 WL 2864483 (June 25, 2014), which held that the search-incident-to-arrest doctrine does not extend to searches of cell phones, is inapplicable to the border search context.

This makes sense. There is no reason that an individual who hides contraband on a computer — for example, by encrypting the files, requiring entry of a password to open the files, or storing the files in an area of the hard drive not readily visible to a searching officer — as he crosses the border should receive greater Fourth Amendment protections than the offender who carries that same contraband across the border in his suitcase or on a computer but without measures in place to impede a government search.

In *Ramsey*, 431 U.S. at 620, the Supreme Court reasoned: "It is clear that there is nothing in the rationale behind the border-search exception which suggests that the mode of entry will be critical. It was conceded at oral argument that customs officials could search, without probable cause and without a warrant, envelopes carried by an entering traveler, whether in his luggage or on his person. Surely no different constitutional standard should apply simply because the envelopes were mailed not carried. The critical fact is that the envelopes cross the border and enter this country, not that th[ey] are brought in by one mode of transportation rather than another." The same principles apply here and render erroneous *Cotterman*'s holding that forensic computer examinations at the border are sufficiently unique as to require that they be supported by reasonable suspicion. *Cf. Irving*, 2003 WL 22127913, at *5 ("Several courts have compared personal notebook computers to closed containers for the purposes of the Fourth Amendment analysis. Inspection of the contents of closed containers comes within the scope of a routine border search and is permissible even in the absence of reasonable suspicion or probable cause. . . . [A]ny other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search simply by scanning images onto a computer disk before arriving at the border."). It is illogical to afford greater Fourth Amendment protection to those who more effectively conceal their contraband.

Similarly, it is well established that an individual's desire to keep material private does not itself require individualized suspicion to search when a suspicionless search is otherwise authorized. As the Supreme Court explained in *United States v. Ross*, 456 U.S. 798, 823 (1982): "The luggage carried by a traveler entering the country may be searched at random by a customs officer; the luggage may be searched no matter how great the traveler's desire to conceal the contents may be." It follows that an individual's efforts to hide computer data beneath layers of password-protection or encryption, or to stash documents in an area of the hard drive not accessible absent specialized forensic software, may well reflect that individual's expectation that the material will be kept private, but such an expectation is not a reasonable one in the context of a border crossing. Fourth Amendment protections in the border search context do not rise and fall with the means and methods by which a would-be criminal attempts to hide his contraband from an otherwise lawful search.

Moreover, the foundational underpinnings of the border search doctrine — the right of the sovereign to protect its territory and its citizens from the introduction of contraband, and the substantially lower expectation of privacy that individuals have at the border as compared to once inside the country — do not vary depending on whether the traveler carries the contraband in luggage, in a readily visible way on a computer, or hidden on a computer. Allowing suspicionless forensic examinations of laptops at the border serves "the essential purposes" of the border search doctrine and does not infringe any reasonable expectation of privacy on the part of individuals entering the United States. *See generally California v. Carney*, 471 U.S. 386, 394 (1985) ("Applying the vehicle exception in these circumstances allows the essential purposes served by the exception to be fulfilled, while assuring that the exception will acknowledge legitimate privacy interests.").

**4. Compelling Government Interests Are Served By The Ability To Conduct Suspicionless Forensic Examinations Of Computers At The Border**

As set forth above, the foundation of the border search doctrine rests on "the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." *Flores-Montano*, 541 U.S. at 152 (internal quotation marks omitted). "It is axiomatic," therefore, that the United States "has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Id.* at 153. In this way, the border search doctrine is closely related to the government's goal of protecting the nation's security against individuals and governments that intend to do harm. *See, e.g.*, *United States v. Navedo*, 694 F.3d 463, 473 (3d Cir. 2012) (border searches "require[] far less justification than an arrest that does not implicate the nation's interest in the security of its borders"); *Alfaro-Moncada*, 607 F.3d at 728 ("The United States' paramount interest in conducting searches at its borders is national self-protection."); *id.* at 730 ("The concern that contraband or worse will be smuggled into this country has special force in modern times."); *United States v. Seljan*, 547 F.3d 993, 1009 (9th Cir. 2008) (en banc) (Callahan, J., concurring) ("The rationale behind the border search exception has its origins in national self-protection . . . . At perhaps no other time in our nation's history are border searches as vital to maintaining national security."); *Ickes*, 393 F.3d at 506 ("The government has an overriding interest in securing the safety of its citizens and to do this it must seek to prevent 'the introduction of contraband into this country.'") (quoting *Montoya de Hernandez*, 473 U.S. at 537).

