2015 WL 2148070
Only the Westlaw citation is currently available.
United States District Court,
District of Columbia.

United States of America
v.
Jae Shik Kim, Karham Eng. Corp., Defendants.

Crim. Action No. 13–0100 (ABJ) | Signed May 8, 2015

**Synopsis**

**Background:** Defendant charged with violating export control laws moved to suppress evidence discovered during warrantless search of laptop computer that was seized as he was departing from the United States for his home country of Korea.

**Holdings:** The District Court, Amy Berman Jackson, J., held that:

[1] mere fact that alien may have previously participated in unlawful export of controlled articles to Iran in violation of export control laws did not provide special agent of the Department of Homeland Security (DHS) with reasonable suspicion of any ongoing or imminent criminal activity, of kind sufficient to support seizure and search of contents of alien's laptop computer as he was departing for his home country of Korea following his most recent visit to the United States;

[2] in assessing reasonableness of search,, it was not appropriate for court to simply categorize the laptop as "container," of kind which may be subjected to warrantless search at border; and

[3] search was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of defendant's privacy and so disconnected from not only the considerations underlying the breadth of government's authority to search at border, but also the actual border itself, that it was unreasonable and violative of Fourth Amendment.

Motion granted.

West Headnotes (14)

[1] **Arrest**
Reasonableness; reason or founded suspicion, etc

Law enforcement officer has reasonable suspicion of criminal activity, of kind sufficient to support investigatory stop, if officer can point to specific and articulable facts which, when considered together with rational inferences that can be drawn from those facts, indicate that criminal activity may be afoot. U.S. Const. Amend. 4.

Cases that cite this headnote

[2] **Arrest**
Reasonableness; reason or founded suspicion, etc

Court's determination of whether officer had reasonable suspicion of criminal activity, of kind required to support investigatory stop, must be based on totality of the circumstances. U.S. Const. Amend. 4.

Cases that cite this headnote

[3] **Arrest**
Reasonableness; reason or founded suspicion, etc

Reasonable suspicion of criminal activity, of kind required to support investigatory stop, is reasonable suspicion of ongoing or imminent crime. U.S. Const. Amend. 4.

Cases that cite this headnote

[4] **Customs Duties**
Particular Objects or Products

Mere fact that alien may have previously participated in unlawful export of controlled articles to Iran in violation of export control laws did not provide special agent of the Department of Homeland Security (DHS) with reasonable suspicion of any ongoing or imminent criminal activity, of kind sufficient to support seizure and search of contents of alien's laptop computer as he was departing for his home country of Korea following his most recent visit to the United States, where alien had business interests in the United States sufficient to explain his frequent visits, where prior incident in which alien allegedly participated in unlawful export of controlled articles to Iran did not involve his travel to the United States, and where special agent conducted no surveillance of alien while he was in the United States on his latest trip and uncovered nothing during his encounter with alien in airport to suggest any ongoing or imminent violation of export laws. U.S. Const. Amend. 4.

Cases that cite this headnote

[5] **Arrest**
Reasonableness; reason or founded suspicion, etc

Evidence of prior criminal conduct alone is insufficient to give rise to reasonable suspicion of ongoing or imminent criminal activity, of kind required to support investigatory stop. U.S. Const. Amend. 4.

Cases that cite this headnote

[6] **Aliens, Immigration, and Citizenship**
Border Stops and Inspections
**Customs Duties**
Searches and Seizures

Government's interest in preventing the entry of unwanted persons and effects is at its zenith at international border. U.S. Const. Amend. 4.

Cases that cite this headnote

[7] **Customs Duties**
Grounds or cause for stop, search, or seizure

Routine searches of the persons and effects of entrants at international border are not subject to any requirement of reasonable suspicion, probable cause, or warrant. U.S. Const. Amend. 4.

Cases that cite this headnote

[8] **Searches and Seizures**
Fourth Amendment and reasonableness in general

Ultimate touchstone of validity of search under the Fourth Amendment is reasonableness. U.S. Const. Amend. 4.

Cases that cite this headnote

[9] **Searches and Seizures**
Necessity of and preference for warrant, and exceptions in general

When search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of judicial warrant. U.S. Const. Amend. 4.

Cases that cite this headnote

[10] **Searches and Seizures**
Necessity of and preference for warrant, and exceptions in general

In the absence of warrant, search is reasonable only if it falls within a specific exception to warrant requirement. U.S. Const. Amend. 4.

Cases that cite this headnote

[11] **Customs Duties**
Particular Objects or Products

In assessing the reasonableness, for Fourth Amendment purposes, of law enforcement agent's conduct in seizing laptop computer of alien suspected of having violated export laws in the past before alien boarded aircraft to return to his home country of Korea, and in having hard drive copied so that it could be subjected to search of indefinite duration using specialized computer software, it was not appropriate for court to simply categorize the laptop as "container," of kind which may be subjected to warrantless search at border, especially given the wealth of personal information that could be stored on laptop and fact that actual examination and analysis of contents of laptop's hard drive occurred over period of weeks at location far removed from border; rather, to determine constitutionality of agent's conduct, district court had to proceed by assessing, on the one hand, the degree to which search intruded on alien's privacy and, on the other, the degree to which it was necessary for promotion of legitimate governmental interests. U.S. Const. Amend. 4.

Cases that cite this headnote

[12] **Aliens, Immigration, and Citizenship**
Border Stops and Inspections
**Customs Duties**
Searches and Seizures

Government's power to conduct warrantless searches at the border arises out of the sovereign's right and need to protect its territorial integrity and national security; searches made at the border, pursuant to longstanding right of the sovereign to protect itself by stopping and examining persons crossing into the country, are reasonable simply by virtue of fact that they occur at the border. U.S. Const. Amend. 4.

Cases that cite this headnote

[13] **Customs Duties**
Time and distance factors; checkpoints
**Customs Duties**
Scope and Nature; Successive or Secondary Searches

Law enforcement agent's imaging and search of entire contents of alien's laptop computer, aided by specialized forensic software, over period of unlimited duration and conducting examination of unlimited scope, for the purpose of gathering evidence of pre-existing export violation, was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of alien's privacy and so disconnected from not only the considerations underlying the breadth of government's authority to search at border, but also the actual border itself, that it was unreasonable and violative of alien's Fourth Amendment rights. U.S. Const. Amend. 4.

Cases that cite this headnote

[14] **Aliens, Immigration, and Citizenship**
Checkpoints
**Customs Duties**
Time and distance factors; checkpoints

Concept of "border" search, for Fourth Amendment purposes, extends beyond the physical boundary itself to the functional equivalent of border, which may include an established station near the border or other nearby convenient locations. U.S. Const. Amend. 4.

Cases that cite this headnote

**Attorneys and Law Firms**

Frederick Walton Yette, U.S. Attorney's Office, Washington, DC, for United States of America.

***MEMORANDUM OPINION AND ORDER***

AMY BERMAN JACKSON, United States District Judge

***1** In this case involving the enforcement of export control laws and the trade embargo with Iran, defendant Jae Shik Kim has moved to suppress the evidence the United States harvested from a laptop computer it seized from him when he was departing the country through Los Angeles International Airport. Kim is a Korean businessman with business operations in both Korea and California, and in October of 2012, investigators with the Department of Homeland Security obtained information that he was involved in a previous shipment of controlled articles to a Chinese businessman in Korea, who then forwarded them to customers in Iran. The Special Agent handling the investigation decided to search Kim's laptop computer for evidence the next time Kim came to the United States, and in December 2012, he obtained the computer from Kim before permitting him to board his flight home. The next day, the laptop was shipped to an agency forensic specialist in San Diego, who created an identical copy of the hard drive, which was then searched using specialized software and a list of keywords. The thousands of files that were extracted from the keyword search were then burned onto a DVD and returned to the case agent for further review.

After incriminating emails were uncovered through that process, the agent sought and obtained a warrant based upon the content of the emails to conduct the search of the hard drive that had already been completed and to seize the emails that had already been reviewed. Those emails now form a part of the basis of this prosecution, and Kim moves to suppress that evidence, arguing that his rights under the Fourth Amendment of the Constitution have been violated.

The government points to its plenary authority to conduct warrantless searches at the border. It posits that a laptop computer is simply a "container" that was examined pursuant to this authority, and it submits that the government's unfettered right to search cargo at the border to protect the homeland is the beginning and end of the matter.

But to apply those principles under the facts of this case would mean that the border search doctrine has no borders. The search of the laptop began well after Kim had already departed, and it was conducted approximately 150 miles away from the airport. The government engaged in an extensive examination of the entire contents of Kim's hard drive after it had already been secured, and it accorded itself unlimited time to do so. There was little or no reason to suspect that criminal activity was afoot at the time Kim was about to cross the border, and there was little about this search—neither its location nor its scope and duration—that resembled a routine search at the border. The fundamental inquiry required under the Fourth Amendment is whether the invasion of the defendant's right to privacy in his papers and effects was reasonable under the totality of the circumstances, and the Court finds that it was not.

**PROCEDURAL HISTORY**

On March 28, 2013, Kim and his company, Karham Eng. Corp. ("Karham"), were indicted for violations of a number of statutes, including the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C § 1701 *et. seq.*, the Arms Export Control Act ("AECA"), 22 U.S.C. § 2778, and the International Traffic in Arms Regulation ("ITAR"), 22 C.F.R. pts. 120–30. Indictment [Dkt. # 1]. These laws and regulations govern economic sanctions imposed by the United States against certain countries, such as Iran, and the export of certain "defense articles" from the United States. The United States alleges that from around December 2007 through March 2010, defendants conspired to export defense articles without the required export licenses for sale to intermediaries in China and Korea and ultimate customers in Iran. Indictment ¶ 17. The defense articles at issue—six Q–Flex Accelerometers, Models QA–2000–10, QA–2000–20, or QA–3000—are aircraft parts manufactured by Honeywell Aerospace which are used in aircraft and missile navigation systems. Indictment ¶¶ 3, 16(1), 17(3). They appear on the export control list, and an export license is required before they may be exported legally from the United States. 22 U.S.C. § 2778(b)(2); 22 C.F.R. pt. 123.1(a).

***2** On March 2, 2015, defendants filed the instant motion to suppress. Defs.' Mot to Suppress Evidence [Dkt. # 35] ("Defs.' Mot."). The parties briefed the motion, Gov't's Opp. to Defs.' Mot. [Dkt. # 37] ("Gov't Opp."); Defs.'

Reply in Supp. of Defs.' Mot. [Dkt. # 38] ("Defs.' Reply"), and the Court held an evidentiary hearing on April 7 and 8, 2015, at which the following facts were established.

## FACTUAL BACKGROUND

### A. The Government's Investigation of Bin Yang

In 2011, Special Agent Kevin Hamako of the Department of Homeland Security ("DHS") Homeland Security Investigations office was investigating a Chinese national, Bin Yang, also known as Raymond Yang, for export control violations, specifically the unlawful export of accelerometers to China and Iran. Mots. Hr'g Tr., April 7, 2015 ("4/7 Tr.") at 7. As part of the investigation, Special Agent Hamako worked with an undercover agent who communicated with Yang by email and telephone. 4/7 Tr. at 14.

On April 1, 2011, Yang sent the undercover agent an email asking to obtain Honeywell QA–3000–30's from him, and he offered: "Because my uncle has a sudden schedule to USA, he may could meet you and pay you." Report of Investigation, No. 107, May 20, 2011, Gov't Ex. 3 ("May 2011 ROI") at 3.

On April 4, 2011, Yang sent the undercover agent another email stating, "My uncle just has his sudden trip to US, he may meet you and only see the goods and maybe pay you." May 2011 ROI at 3.

In an April 5, 2011 telephone conversation between Yang and the undercover agent, Yang again volunteered that he had a contact who would be traveling to the United States who could inspect the QA–3000 accelerometers that Yang hoped to buy. May 2011 ROI at 3; 4/7 Tr. at 15–16. Yang proposed to have his "uncle" travel to the United States, inspect the accelerometers, and provide payment for them. 4/7 Tr. at 15–16. He also stated he did not want his "uncle" to physically carry the items out of the country because he was afraid that U.S. customs officials would discover them. 4/7 Tr. at 16; *see also* Report of Investigation, No. 114, Jun. 22, 2011, Gov't Ex. 2 ("Jun. 2011 ROI") at 3 (detailing information about the April 5, 2011 telephone call). At that point, the unidentified "uncle" became a further subject of the investigation. 4/7 Tr. at 16.

On April 27, 2011, Special Agent Hamako obtained and executed a warrant to search and seize Yang's emails, and on May 12, 2011, he received the emails. May 2011 ROI at 3; *see also* 4/7 Tr. at 17. The emails included several communications with "Uncle Kim" atJS@karham.co.kr:

> • an email dated June 24, 2010 from Yang to Kim that stated, "There is an inquiry from a domestic client for Honeywell products. It is not for military application and I confirm the end user is not Iranian," to which Kim responded on the same day, "Thanks! Raymond, I will also check the Honeywell parts whether [w]e can buy them."
>
> • emails between Yang and Kim from July 2010 relating to the purchase of various items not subject to export controls
>
> • an email from almost a year later, dated March 28, 2011, in which Yang asked Kim if he could identify a source for other parts that are not subject to controls: "Dear Uncle Kim Hi. I have the inquiry for Honeywell QAT 185/160 model, about 150pcs for each model per year. 3pcs is a completed unit. First trial order, the client will buy 9pcs for each model as a start. Do you have any good sources to supply them." On the same date, Kim responded, "Now, Mr Ji are checking it with our USA office. And also, Tomorrow, I will go to USA with Mr. Ji and stopped in USA office. We will check it again and feed back you soon."
>
> ***3** • an email from Yang to Kim dated April 1, 2011, stating: "I see that you will go to U.S.A, it is very good. For your reference, I get a message that there is supplier could supply us some stocks of QA3000. But I don't have successful business with him before, but we could buy his goods if his stocks are ok. Dear Uncle Kim, can you please have a check if you agree. We could pay you, so you can buy it in USA.... QAT 185 and 160 are not sensitive products, and if you can supply, we could buy from you, and there is no worry to pay the deposit, because I trust my uncle."

May 2011 ROI at 4–6.

On April 5, 2011, Yang had the recorded telephone call with the undercover agent described above in which he proposed that his "uncle" could inspect the parts Yang hoped to buy. As of May 2011, though, the agents were aware that Yang's inquiry to Kim had borne no fruit and the undercover operation was over. 4/7 Tr. at 72 (stating the agents knew "fairly soon after, within maybe a couple of weeks" that the operation was not going ahead).

**B. The Identification of "Uncle Kim" and his Companies**

On June 21, 2011, Special Agent Hamako was able to identify "Uncle Kim" as defendant Jae Shik Kim by searching a government database for theJS @karham.co.kr email address. 4/7 Tr. at 21–22; Jun. 2011 ROI at 3–4. The email address appeared in U.S. State Department records on a non-immigrant visa application submitted by Kim. 4/7 Tr. at 21–22; Jun. 2011 ROI at 3. The application provided Special Agent Hamako with other information about Kim, including his date of birth, passport number, and nationality. Jun. 2011 ROI at 3–4; 4/7 Tr. at 22.

From the visa application, Special Agent Hamako also determined that Kim was president of corporate defendant Karham. 4/7 Tr. at 22. Through further research, he learned that Karham was located in South Korea and Stevenson Ranch, California, and that Karham shared its Stevenson Ranch, California address with a company called Apex Components. 4/7 Tr. at 22–23; *see also* Jun. 2011 ROI at 3–5 (providing information about the identification of Kim).

Special Agent Hamako researched Karham and Apex Components and found that Karham was involved in the export and sale of equipment used in the oil industry and petrochemical industries, including types of meters. 4/7 Tr. at 24. On a web-based government database, Special Agent Hamako found approximately thirty-nine shipper's export declarations ("SEDs") from Karham for the export of meters from the United States to Australia and South Korea. 4/7 Tr. at 24. He found eight shipper's export declarations from Apex Components, which also showed exports of various industrial equipment from the United States to South Korea. 4/7 Tr. at 25.

Finally, Special Agent Hamako found travel records showing that defendant Kim arrived in Los Angeles International Airport ("LAX") on April 2, 2011, and departed LAX for Narita, Japan on April 14, 2011. Jun. 2011 ROI at 4; *see also* 4/7 Tr. at 26.

**C. Yang's Arrest and Debrief**

Early the following year, in January 2012, Yang was arrested and, in May 2012, he was extradited from Bulgaria to the United States. 4/7 Tr. at 9. He agreed to be debriefed by U.S. authorities in an effort to ameliorate his sentence. 4/7 Tr. at 9; *see also* Search Warrant, Ex. B to Defs.' Mot. [Dkt. # 35–2] ("Search Warrant"); Aff. in Supp. of Appl. for Search Warrant, Ex. B to Defs.' Mot. [Dkt. # 35–2] ("SW Aff."), at 7 n.1.

On October 18, 2012, Special Agent Hamako interviewed Yang. 4/7 Tr. at 9; *see also* Report of Investigation No. 146, Nov. 15, 2012, Gov't Ex. 1 ("Nov. 2012 ROI") at 3–5 (reporting results of the Yang debrief). Yang told investigators that at some point in 2008 or 2009, he purchased six QA–2000 accelerometers from Kim, which were shipped to him in China without an export license. 4/7 Tr. at 10. Yang said that once he received the accelerometers, two of his Iranian customers traveled from Iran to China to receive them directly. *Id.* Yang told Special Agent Hamako that Kim purchased the accelerometers through his connections in the United States, and they were shipped from the United States to China. 4/7 Tr. at 11; Nov. 2012 ROI at 3. While this is not reflected in the report of the interview, Special Agent Hamako testified that Yang also told him that Kim knew the accelerometers were destined for customers in Iran. 4/7 Tr. at 11.

***4** As a result of the Yang interview, Special Agent Hamako decided to conduct what he characterized as a border search of Kim's electronic devices "as he was leaving the U.S. on his next travel." 4/7 Tr. at 110.

> I wanted to know when [Kim] was returning to further my investigation in the sense that I wanted to be ready to conduct more proactive steps if he was in the U.S.; specifically, to include a border search, surveillance, or other activities to determine if he was engaged in any potential criminal activity while in the United States.

4/7 Tr. at 33. At that time, it was the agent's understanding that no suspicion was required to conduct a border search of any items Kim might be carrying, including electronic devices. 4/7 Tr. at 32.

Because of the ongoing investigation, Kim's name was in DHS's case management system, which meant Special Agent Hamako would receive an automatic email if Kim was booked on a flight to or from the United States. 4/7 Tr. at 32–33. Some time later, the agent received an email notifying him that Kim was going to return to the United States in November 2012, and that he would be departing LAX for South Korea on December 5, 2012. 4/7 Tr. at 33.

**D. The December 5, 2012 Search of Kim**

Special Agent Hamako testified that while he understood that he had the authority to conduct a border search of

Kim without any level of suspicion that Kim was engaged in criminal activity, 4/7 Tr. at 34, he had grounds for that suspicion in any event.