This case presents the type of serious national security concern that animates and justifies the border search doctrine and underscores why, pursuant to that doctrine, officers are authorized to conduct suspicionless searches. Hassanshahi was charged with unlawfully conspiring to export goods and services — namely, protection relays and related parts and accessories — to

Iran, in violation the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. § 1705, and the Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. Part 560. Both IEEPA and ITSR have obvious national security purposes. *See, e.g., Islamic Am. Relief Agency v. Gonzales*, 477 F.3d 728, 735 (D.C. Cir. 2007) ("The President may exercise his authority under the IEEPA 'to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.'") (quoting 50 U.S.C. § 1701(a)); *Ministry of Defense & Support for the Armed Forces of the Islamic Republic of Iran v. Cubic Defense Sys., Inc.*, 665 F.3d 1091, 1097 (9th Cir. 2011) (the ITSR is "a means toward the larger end of exerting economic pressure on Iran, in order to induce Iran to abandon policies that the United States deems adverse to its interests") (internal quotation marks and citation omitted).

*Cotterman*'s "decision to insulate electronic devices from search at the border creates serious national security concerns." *Cotterman*, 709 F.3d at 984 (Smith, J., dissenting). Searches of electronic devices are a critical component of law enforcement efforts to protect the national security. This is true now and will become only more true in the future as computers and electronic media become capable of storing increasing amounts of data and as individuals intent on doing harm become more sophisticated at hiding that data. *See generally* Michael Chertoff, *Searches Are Legal, Essential*, USA TODAY, July 16, 2008, at 10A ("In the 21st century, the most dangerous contraband is often contained in laptop computers or other electronic devices, not on paper."). A rule requiring reasonable suspicion before conducting a forensic computer examination as part of a lawful border search would hamper law enforcement

efforts to protect the nation's security precisely at the moment when the government's interest in ensuring that security is at its "zenith." *Flores-Montano*, 541 U.S. at 152.

It is an insufficient resolution to this problem to conclude, as the *en banc* majority did in *Cotterman*, 709 F.3d at 967 n.14, that "[a]ny contention that national security will be critically hampered by stripping border agents of a critical law enforcement tool — suspicionless forensic examinations of electronics — is undermined by the fact that, as a matter of commonsense and resources, it is only when reasonable suspicion is aroused that such searches typically take place." The Ninth Circuit's rule would require suppression of evidence that was recovered pursuant to an officer's hunch, even one that turned out to be correct. *See United States v. Sokolow*, 490 U.S. 1, 7 (1989) (reasonable suspicion requires more than a hunch). This, in turn, could foreseeably result in officers declining to conduct a forensic search for fear that a court will conclude that reasonable suspicion was lacking, *see Cotterman*, 709 F.3d at 979–80 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment); *id.* at 985–86 (Smith, J., dissenting),[11] even though, as the Supreme Court has emphasized, such searches are generally in the public's interest and interfere with no substantial expectation of privacy. And to the extent these concerns arise every time an officer is confronted with facts that might or might not rise to the level of reasonable suspicion, the fact that the government's interest in conducting such searches is at its "zenith" in the border search context renders any comparison to other contexts inapposite.

[11] *See also* Chertoff, *supra* (requiring "a particular standard for [border] searches [of electronic devices] would have a dangerous, chilling effect as officers' often split-second assessments are second-guessed").

**5. The Supreme Court's Recent Decision In *Riley v. California* Does Not Prohibit Officers From Conducting Suspicionless Searches Of Computers At The Border**

Subsequent to the filing of Hassanshahi's motion to suppress, the Supreme Court held in *Riley v. California*, __ S. Ct. __, 2014 WL 2864483, at *9 (2014), that law enforcement officers' authority to conduct warrantless searches incident to arrest does not extend to warrantless searches of cell phones. In reaching that conclusion, the Court reasoned that "[a]bsent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Id.* (internal quotation marks and citation omitted). The decision turned on the Court's determination that (i) the purposes of the search-incident-to-arrest doctrine — officer safety, preventing escape, and preventing the destruction of evidence — were only minimally implicated by warrantless searches of cell phones, but that (ii) the privacy implications of such searches were substantial in light of the vast and varied amount of personal information people generally keep on their cell phones. *See id.* at *9-*16.