> At that time my suspicion was based on the debriefing of Yang in which Yang stated he had previously successfully procured ITAR controlled accelerometers from Mr. Kim, as well as the fact that Mr. Kim's company appeared to be engaging in exports from the U.S. to South Korea and other foreign locations, as well as the fact that, more recently, Mr. Yang had asked Mr. Kim to view products in the U.S., inspect them and pay for them.

4/7 Tr. at 35. Special Agent Hamako stated that although he knew Yang was incarcerated, he "wasn't sure if Mr. Kim was in contact with other individuals who might be seeking to illegally procure U.S. goods," and that his goal was to ascertain whether Kim had other customers. 4/7 Tr. at 35–36. Under questioning by the prosecutor at the hearing, the agent agreed that he also thought it was reasonable to believe that records of the 2008 transactions, including emails, could still be saved on the computer. 4/7 Tr. at 38–39.

Special Agent Hamako said he intended to conduct a border search of Kim as he departed the country rather than as he entered the country,

> because if I believed at that time that he was traveling to the U.S. and might be conducting criminal activity while he was in the U.S., such as procuring products or attempting to set up subsequent deals, I would want to capture that information after he had done so, rather than before he had conducted any such activity. So, conducting a border search on the inbound side could cause him to decide not to conduct whatever activities or operations he might have been planning. Whereas, conducting the border search as he was leaving, in our view, would be more likely to obtain evidence of any criminal activity he had conducted during his trip.

***5** 4/7 Tr. at 34–35. He added that based on Yang's statements and Karham's general business activities, he was "concerned that [Kim] could be involved in further activity in the [S]tates regarding illegal exports." 4/7 Tr. at 39. But he testified that he did not know at the time—and he does not know now—what Kim did while he was in the United States between November 25 and December 5, 2012, and that he did not conduct any surveillance or take any steps to find out before carrying out his plan to obtain the laptop. 4/7 Tr. at 81.

On December 5, 2012, working with a LAX duty agent and Customs and Border Protection officers, Special Agent Hamako conducted the planned search of Kim as he departed the country. 4/7 Tr. at 40. First, he searched Kim's checked luggage, which was located behind the check-in counter with Korean Airlines. *Id.* He found no accelerometers or contraband. 4/7 Tr. at 82–83. He did find a small plastic bag containing plastic o-rings, some unidentified industrial metal objects, and some product brochures. 4/7 Tr. at 40–41, 90. The agent was not able to identify the applications of these particular o-rings because he was not an aircraft parts expert, but said that he knew "in other cases the Iranian Air Force had been seeking o-rings for their aircraft," and so he thought that these small plastic ones "could be" on the munitions list, and he kept them to determine their application. 4/7 Tr. at 41–42. He later spoke with the manufacturer, and determined "it was very unlikely that they were export controlled items," and shipped them back to Kim. 4/7 Tr. at 43. Special Agent Hamako also testified that the metal objects in the luggage did not appear to have any moving parts or sensors or electronics and may have been a tripod, and the product brochures "didn't seem to be pertinent at the time." 4/7 Tr. at 87–88, 90. So he did not retain either the metal objects or the brochures and did not photograph or document what they were. 4/7 Tr. at 88–89.

Next, Special Agent Hamako stopped Kim on the jetway between the gate and the airplane as Kim was boarding his flight. 4/7 Tr. at 40, 43. He identified himself and asked Kim if he had any electronics, to which Kim responded that he had a laptop. 4/7 Tr. at 44. Special Agent Hamako told Kim that he would be detaining the laptop pursuant to a border search and that he would return it once the search was complete. *Id.* He also told Kim that he would be detaining the o-rings until their export control status was determined. *Id.* Special Agent Hamako testified that he did not have an interpreter during the encounter with Kim because he did not anticipate that he was likely to say anything incriminating. 4/7 Tr. at 94.

> My goal at that time wasn't to

> conduct an in-depth interview or subject interview of Mr. Kim, reading him his rights or anything like that, since my main goal was to obtain his electronics and then let him go on his way.

4/7 Tr. at 95. This is precisely what took place, and Kim boarded his flight. 4/7 Tr. at 45.

Special Agent Hamako did not turn the laptop on or review its contents in any way during his search of Kim at LAX. 4/7 Tr. at 45. He explained that "it would be inappropriate to search his laptop without—without an individual who's qualified to preserve the contents of the laptop. Because if I were to turn on the laptop and just begin searching it there, that would be altering the information on the laptop and could render any evidence I found on it tainted or otherwise questionable, since I would be modifying the contents of the laptop by conducting searches on it. And also, because based on the time available, it could have taken who knows how long." 4/7 Tr. at 45; *see also* 4/7 Tr. at 115 (stating that "conducting a live search on his computer would have necessarily changed and altered the contents of the laptop, so I would not have conducted such a search"). Special Agent Hamako testified, "[M]y main goal was to obtain any electronics that he had on his person at that time." 4/7 Tr. at 94.

**E. The Search of Kim's Computer**

***6** On December 6, 2012, Special Agent Hamako submitted Kim's laptop to Special Agent David Marshall of the Homeland Security Investigation San Diego Computer Forensics Group. Report of Investigation, No. 147, Dec. 11, 2012, Gov't Ex. 5 ("Dec. 2012 ROI") at 1, 3; Mots. Hr'g Tr., April 8, 2015 ("4/8 Tr.") at 7–8;[1] *see also* 4/7 Tr. at 99–100. Special Agent Hamako "requested a border search of the laptop" from Special Agent Marshall. 4/8 Tr. at 8.

To carry out Special Agent Hamako's request, Special Agent Marshall removed the hard drive from Kim's laptop and created a forensic image, or a duplicate copy, of it. 4/8 Tr. at 8. To do this, Special Agent Marshall connected a piece of hardware "about the size of a shoebox" to the laptop hard drive: the hardware creates "an exact copy, reading every single bit, as we call it, every single piece of data on the hard drive and making a copy of that for me to analyze later on." 4/8 Tr. at 8–9.

The imaged copy included all files from both the allocated and unallocated space on the computer, which Special Agent Marshall explained as follows:

> Allocated space, in general, means space in your hard drive where ... files are living, files that you see on your desktop, maybe a photo of a family vacation or Word documents. Unallocated space refers to space that's not currently being used by—let's say it's Windows, by Windows for any files. And when you delete a file, it goes into unallocated space.... [U]nallocated space is space that's not currently being used by the computer.

4/8 Tr. at 9.

Special Agent Marshall placed the hard drive back into Kim's laptop and returned the laptop to Special Agent Hamako on December 7, 2012. 4/8 Tr. at 8.[2]

Also on December 7, 2012, Special Agent Marshall employed a software program called EnCase to export files from Kim's computer. 4/8 Tr. at 10; *see also* Dec. 2012 ROI at 4 (stating that he used commercially available email analysis software to export files). He used EnCase to export six Microsoft Outlook email containers,[3] 8,184 Microsoft Excel spreadsheets, 11,315 Adobe PDF files, 2,062 Microsoft Word files, and 879 Microsoft PowerPoint files from the image. Dec. 2012 ROI at 4; *see also* 4/8 Tr. at 11.

Special Agent Marshall used another program, Intella, to process the files. 4/8 Tr. at 10; *see also* Dec. 2012 ROI at 4. He testified that Intella is a powerful piece of software with a variety of capabilities, including the ability to search the text of emails that are not otherwise searchable. 4/8 Tr. at 31. It also indexes and categorizes emails:

> [A]n e-mail container can contain thousands of e-mails. So Intella will go through and open up the e-mail, and what we call index and categorize the e-mail. So it looks at all the e-mail information, the to and the from, the dates, things like that, the attachments, and it processes those and categorizes all that information so that the user can then go in and see all the e-mails from a certain person, you know, or to a certain person or on a date.

***7** 4/8 Tr. at 31–32. And according to Special Agent Hamako, it would have been "impractical" to use the search function in Outlook instead; given the investigators' search methodologies, "Intella is more efficient." 4/7 Tr. at 105.

These files were copied to a "case agent review" laptop for Special Agent Hamako to review. 4/8 Tr. at 11. When Special Agent Marshall saw the number of files on the laptop, he asked Special Agent Hamako to give him a keyword list to use to "filter down the amount of information for him to review." 4/8 Tr. at 11.

On December 10, 2012, Special Agent Hamako gave Special Agent Marshall a list of twenty-two keywords: QA–2000, QA–3000, G–2000, 7270A, accelerometers, gyroscope, angular, sensor, Honeywell, Endevco, Northrop, Grumman, ITAR, sensitive, export, shipment, military, aircraft, missile, satellite, ballistic, and nuclear. 4/8 Tr. at 12–13. Using these keywords to screen the files on Kim's laptop, Special Agent Marshall found approximately 5,900 files that had a keyword match. 4/8 Tr. at 13. He burned the files to a DVD and gave the DVD to Special Agent Hamako, along with the case agent review laptop. Dec. 2012 ROI at 4; 4/8 Tr. at 13.

The next day, on December 11, 2012, Special Agent Marshall exported all of the picture files, which can include images of documents and not simply photographs, that were located in the allocated space of the computer—approximately 24,900 .jpg files. 4/8 Tr. at 13–14; Dec. 2012 ROI at 4. He copied all of those onto another DVD and gave the DVD to Special Agent Hamako. 4/8 Tr. at 13–14; Dec. 2012 ROI at 4.

Special Agent Hamako then spent "[s]everal days" reviewing the files obtained from Kim's computer, conducting keyword searches of the emails and documents. 4/7 Tr. at 47; Search Warrant ¶ 17 (stating that Special Agent Hamako received the emails on December 10, 2012 and reviewed them until December 19, 2012). He found emails consistent with the 2008 transaction Yang described during the interview, and those form the basis for the criminal charges in this case. 4/7 Tr. at 47–48.

**F. The Search Warrant**

On January 13, 2013, Special Agent Hamako filed an application for a search warrant in the U.S. District Court for the Southern District of California. Search Warrant. He provided an affidavit with the application, in which he stated his belief that there was "probable cause to believe that evidence relating to violations" of the ACEA, IEEPA, the Iranian Transactions Regulations, and other statutes would be contained in the files on Kim's laptop. SW Aff. ¶ 10. The affidavit states that the laptop was detained during a border search, that the government had imaged the laptop, and that Special Agent Hamako reviewed emails obtained from the laptop for ten days. SW Aff. ¶¶ 16–17. The affidavit then describes the contents of emails between Kim and Yang from December 2007 through April 2008, showing that Kim helped Yang purchase six accelerometers without the required export control license, and that the items were to be forwarded to Iran. SW Aff. ¶¶ 18–40.

The application stated further that, "[w]ith the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures" to search Kim's computer: forensic imaging, which the affidavit acknowledged had already occurred, and identification and extraction of relevant data. SW Aff. ¶¶ 43–50. Special Agent Hamako explained:

> ***8** Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment and software. There are literally thousands of different hardware items and software programs, and different versions of the same program, that can be commercially purchased, installed and custom-configured on a user's computer system.
>
> * * *
>
> Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits.... Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue: who created it, when and how it was created or downloaded or copied, when was it last accessed, when was it last modified, when was it last printed and when it was deleted.... Moreover, certain file formats do not lend themselves to keyword searches.... Many common electronic mail, database and spreadsheet applications do not store data as searchable text.

SW Aff. ¶¶ 45–46.

According to the agent's affidavit, the "mind-boggling" amount of data stored on computers makes analyzing the data "increasingly time-consuming." SW Aff. ¶ 48. Therefore, Special Agent Hamako predicted that "[t]he identification and extraction process ... may take weeks or months." SW Aff. ¶ 49. He also averred that the

government "has not attempted to obtain this data by other means, except 1) through border search authority ... and 2) some email communications between Kim and Yang ... previously obtained pursuant to court authorized search warrants of Yang's email accounts." SW Aff. ¶ 52.

On January 16, 2013, the U.S. District Court for the Southern District of California signed the warrant. Search Warrant.

But Special Agent Hamako and Special Agent Marshall each testified that after the search warrant was obtained, no further searches or analyses were undertaken. 4/7 Tr. at 51 ("THE COURT: Was there some new, different program that was applied after you got the warrant that did something more to the computer, or is it just a matter that you actually seized the e-mails? [Special Agent Hamako]: That's correct, Your Honor. We didn't use any different programs after obtaining the search warrant."); 4/8 Tr. at 23 ("THE COURT: Did you do anything to—either the complete image that you had created or the case agent's laptop, did you do any further searching or application of any programs after the search warrant was obtained? [Special Agent Marshall]: No.").

## ANALYSIS

The government argues first and foremost that a laptop is nothing more than a sort of container, and that the agents had full authority to scour its contents without the need for a warrant or a showing of any particular level of suspicion simply because the search was initiated at the border. Gov't Opp. at 6, citing, *inter alia, United States v. Ramsey,* 431 U.S. 606, 97 S.Ct. 1972, 52 L.Ed.2d 617 (1977), and 19 U.S.C. § 1581.[4] But the government also suggests that a search which took place at LAX, involving a passenger traveling to and from California, should be assessed utilizing the Ninth Circuit precedent set forth in *United States v. Cotterman,* 709 F.3d 952 (9th Cir.2013). 4/8 Tr. at 86; Gov't Opp. at 10, n.9, 11 n.11.

***9** In *Cotterman,* the Ninth Circuit announced that reasonable suspicion was required before investigators could undertake the forensic examination of a computer hard drive as part of a search that began as a cursory review at the border. 709 F.3d at 957. In this case, the government argues both that no suspicion was necessary since this was an ordinary, reasonable border search that can be distinguished from the forensic examination that took place in *Cotterman,* and also that the necessary suspicion was present. Gov't Opp. at 10–14.

Neither the Supreme Court nor the D.C. Circuit has weighed in on this issue, so there is no binding precedent to be applied by this Court.[5] In 2014, a District Court in Maryland also concluded that reasonable suspicion was needed to justify a forensic search of a defendant's electronic data storage devices. *United States v. Saboonchi,* 990 F.Supp.2d 536, 539 (D.Md.2014). And later that year, another court in this District was asked to apply the *Cotterman* rule to a search of a laptop seized from a passenger flying into LAX, but in that case, the court determined that it was not necessary to reach the constitutional question of whether reasonable suspicion was required because it found that such suspicion was present in any event. *United States v. Hassanshahi,* No. 13–0274(RC), —— F.Supp.3d ——, ——, 2014 WL 6735479, at *12 (D.D.C.2014). In an effort to follow that sensible approach, this Court took up the reasonable suspicion question first.

### I. Was there reasonable suspicion to support the search of Kim's laptop?

[1] [2]The Supreme Court has defined reasonable suspicion as "a particularized and objective basis for suspecting the particular person stopped of criminal activity." *United States v. Cortez,* 449 U.S. 411, 417–18, 101 S.Ct. 690, 66 L.Ed.2d 621 (1981). The standard is met when a law enforcement officer can point to "specific and articulable facts," which, when considered together with the rational inferences that can be drawn from those facts, indicate that criminal activity "may be afoot." *Terry v. Ohio,* 392 U.S. 1, 21, 30, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968). As the government has pointed out in this case, a court's determination of whether the officer had reasonable suspicion must be based upon the totality of the circumstances. *See United States v. Arvizu,* 534 U.S. 266, 273, 122 S.Ct. 744, 151 L.Ed.2d 740 (2002); *see also Cortez,* 449 U.S. at 418, 101 S.Ct. 690 (recognizing that law enforcement agents will draw upon their training and experience to piece together subtle clues that may seem innocent to others); *United States v. Tiong,* 224 F.3d 1136, 1140 (9th Cir.2000).

[3]But what is it that the officer must reasonably suspect? Neither party focused in on that issue, but a review of the cases decided in the wake of *Terry* makes it clear that the reasonable suspicion standard relates to ongoing or imminent crime. *See Cortez,* 449 U.S. at 417, 101 S.Ct. 690 ("An investigatory stop must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity."); *United States v. Edmonds,* 240 F.3d 55, 59 (D.C.Cir.2001) ("[T]he issue is whether a reasonably prudent man in the circumstances would be warranted in his belief that the suspect is

breaking, or is about to break, the law.") (citation and internal quotation marks omitted). Therefore, if this Court were to determine, after considering the totality of the circumstances, that a reasonably prudent officer would have been justified in his belief that Kim was engaged in ongoing criminal activity at the time he was stopped at LAX, then the search would have been lawful under the *Cotterman* standard. And then, the Court could adopt the approach taken by the District Court in *Hassanshahi* and find the constitutional question of whether the search of the computer required reasonable suspicion to be moot.

***10** [4]In this case, though, the Court is troubled by the lack of particularized grounds to believe that this defendant was engaged in criminal activity at the time he was exiting the United States. First of all, there is no question that the decision to conduct the search was not made on that basis: Special Agent Hamako candidly testified that he made the decision to obtain the laptop and search it for evidence of the alleged conspiracy with Yang based upon his understanding that such a search required no level of suspicion at all. 4/7 Tr. at 34. He testified that once he had information from Yang that defendant Kim had been his source in 2008, he decided to conduct what he termed a "border search" the next time Kim came to the United States for the purpose of obtaining the laptop. 4/7 Tr. at 33–34, 94. And he made that decision before he knew when Kim would be travelling to the United States, whether he would be travelling, or why, and in the absence of any information whatsoever about what Kim would or did do while he was in the country. 4/7 Tr. at 81, 33.[6] Even after the agent had been notified that Kim was on his way, he took no steps to monitor Kim's activities in any way while he was in the United States. 4/7 Tr. at 81.

Notwithstanding these undisputed facts, the government takes the position that the agent had reasonable suspicion to search the laptop under the *Terry* standard adopted in *Cotterman* based upon the totality of the circumstances. It argued in its opposition to the motion to suppress, "Yang's admission that he previously conspired with Kim ... created reasonable suspicion that Kim had been, and perhaps still was, involved in illegal activity." Opp. at 12. And, "SA Hamako had reason to suspect that Kim would be crossing the border with a laptop that still contained evidence of his earlier criminal conspiracy with Yang, as well as any recent illegal activities." Gov't Opp. at 14.

But the government's use of such language as "perhaps" and "any" was not at all reassuring, as it served to highlight how thin the showing is in this case. And the agent's testimony confirmed that gathering evidence of a completed crime was the central motivation here. *See* 4/7 Tr. at 95 ("[M]y main goal was to obtain his electronics and then let him go on his way.").

The government points out that the subjective intent of the agent is irrelevant. Gov't Opp. at 12 (stating that "only a 'minimal level of objective justification' " is required), quoting *Hassanshahi,* —— F.Supp.3d at ——, ——, 2014 WL 6735479, at *16. And at the hearing on the motion, it posited that there was reasonable suspicion to support the search based upon the following circumstances: the preexisting ongoing investigation into Kim's involvement in Yang's 2008 transaction with Iran; the fact that Kim's name came up in connection with the more recent attempt to engage Yang in an undercover transaction; the fact that Kim did travel to the United States at the time Yang said he would be traveling; the business relationship between Kim and Yang; and the discovery of the o-rings. 4/8 Tr. at 77–78; Gov't Opp. at 12–14.