But the balance between governmental interests and privacy intrusions is struck much differently — and much more favorably to the government — at the border than in the search-incident-to-arrest context. And that is true notwithstanding that laptops, like cell phones, are capable of storing substantial amounts of varying kinds of personal information. Accordingly, *Riley* does not apply here.

The government's compelling interest in conducting suspicionless searches at the border predates even the adoption of the Fourth Amendment. The government's plenary border search authority has been in existence "since the beginning of our Government." *Flores-Montano*, 541 U.S. at 153; *see also Ramsey*, 431 U.S. at 619 ("Border searches, then, from before the adoption

of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside."); *id.* ("This 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."). The Congress that proposed the Bill of Rights had, two months earlier, enacted the first customs statute, which allowed for "plenary customs power" to conduct searches at the border. *See id.* 616. And that power "was differentiated from the more limited power to enter and search any particular dwelling-house, store, building, or other place where a warrant upon cause to suspect was required." *Id.* (internal quotation marks and ellipsis omitted). As the Supreme Court has reasoned, "[t]he historical importance of the enactment of this customs statute by the same Congress which proposed the Fourth Amendment is . . . manifest." *Id.* at 616-17. It underscores the fundamental importance of the long-established authority to conduct suspicionless searches at the border.

The authority to conduct warrantless searches at the border stems from "[t]he Government's interest in preventing the entry of unwanted persons and effects" from entering the United States — an interest that is "at its zenith" at the border. *Flores-Montano*, 541 U.S. at 152. This border search authority protects the nation's territorial integrity and advances indisputably consequential national security interests. *See generally supra* Part II.A.4. Indeed, the border search authority is "inherent" in the government's authority to protect the nation, *Flores-Montano*, 541 U.S. at 153, and constitutes an interest that is both "paramount," *id.*, and "overriding," *Ickes*, 393 F.3d at 506. This substantially elevated governmental interest renders "the Fourth Amendment's balance of reasonableness . . . qualitatively different at the international border than in the interior." *Montoya de Hernandez*, 473 U.S. at 538; *cf. Ramsey*,

431 U.S. at 619 ("Import restrictions and searches of persons or packages at the national borders rest on different considerations and different rules of constitutional law from domestic regulations." (quoting *United States v. 12 200-Ft. Reels of Film*, 413 U.S. 123, 125 (1973)). Thus, whereas *Riley* held that the government's interests in conducting searches incident to arrest were diminished in the context of cell phone searches, the same cannot be said for similar searches conducted pursuant to the government's plenary border-search authority. Upholding the search here, even after *Riley*, reflects only that "extensive searches at the border are permitted, even if the same search elsewhere would not be." *Ickes*, 393 F.3d at 502.

As to privacy concerns, a traveler's reasonable expectation of privacy at the international border is markedly less pronounced than it is in the search-incident-to-arrest context. It would be unreasonable for a traveler to assume, in light of the compelling government interests described above and which inhere generally in the nature and functions of government, that law enforcement officers would be prohibited from conducting suspicionless searches at the border. Moreover, international travelers know that, by virtue of their voluntary decision to present themselves for entry into the United States, they are subject to the government's plenary search authority. *See, e.g.*, *Ramsey*, 431 U.S. at 623 n.17; 5 Wayne R. LaFave, Search & Seizure § 10.5(a) (5th ed. 2012) ("[S]ince the individual crossing a border is on notice that certain types of searches are likely to be made, his privacy is less invaded by those searches.") (internal quotation marks omitted). Knowing this, travelers have options: they can avoid traveling to the United States; they can leave their personal technology devices behind; or they can remove from their personal technology devices any information that they would not want searched. *See id.* ("The individual traveler determines the time and place of the search by his own actions, and he thus has ample opportunity to diminish the impact of that search by limiting the nature and character

of the effects which he brings with him."). This is all in considerable contrast to the search-incident-to-arrest context, which typically involves situations in which the search is triggered by unanticipated and non-voluntary conduct on the part of the arrestee (*i.e.*, getting arrested).