[5]But even if one credits Special Agent Hamako's testimony that Yang told him Kim knew that the items shipped in 2008 were bound for Iran, *see* 4/7 Tr. at 10–11—despite the agent's failure to mention that key detail in either his contemporaneous report or the affidavit he submitted in support of the search warrant, *see* Nov. 2012 ROI; SW Aff.—and even if one credits Yang's account of the previous transaction, evidence of prior criminal conduct alone is not sufficient to give rise to reasonable suspicion. *Hassanshahi,* —— F.Supp.3d at ——, ——, 2014 WL 6735479, at *14, citing *United States v. Johnson,* 482 Fed.Appx. 137, 148 (6th Cir.2012); *United States v. Walden,* 146 F.3d 487, 490 (7th Cir.1998). This is particularly true under the circumstances of this case, where the only evidence of more recent activity was Yang's inquiry to Kim on behalf of the undercover officer, which did not result in any action on Kim's part. As of December 5, 2012, all that Special Agent Hamako knew about ongoing activity was that Yang had contacted Kim and the approach had quickly come to a dead end, that Yang was under arrest and no longer conspiring with anyone, and that the search of Kim's luggage revealed no accelerometers or obviously controlled items.

***11** The government points to Kim's previous travel and the fact that exports to Yang and others were a regular part of his business, but this is the sort of evidence the Supreme Court has cautioned against according much weight in the reasonable suspicion analysis because it "describe[s] a very large category of presumably innocent travelers." *Reid v. Georgia,* 448 U.S. 438, 441, 100 S.Ct. 2752, 65 L.Ed.2d 890 (1980).

Further, it is difficult to find that the o-rings had anything other than marginal importance. The testimony was that they were small and plastic, and it was not obvious to an agent who was well trained in the contents of the

munitions list that they were listed at all. 4/7 Tr. at 41, 83–86. Indeed, they were of so little value to his investigation that the agent did not retain them, photograph them, or even describe them in any report. 4/7 Tr. at 86–87. According to Special Agent Hamako, that was because his "main goal was to obtain [Kim's] electronics and then let him go on his way." 4/7 Tr. at 95. And the agent testified that that the decision to search the laptop well preceded the discovery of the o-rings in any event. 4/7 Tr. at 110–12.

The agent's answers to questions posing obvious propositions that do not depend on sophisticated investigatory experience, *see* 4/7 Tr. at 48 ("Q.... [I]f you knew that Mr. Yang and Mr. Kim had conspired to export the accelerometers Mr. Yang told you about, did you have reason to suspect Mr. Kim could have had other people he was working with? A. That's correct. It's common in our investigations that individuals will have different coconspirators and customers for goods, ...."), did little to lift the evidence out of the realm of hunch or speculation, particularly given the fact that the one known prior alleged conspiracy did not involve entry into or exit from the United States at all. 4/7 Tr. at 10–11; *see also id.* at 53 (agent admitted on cross examination that while it was a "possibility" that Kim had other co-conspirators, he had no evidence of any other questionable transactions besides the one with Yang).

Looking at all of the circumstances presented, then, while it is a close case, it seems clear to the Court that the search of the laptop was predicated upon the agent's expectation that the computer would contain evidence of past criminal activity, but there was no objective manifestation that Kim was or was "about to be, engaged in criminal activity" at that time. *Cortez,* 449 U.S. at 417, 101 S.Ct. 690; *see also* 4/7 Tr. at 32–33 (after the Yang debriefing, the agent arranged to be notified of any planned travel by Kim so that he could take proactive steps such as surveillance or a border search "to determine *if* he was engaged in any potential criminal activity while in the United States") (emphasis added). With respect to ongoing activity, the search was nothing more than a fishing expedition to discover what Kim might have been up to. *See also* 4/7 Tr. at 35–36 ("Q [by AUSA]. Now, you knew that Mr. Yang was locked up and could not engage in activity with Mr. Kim, correct? A. That's correct. However, based on the fact that I wasn't able to search Mr. Kim's e-mail, I wasn't sure if Mr. Kim was in contact with other individuals.... So, at that time I wasn't sure if Mr. Yang was Mr. Kim's only customer. Q. Were you intending to investigate whether he had other customers? A. I was. That was a primary goal of our investigation.") Indeed, when Special Agent Hamako took the time to detail the evidence against Kim in the affidavit in support of the search warrant, he did not include any facts or allegations related to anything that was supposedly going on in December of 2012. He simply averred, "[a]fter his arrest, Yang stated that he had previously purchased six Honeywell QA–2000 accelerometers from Kim." *See* SW Aff. ¶ 15. And therefore, this case is distinguishable from *Cotterman* and the decision from this District in *Hassanshahi.*

***12** The court in *Cotterman* noted that the agents at the Mexican border made their initial decision to search the defendant's belongings on his way into the country after the Treasury Enforcement Communication System ("TECS") revealed that the defendant was a known sex offender. 709 F.3d at 957. Based on the TECS alert, the border agents believed that the defendant had a prior conviction for child pornography, that he was possibly involved in child sex tourism, and that he was arriving from a country associated with that activity. *Id.* at 957, 968–69.[7] The agents' review of Cotterman's passport confirmed that he travelled frequently out of the country. *Id.* at 968. The Immigration and Customs Enforcement ("ICE") "field office specifically informed [the border agent] that the alert was part of Operation Angel Watch, which targeted individuals potentially involved in sex tourism and alerted officials to be on the lookout for laptops, cameras and other paraphernalia of child pornography." *Id.* at 969. A search of the Cottermans' vehicle produced two laptop computers and three digital cameras, and an initial inspection of the devices on the scene revealed what appeared to be personal photos, as well as a set of password-protected files on the laptop. *Id.* at 957–58.

While neither the prior conviction nor the use of password-protected files alone would have sufficed, the court concluded that "Cotterman's TECS alert, prior child-related conviction, frequent travels, crossing from a country known for sex tourism, and collection of electronic equipment, plus the parameters of the Operation Angel Watch program, taken collectively, gave rise to reasonable suspicion of criminal activity." *Id.* at 969. The court added that where there are other indicia of criminal activity, the password protection of individual files—as opposed to the commonplace use of a password to protect an entire device—could be considered as part of the totality of the circumstances, but only in a situation, such as a child pornography case, where the encryption or protection of files would have some relationship to the suspected criminal activity. *Id.* at 969. Given the combination of the TECS hit and the discovery of the inaccessible files, and crediting the agents' observations and experience, the Ninth Circuit found that "[t]he border agents 'certainly had more than an inchoate and unparticularized suspicion or hunch' of criminal activity

to support their decision to more carefully search for evidence of child pornography." *Id.* at 970, quoting *United States v. Montoya de Hernandez,* 473 U.S. 531, 542, 105 S.Ct. 3304, 87 L.Ed.2d 381 (1985).[8]

Here there was nothing about Kim's particular travel plans that would arouse suspicion; he was returning to his home in Korea and he was known to have business operations within the United States. And, the agent did not even open the laptop—which did not turn out to contain password protected files in any event—on the scene. So while in *Cotterman,* the court characterized the forensic search as one that grew out of observations made during the initial cursory examination at the border, the search here was not prompted, even in part, by anything that raised the agent's level of concern upon a first glance at the device at the border. *Compare Cotterman,* 709 F.3d at 969–70 (pointing to the password-protected files on Cotterman's computer as a circumstance justifying the scope of the search).

***13** In *United States v. Hassanshahi,* the court found that there was reasonable suspicion that the defendant was engaged in efforts to violate the trade embargo with Iran, which supported the decision to conduct a forensic search of his laptop upon his return to the United States in January 2012 after travel to Iran. *Hassanshahi,* —— F.Supp.3d at ——, —— – ——, 2014 WL 6735479, at *11–18. The case began with an anonymous tip received by Homeland Security Investigations from a source who had been contacted by an Iranian seeking assistance in procuring parts for an Iranian power project. *Id.* ——F.Supp.3d at ——, ——, at *1. Further investigation (utilizing information that was ultimately suppressed and therefore not included in the reasonable suspicion calculus) led to Hassanshahi. *Id.* —— F.Supp.3d at ——, —— – ——, ——, at *1–2, 13. The investigating agent discovered information in TECS about a federal criminal investigation in 2003 concerning Hassanshahi's alleged participation in a conspiracy to establish an American company to partner with a Chinese company to build a computer manufacturing facility in Iran. *Id.* —— F.Supp.3d at ——, ——, at *13. While no criminal charges were filed at that time, the underlying facts were later admitted in a civil action brought by Hassanshahi himself against the Chinese entity. *Id.* —— F.Supp.3d at ——, ——, at *13, n. 12. The information concerning the prior transaction, while not sufficient on its own, was found to contribute to the reasonable suspicion calculus, and in the court's view, it "also negatively colored the perception of any future travel by [Hassanshahi] to that specific country," transforming what might otherwise be general information about travel outside the United States into a "particularized and objective fact potentially indicative of ongoing criminal activity." *Id.* —— F.Supp.3d at ——, ——, at *14.

The TECS information about Hassanshahi revealed additional travel involving Iran: in 2006, twice in 2008, once in 2010, in May 2011, and in either late 2011 or early 2012, all of which supported the notion that his Iranian business dealings were ongoing. *Id.* In addition, the fact that the defendant's email account was accessed twenty-four times from an Iranian IP address between December 8, 2011 and December 15, 2011, and the evidence that around the time the defendant traveled to Iran, he made contact with one Iranian telephone number and received a missed call from another, reinforced the conclusion that Hassanshahi was engaged in business activity during his recent trip. *Id.* —— F.Supp.3d at ——, ——, at *15. Finally, the court took note of the fact that Hassanshahi was travelling with multiple electronic devices and data storage accessories, including a laptop computer, multimedia cards, thumb drives, a camcorder, SIM cards, and a cell phone. *Id.* It observed, "[t]hough it generally is unremarkable nowadays for a person traveling abroad to bring a computer, camcorder, or cell phone with them, Hassanshahi's possession of multiple data storage devices appears to be inconsistent with just personal use while traveling," and it found that the volume of equipment supported the inference that the defendant had traveled to Iran to continue the same sorts of business activity in which he had been engaged in the past. *Id.*[9]

Here, the fact that Kim's name had been provided in connection with a prior alleged export violation did not add shades of a more sinister meaning to what could have been a routine trip to the United States, because nothing about the one completed prior incident even involved a trip to the United States. *Cf. id.* —— F.Supp.3d at ——, ——, at *17 ("Hassanshahi traveled on multiple occasions to the specific country at issue in the 2003 criminal investigation, thus making his travel far more probative of criminal conduct."). Also, in contrast to the information about Hassanshahi's phone calls and emails in Iran, the record here was devoid of any information revealing where Kim had gone during his trip or who he contacted during his travels. There was nothing about the fact that Kim was travelling with an ordinary laptop that can be compared to the array of devices discovered in *Hassanshai.* And finally, the court in *Hassanshahi* made a point of " 'considering the totality of the circumstances as the officer on the scene experienced them,' " giving due credit to that officer's ability to draw inferences and deductions based upon the facts before him at the time. *Id.* —— F.Supp.3d at ——, ——, at *16, quoting *United States v. Edmonds,* 240 F.3d 55, 59–60 (D.C.Cir.2001). Here, while the o-rings may be a circumstance this Court can consider, the fact is that Special Agent Hamako was

implementing a decision he had previously made elsewhere, and his collection of the laptop was not informed in any way by his observations on the scene, filtered through his training and experience or otherwise.[10]

***14** Since there was little or nothing to indicate that a crime was "afoot" in this case, the Court is of the view that it cannot rely upon the approach utilized in *Hassanshahi,* and that it must go on to consider the constitutional question of whether the nature, scope, and duration of the search were reasonable under the Fourth Amendment. In the end, the reasonable suspicion analysis may be largely beside the point because what took place here cannot be fairly compared to a *Terry* stop.

**II. Does the search pass muster under the Fourth Amendment?**

[6]"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, 124 S.Ct. 1582, 158 L.Ed.2d 311 (2004). Notwithstanding the broad scope of the government's authority at the border, the Supreme Court has suggested that even this power to search may be bounded by limits derived from the Fourth Amendment, particularly when the search cannot be characterized as "routine." *See Montoya de Hernandez,* 473 U.S. at 540, 105 S.Ct. 3304 (observing that the Court has "not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search"); *Flores–Montano,* 541 U.S. at 152, 155–56, 124 S.Ct. 1582 (discussing "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," as well as when searches of property are ultimately "destructive"). While the Supreme Court has not provided much specific guidance about what those limits might be, "reasonableness remains the touchstone for a warrantless search." *Cotterman,* 709 F.3d at 957; *see also Brigham City, Utah v. Stuart,* 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006).

The few Supreme Court cases that explore the sorts of border searches that might require some level of suspicion involved unique and extreme situations: a highly intrusive physical examination of the defendant's person, *Montoya de Hernandez,* 473 U.S. 531, 105 S.Ct. 3304, 87 L.Ed.2d 381, and the complete destruction of another defendant's automobile gas tank, *Flores–Montano,* 541 U.S. 149, 124 S.Ct. 1582, 158 L.Ed.2d 311, and they do not deal directly with the world of electronic media. The government takes the position, then, that the search of a laptop is the functional equivalent of the inspection of a piece of luggage or a cargo container, and that therefore it was presumptively reasonable and subject to no limitation under the border search doctrine. Gov't Opp. at 6, 9. After all, the prosecution points out, the experience was not physically invasive or embarrassing and not even destructive of the laptop itself, which was returned to the defendant intact. Gov't Opp. at 8–9.

But neither of those precedents can be easily compared to this case, and given the vast storage capacity of even the most basic laptops, and the capacity of computers to retain metadata and even deleted material, one cannot treat an electronic storage device like a handbag simply because you can put things in it and then carry it onto a plane. As the court observed in *Cotterman* :

> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. This is no longer the case. Electronic devices are capable of storing warehouses full of information.
>
> * * *
>
> Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails.
>
> ***15** * * *
>
> Electronic devices often retain sensitive and confidential information far beyond the point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel.

709 F.3d at 964–65. Judges across the country have strained to select artful metaphors to use when comparing digital devices to containers ranging from slim leather valises to shipping containers, but this Court will not engage in that semantic exercise because the fact is, the metaphors do not fit. As the District Court in Maryland put it in *Saboonchi,* "a forensic search is *sui generis* ":

> I cannot help but find that even if a computer or cell phone is analogized to a closed container, a forensic search cannot be analogized to a conventional search of luggage or even of a person. A forensic search is far more invasive than any other property search that I

> have come across and, although it lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing.
>
> A conventional computer search allows Customs officers to choose, within the finite amount of time available to them while they detain the traveler, to decide where, within a veritable mountain of personal data, to focus their attention while searching for contraband, threats, or criminality. And at the end of a conventional search, as with the conventional search of a suitcase, a traveler regains custody of his possessions and information and proceeds about his business with a minimum of lingering inconvenience. A forensic search, on the other hand, allows a Customs officer to give uniquely probing review not only to the files on one's computer, but also any files that ever may have been on that computer. And even after a traveler is cleared to enter the country, the search may continue for months or even years afterwards.

990 F.Supp.2d at 568.

But when faced with the task of applying eighteenth-century principles to this twenty-first-century technology, the Ninth Circuit and the District Court in Maryland adopted slightly different approaches. *Cotterman* concluded that a forensic search of an imaged computer was as invasive of the defendant's privacy as a strip search, 709 F.3d at 966, and it concluded that reasonable suspicion was required before investigators could engage in that sort of examination. *Id.* at 962. ("It is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here.... Agent Owen used computer forensic software to copy the hard drive and then analyze it in its entirety, including data that ostensibly had been deleted."). The court expressed "confidence in the ability of law enforcement to distinguish a review of computer files from a forensic examination," noting that "it requires that officers made a commonsense differentiation between a manual review of files on an electronic device and the application of computer software to analyze a hard drive." *Id.* at 967.

***16** The *Saboonchi* court took issue with the Ninth Circuit's failure to define precisely what a "forensic" search might be. *See* 990 F.Supp.2d at 552–58. It attacked the question by differentiating a "routine" border search from a non-routine border search and creating its own test for distinguishing the "forensic" examination for which reasonable suspicion is required from a "conventional" computer search. *Id.* at 560–69.[11] According to that opinion,

> [a] conventional search at the border of a computer or device may include a Customs officer booting it up and operating it to review its contents, and seemingly, also would allow (but is not necessarily limited to) reviewing a computer's directory tree or using its search functions to seek out and view the contents of specific files or file types.... And, just as a luggage lock does not render the contents of a suitcase immune from search, a password protected file is not unsearchable on that basis alone.

*Id.* at 560–61. By contrast, "[i]n a forensic search of electronic storage, a bitstream copy is created and then is searched by an expert using highly specialized analytical software—often over the course of several days, weeks, or months—to locate specific files or file types, recover hidden, deleted, or encrypted data, and analyze the structure of files and of a drive." *Id.* at 561.

[7]Which sort of search was conducted here? Another way to phrase the inquiry might be: the Supreme Court has stated that "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant," *Montoya de Hernandez,* 473 U.S. at 538, 105 S.Ct. 3304, but was this search "routine"?[12]

The record reflects that the examination of Kim's laptop fell somewhere on the spectrum between the two poles described by other courts.

Certainly no one simply turned it on and perused the files as might have been possible at the border. By making an exact copy of the hard drive and retaining it so that it could be subjected to a series of searches, using whatever software investigators deemed necessary, for a period of unlimited duration, the investigators gave themselves the luxury of the one thing that is absolutely not available on the jetway: time. This, in and of itself, was one of the key factors identified in *Saboonchi* as differentiating a routine border search from a non-routine border search. 990 F.Supp.2d at 547.

In addition, the search was facilitated by the application of additional forensic software that was not already loaded onto the computer, 4/8 Tr. at 10, which was another factor in both *Saboonchi* and *Cotterman* underlying the determination that reasonable suspicion was required. 990 F.Supp.2d at 564–66; 709 F.3d at 962,

967.

***17** The *Cotterman* court placed some emphasis on the fact that the forensic examination there enabled the agents to access even those files that have been deleted. 709 F.3d at 962, 965. And Special Agent Marshall, who conducted the search, attempted to differentiate the search in this case from that sort of "full" forensic examination, which is often called for in cases involving child pornography. 4/8 Tr. at 15–16, 19–20. But the forensic specialist also acknowledged that the term "forensic search" can describe a range of examinations and that the term has no specific definition. 4/8 Tr. at 25. In the Court's view, the fact that the agents in this case did not search the unallocated space for deleted material as they did in *Cotterman* is not dispositive. Once an entire hard drive has been copied, the investigative imperatives of the case dictate the extent and nature of the examination, and the fact is that here, the agents found what they were looking for sitting in the computer's allocated space and email containers, and they did not need to go further. But they had created a copy of the unallocated space as well in the event a search for deleted matter turned out to be indicated.