### B. Even if the Fourth Amendment Required Reasonable Suspicion For The Laptop Search, Information Gathered By HSI Established Reasonable Suspicion

In *Cotterman*, 709 F.3d at 957, the Ninth Circuit held that the government must have reasonable suspicion before it can undertake a forensic examination of a laptop seized at the border. As we argue above, the border search exception applies to all property carried by a traveler entering the United States, and no suspicion was required to search Hassanshahi's laptop. But even if this Court finds that reasonable suspicion was required to search Hassanshahi's laptop, the facts known to the government before Hassanshahi reached inspection at LAX were more than sufficient to provide the Customs and Border Patrol agents with a particularized and objective basis for suspecting him of wrongdoing. *See United States v. Arvizu*, 534 U.S. 266, 273 (2002).

To begin, in August and September 2011, and prior to the seizure of the laptop, HSI agents learned from a voluntary source that M. Sheikhi, an Iranian national acting on behalf of Radyab Bartar Company, wanted to buy protection relays from the United States for use in an Iranian power project. An e-mail from Sheikhi to the source contained Sheikhi's business phone number.

In early October 2011, HSI served an Administrative Export Enforcement Control Subpoena on Google, seeking subscriber information and call records for a phone number with a California area code. The information provided by Google showed that the number was subscribed to by Hassanshahi, who resided in California. Call log records for the period between

September 6 and October 6, 2011, showed numerous calls between Hassanshahi's Google-issued phone number and an Iranian number. Pursuant to a second subpoena, HSI subsequently obtained from Google Internet protocol logs for Hassanshahi's gmail account, which showed that the password-protected account had been accessed from Iran 24 times during the second week of December, 2011. This information suggested that Hassanshahi had traveled to Iran to pursue the sale of protection relays to Sheikhi's business. But HSI had more. A TECS search showed that Hassanshahi had, in the past, worked with a Chinese company to build a computer production facility in Iran, and that Hassanshahi had returned to the United States from Iran on multiple occasions in recent years. When viewed together, the facts gathered by HSI firmly established reason to suspect that Hassanshahi was facilitating the export of protection relays to Sheikhi's business in Iran, in violation of United States law.

Hassanshahi nevertheless argues (Mot. 33-35) that reasonable suspicion was lacking because no informant identified him; the government did not have the content of the calls between Hassanshahi's phone and Sheikhi's business phone or the content of his e-mails; someone other than Hassanshahi could have made the calls to Iran; someone with his password could have accessed his gmail account from Iran; and he did not have a criminal record. But reasonable suspicion does not require the government to know all the facts or to confirm every suspicion. To the contrary, "[t]he required level of suspicion 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 *Sokolow*, 490 U.S. at 7). Moreover, contrary to Hassanshahi's suggestion, the facts supplying reasonable suspicion "'need not rule out the possibility of innocent conduct.'" *United States v. Brown*, 334 F.3d 1161, 1168 (D.C. Cir. 2003) (quoting *Arvizu*, 534 U.S. at 277). Hassanshahi

does not dispute that the government had sufficient grounds to believe that Sheikhi was trying to buy transfer relays from an American seller, and that federal law barred the sale of transfer relays to Iran. Hassanshahi argues only that the government's record of calls, e-mails, and travel were too slim to provide reason to suspect that Sheikhi was doing business or attempting to do business with *him*. Hassanshahi is wrong. The evidence provided strong indication of his involvement with Sheikhi's illegal endeavor. Especially when viewed in light of information in the TECS system indicating that Hassanshahi had previously been investigated for attempting to do business in Iran, Hassanshahi's travel, phone, and e-mail records suggested that he was not just catching up with relatives but was engaged in a prohibited business deal. In short, the information known to HSI was more than sufficient to meet the low threshold of reasonable suspicion.

## CONCLUSION

For the reasons stated above, Hassanshahi's motion to suppress should be denied.

July 10, 2014

Respectfully submitted,

JOHN P. CARLIN
Assistant Attorney General for
National Security

RONALD C. MACHEN JR.
United States Attorney

/S/

Jeffrey M. Smith, D.C. Bar 467936
Casey T. Arrowood, D.C. Bar 996381
Attorneys
National Security Division
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

Frederick Yette, D.C. Bar 385391
Assistant United States Attorney
National Security Section
555 4th Street, N.W.
Washington, D.C. 20530
(202) 252-7733
frederick.yette@usdoj.gov