The government tried to make the point that the use of the particular forensic search programs here was not significant, since a person with unlimited time (and presumably, patience) could use the search tools already offered on a Windows-based laptop and eventually find the emails and documents that the agent found. 4/8 Tr. at 81. Neither side produced much in the way of expert testimony or literature that would illuminate these issues, but Special Agent Hamako did testify that the mere use of a password on the device or changed file extensions on individual documents could inhibit such an effort. 4/7 Tr. at 45–47, and that Intella was more efficient than Outlook. 4/7 Tr. at 105. He also explained that Intella allows agents to run keyword searches through emails, tracks what searches have been conducted, and provides for tagging, marking, and categorizing emails without modifying the content of the emails themselves. 4/7 Tr. at 50; *see also* 4/8 Tr. at 31–32 (testimony from Special Agent Marshall explaining that Intella indexes and categorizes the emails by information contained in them, such as sender, recipient, dates, and attachments). More importantly, the agents' testimony about how long it took them to do what they did, even when they had the benefit of these additional programs, belies the notion that what was done is comparable to what an agent could have accomplished if he had simply powered up the computer then and there and stood around the airport for a while. *See Saboonchi,* 990 F.Supp.2d at 561 ("It is the potentially limitless duration and scope of a forensic search of the imaged contents of a digital device that distinguishes it from a conventional computer search."). Similarly, the volume of the material exported and presented to Special Agent Hamako—six Microsoft Outlook email containers, each potentially containing thousands of emails, 8,184 Microsoft Excel spreadsheets, 11, 315 Adobe PDF files, 2,062 Microsoft Word documents, and 879 Microsoft PowerPoint files, Dec. 2012 ROI at 4, from which 5,900 files were extracted using Special Agent Hamako's twenty-two keywords, plus approximately 24,000 .jpg files, 4/8 Tr. at 13–14—is hardly consistent with what the *Cotterman* and *Saboonchi* courts envisioned a "conventional" search to be. Even after the hard drive had been copied and the agent would have had all the time he needed, Special Agent Marshall was concerned that the material on the hard drive "would be a lot of data to look through manually," and he proposed narrowing the contents for Special Agent Hamako using forensic software and keywords. 4/8 Tr. at 33.

Still, the search here was something of a hybrid, and not quite the scouring that was involved in *Cotterman,* so did it constitute a "forensic" search under either test?[13] Which test is the appropriate formulation? Both sides steered the Court away from engaging in that sort of academic analysis. 4/8 Tr. at 58–59; 90. While the parties did not agree on whether reasonable suspicion was needed, they both urged the Court not to select one test over the other and not to articulate yet another general rule for computer searches, and that is sound advice.

***18** In the end, the Court is not persuaded that it is necessary to develop law that does not exist in this Circuit on the question of whether and when reasonable suspicion would be constitutionally required, or to articulate a broad rule of general applicability to future searches of electronic media when the technology is constantly changing and the parties have not provided much technical guidance. Because while the courts in *Ickes, Cotterman,* and *Saboonchi* had little in the way of Supreme Court precedent to guide their way, the Supreme Court has since issued its opinion in *Riley v. California,* —— U.S. ——, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014). And in *Riley,* the Court made it clear that the breadth and volume of data stored on computers and other smart devices make today's technology different in ways that have serious implications for the Fourth Amendment analysis, and it demonstrated how that analysis is supposed to proceed.[14] *Id.* at 2489–91. So it is not necessary to decide the constitutional question of what level of suspicion is required to support a forensic search of a computer that began at the border, or what the determining features of a "forensic" search might be.

[8] [9] [10]*Riley* presented the question of whether the police

may search digital information on a cell phone as part of a warrantless search incident to arrest. *Id.* at 2480. The starting point for the answer was the Fourth Amendment, and the Court reaffirmed two core propositions: first, that "[a]s the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness,' " *Id.* at 2482, quoting *Brigham City,* 547 U.S. at 403, 126 S.Ct. 1943; and second, "that '[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, ... reasonableness generally requires the obtaining of a judicial warrant.' " *Id.* quoting *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). The Court went on to reiterate that "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement," and it acknowledged that a search of the person of the accused incident to arrest is such a well-recognized exception. *Id.*

The Court then reviewed its precedents concerning the lawful scope of a warrantless search of the property found on a suspect. *Id.* at 2483–84. In *Chimel v. California,* 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), the Court announced that it would be reasonable for an arresting officer to search for any weapons that might endanger the officer's safety or be used to resist arrest or effect an escape, and that it would also be reasonable to search for and seize evidence that might otherwise be concealed or destroyed. *Riley,* 134 S.Ct. at 2483, citing *Chimel,* 395 U.S. at 762–63, 89 S.Ct. 2034. In *Robinson v. United States,* 414 U.S. 218, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973), the Court announced that since an arrest based upon probable cause was itself a lawful intrusion under the Fourth Amendment, no further justification or showing of any actual threat to the arresting officer was needed for the officer to extend the search to encompass property—in that case, a crumpled cigarette package—found on the arrestee's person. *Riley,* 134 S.Ct. at 2483–84, citing *Robinson,* 414 U.S. at 234, 94 S.Ct. 467.

But the availability of an exception alone was not enough to end the inquiry in *Riley,* and ultimately, the Court rejected a "mechanical application" of *Robinson*.

> [W]hile *Robinson* 's categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones. On the government interest side, *Robinson* concluded that the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, *Robinson* regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*. We therefore decline to extend *Robinson* to searches of data on cell phones....

***19** *Id.* at 2484–85.[15]

[11]Thus, it appears to this Court that the analysis of whether the search of Kim's laptop was reasonable under the Fourth Amendment does not simply end with the invocation of a statute or the well-recognized border exception, as broad as it may be, and it does not turn on the application of an undefined term like "forensic." Instead, following the approach utilized in *Riley,* the Court must proceed " 'by assessing, on the one hand, the degree to which [the search] intrudes upon an individual's privacy, and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.' " *Riley,* 134 S.Ct. at 2484, quoting *Wyoming v. Houghton,* 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999). As part of that exercise, the Court should, as the Supreme Court did, consider whether the application of the recognized warrant exception to this particular category of personal property would " 'untether the rule from the justifications' " underlying the exception. *Id.* at 2485, quoting *Arizona v. Gant,* 556 U.S. 332, 343, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009). While *Riley* did not have any reason to catalogue the interests underlying the government's authority to search at the border, the opinion did strongly indicate that a digital data storage device cannot fairly be compared to an ordinary container when evaluating the privacy concerns involved. *Id.* at 2491.

So what are the justifications underlying the exception to the warrant requirement that pertain at the border? At the outset, it is important to note that we are not dealing with an exception to the Fourth Amendment reasonableness requirement—only an exception to the warrant requirement. *See Ramsey,* 431 U.S. at 621, 97 S.Ct. 1972.

And the fact that the Supreme Court has specifically likened the border search warrant exception to the search incident to arrest exception reinforces the Court's view that an analysis similar to the one in *Riley* should be undertaken here. *Id.* ("[The border search exception] is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained, and in this respect, is like the similar 'search incident to lawful arrest' exception....").

[12]The government's power at the border arises out of the sovereign's right and need to protect its territorial integrity and national security. "[S]earches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons crossing into this country, are reasonable simply by virtue of the fact that they occur at the border...." *Ramsey* at 616, 97 S.Ct. 1972. While there is authority that states that the government's broad authority at the border extends to those exiting the country as well as to those coming in, *United States v. Seljan,* 547 F.3d 993, 999 (9th Cir.2008), quoting *Ramsey,* 431 U.S. at 616, 97 S.Ct. 1972, the justifications for the exception to the warrant requirement are generally framed in terms of threats posed at the point of entry. *See, e.g., Montoya de Hernandez,* 473 U.S. at 537, 105 S.Ct. 3304 ("Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country."); *Ramsey,* 431 U.S. at 620, 97 S.Ct. 1972 ("The border-search exception is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."); *United States v. Thirty–Seven (37) Photographs,* 402 U.S. 363, 376, 91 S.Ct. 1400, 28 L.Ed.2d 822 (1971) ("Customs officials characteristically inspect luggage and their power to do so is not questioned ...; it is an old practice and is intimately associated with excluding illegal articles from the country."); *Carroll v. United States,* 267 U.S. 132, 154, 45 S.Ct. 280, 69 L.Ed. 543 (1925) ("Travelers may be [stopped and searched] in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belonging as effects which may be lawfully brought in."); *United States v. 12 200–Ft. Reels of Super 8MM Film,* 413 U.S. 123, 125, 93 S.Ct. 2665, 37 L.Ed.2d 500 (1973) (border search authority is justified by the need to the prevent smuggling and enforce import restrictions); *Almeida–Sanchez v. United States,* 413 U.S. 266, 272, 93 S.Ct. 2535, 37 L.Ed.2d 596 (1973) (the power to exclude aliens from entering this country).

***20** [13]None of those significant governmental interests in monitoring what comes *in* to the country apply in this case.

It is true that there is case law that extends the search authority at the border to departures as well, and in particular, to potential violations of the export control laws. *See, e.g., United States v. Boumelhem,* 339 F.3d 414, 423 (6th Cir.2003) (finding that the government properly searched a large cargo container before it left the United States because "the United States's interest in preventing the export of weapons to other countries also implicates the sovereign's interest in protecting itself"). But *Riley* indicates that the Fourth Amendment is not necessarily satisfied by a simplistic likening of a computer to a searchable "container."[16] *See* 134 S.Ct. at 2491.

Applying the *Riley* framework, the national security concerns that underlie the enforcement of export control regulations at the border must be balanced against the degree to which Kim's privacy was invaded in this instance. And as was set forth above, while the immediate national security concerns were somewhat attenuated, the invasion of privacy was substantial: the agents created an identical image of Kim's entire computer hard drive and gave themselves unlimited time to search the tens of thousands of documents, images, and emails it contained, using an extensive list of search terms, and with the assistance of two forensic software programs that organized, expedited, and facilitated the task. Based upon the testimony of both Special Agent Hamako and Special Agent Marshall, the Court concludes that wherever the Supreme Court or the Court of Appeals eventually draws the precise boundary of a routine border search, or however either Court ultimately defines a forensic—as opposed to a conventional—computer search, this search was qualitatively and quantitatively different from a routine border examination, and therefore, it was unreasonable given the paucity of grounds to suspect that criminal activity was in progress.

More fundamentally, after hearing all of the facts, the Court cannot help but ask itself whether the examination in this case can accurately be characterized as a border search at all. And if not, it surely cannot be justified by the concerns underlying the border search doctrine.

It is true that Kim's laptop was *seized* at the border—in this case, LAX—but it was not even opened, much less searched, there. It was transported approximately 150 miles to San Diego, it was retained for a limited period of time, and eventually, the laptop was returned. Meanwhile, there was so little of note found in Kim's luggage, and he posed so little of an ongoing threat to national security, that he was permitted to board his flight.

***21** [14]The Court recognizes that the concept of the "border" for Fourth Amendment purposes extends beyond the physical boundary itself to the "functional equivalent" of the border, which may include "an established station near the border" or other nearby convenient locations. *See Alemida–Sanchez v. United States,* 413 U.S. 266, 272–73, 93 S.Ct. 2535, 37 L.Ed.2d 596 (1973). And the Ninth Circuit has held that the term "border" should be given a geographically flexible reading within limits of reason derived from the underlying constitutional principles. *Castillo–Garcia v. United States,* 424 F.2d 482, 485 (9th Cir.1970); *see also Alexander v. United States,* 362 F.2d 379, 382 (9th Cir.1966) (the legality of a search not in the immediate vicinity of the border "must be tested by a determination whether the totality of the surrounding circumstances, including the time and distance elapsed...."). So if Special Agent Hamako needed the assistance of his forensic team to open the computer in the first instance, and that step was necessarily undertaken at a DHS office rather than on the jetway, that aspect of the proceedings could arguably be considered to be an extension of the border. But while the laptop was within the government's custody and control, it was copied. And it was the exact image of the hard drive that was subjected to the search by the government's forensic team, with the fruits of that search provided to the investigating agent for further study. Indeed, the investigators' sworn testimony to the Court made it clear that the primary, if not the sole, purpose of the pre-planned encounter at the border was to obtain the laptop and search it for evidence.

Once the agents had secured the laptop and preserved every single file and folder it contained for further examination, how does the examination of the copy and the tens of thousands of emails and other files it contained for the next two weeks fall within the definition of a border search, or the statutory provisions found in 19 U.S.C. § 1581(a), at all? And what aspect of the security or territorial integrity of the nation was implicated at that point that would justify unlimited scrutiny of the copy?

This case is entirely distinguishable from *Castillo–Garcia,* which involved continuous surveillance of a car until it was stopped more than 100 miles from the border, 424 F.2d at 485, or *United States v. Bilir,* 592 F.2d 735, 741 (4th Cir.1979). In *Bilir,* the court found that a "delayed search and seizure ... made some three to four miles from the actual border, some seven hours after the observed border crossing; delayed primarily by a desire to confirm developing suspicion; and following practically continuous surveillance in the interval" passed constitutional muster as an extended border search. *Id.* at 741. In that case, the extended surveillance for the purpose of confirming initial suspicion served to " 'maintain[ ] the integrity of the border conditions keeping the search and seizure within the governmental necessities of the border.' " *Id.* quoting *United States v. Fogelman,* 586 F.2d 337, 350 (5th Cir.1978) (Brown, C.J., concurring).

Here, the search of the laptop was not predicated on any observation of Kim's activities within the United States whatsoever. And given the extensive nature and duration of the search here and the use of a list of specific search terms, the search "did not possess the characteristics of a border search or other regular inspection procedures. It more resembled the common nonborder search based on individualized suspicion, which must be prefaced by the usual warrant and probable cause standards...." *United States v. Brennan,* 538 F.2d 711, 716 (5th Cir.1976).[17]

That point is driven home by a review of the warrant application that was filed after the so-called border search was completed. After detailing his own experience and the statutory background, the agent set forth the facts supporting his view that there was probable cause to believe that the computer would contain evidence relating to violations of the Arms Export Control Act. SW Aff. ¶¶ 10–42. First, the agent stated that emails already discovered on the computer revealed that in 2008, Kim had procured six Honeywell accelerometers and shipped them to a Chinese national, who subsequently provided them to two Iranian nationals. SW Aff. ¶¶ 11, 18–40, and Att. A–1. Paragraph 15 then summarizes—in one sentence—the information provided by Yang, and it relates only to the completed transaction in 2008. SW Aff. ¶ 15.

***22** After the affidavit lays out the probable cause, it describes the anticipated computer search protocol: "With the approval of the Court in signing this warrant, agents executing this search will employ the following procedures regarding computers and other electronic storage devices ...." SW Aff. ¶ 43. The first step described was "[f]orensic [i]maging," which, of course, had already been accomplished, SW Aff. ¶ 44, and the next step was going to be the "[i]dentification and [e]xtraction of [r]elevant [d]ata." SW Aff. ¶¶ 45–50.

The warrant affidavit goes on for paragraphs explaining the highly technical process that is involved in identifying and extracting data, the fact that it requires specific expertise, equipment and software, and how challenging it can be. SW Aff. ¶¶ 45–46. There are paragraphs detailing the incredible volume of material that can be stored on a laptop and how much time it takes to review it all: "Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become

mind-boggling." SW Aff. ¶ 48. The agent concludes by predicting that "[t]he identification and extraction process, accordingly, may take weeks or months" from the date of the warrant authorization. SW Aff. ¶ 49.

But Special Agent Hamako and the forensics agent both testified that no one performed any searching or extraction after the warrant was obtained at all. 4/7 Tr. at 51; 4/8 Tr. at 23. In other words, the highly challenging and complicated examination of a mind-boggling volume of data was already complete. These undisputed facts militate against the conclusion that the only search that was undertaken—without the warrant—was just a routine border search.

After considering all of the facts and authorities set forth above, then, the Court finds, under the totality of the unique circumstances of this case, that the imaging and search of the entire contents of Kim's laptop, aided by specialized forensic software, for a period of unlimited duration and an examination of unlimited scope, for the purpose of gathering evidence in a pre-existing investigation, was supported by so little suspicion of ongoing or imminent criminal activity, and was so invasive of Kim's privacy and so disconnected from not only the considerations underlying the breadth of the government's authority to search at the border, but also the border itself, that it was unreasonable. Therefore, the motion to suppress the evidence seized as a result of that search, which includes the materials listed in Attachment B–1 to the warrant affidavit, will be granted.[18]

## CONCLUSION

For the reasons stated above, it is ORDERED that defendants' motion to suppress evidence [Dkt. # 35] is GRANTED. It is further ORDERED that a status conference is scheduled for May 18, 2015 at 10:00 a.m. in Courtroom 3.

### All Citations

--- F.Supp.3d ----, 2015 WL 2148070

Footnotes

1 Agent Marshall appeared by telephone with the consent of defendants for the April 8, 2015 hearing. 4/8 Tr. at 4.

2 The laptop was returned to Kim around December 12, 2012. SW Aff. ¶ 17.

3 Agent Marshall explained that "e-mail messages are stored in what we call a container. So if you have 5,000 e-mails, rather than having 5,000 files on your computer, you'll have one large file where all the e-mails are stored inside of that." 4/8 Tr. at 10.

4 This provision states:

> Any officer of the customs may at any time go on board of any vessel or vehicle at any place in the United States or within the customs waters or, as he may be authorized, within a customs-enforcement area established under the Anti–Smuggling Act, or at any other authorized place, without as well as within his district, and examine the manifest and other documents and papers and examine, inspect, and search the vessel or vehicle and every part thereof and any person, trunk, package, or cargo on board, and to this end may hail and stop such vessel or vehicle, and use all necessary force to compel compliance.

19 U.S.C. § 1581(a) (internal citation omitted).

5 The Fourth Circuit has found that a laptop being transported by a returning traveler at the port of entry fell well within the definition of the term "cargo" in 19 U.S.C. § 1581(a), and it upheld the inspection of a laptop in that case. *See United States v. Ickes,* 393 F.3d 501 (4th Cir.2005). But that opinion provides little guidance here because the constitutional challenge to the search was based on First Amendment grounds, and the search was initiated by agents at the border after they had already discovered child pornography in the defendant's possession and they were notified of an outstanding warrant for his arrest. *Id.* at 507.

6 *See also* 4/7 Tr. at 110 ("THE COURT: ... Basically, the government's opposition in this case ... says: Based upon the information Yang provided about Kim after Yang's arrest, as well as information about Kim obtained during the investigation of Yang, Homeland Security Investigations Special Agent Hamako decided to conduct a border search of Kim when he returned to the United States. So it's fair to say that before you knew whether or when Mr. Kim was coming to the United States, you had already decided that if and when he came, you wanted to do a border search, correct? [SPECIAL AGENT HAMAKO]: That's correct, Your Honor. THE COURT: And did you decide then that the border search would include doing a border search of his laptop? [SPECIAL AGENT HAMAKO]: Yes, Your Honor.").

7 The dissent in *Cotterman* criticized the majority's decision to rely in part on the fact that the defendant was returning from Mexico based on its vague association with "sex tourism," finding that Mexico is a popular travel destination for innocent reasons, including its "beaches, culture and weather, and not for its sex tourism." 709 F.3d at 992 (Smith, J., dissenting).

8 The agents retained the electronic devices, and the next day, they were delivered to an ICE Computer Forensic Examiner who made copies of the hard drives. 709 F.3d at 958. On the following day, aided by the use of forensic software, the agent found seventy-five images of child pornography within the unallocated space of one of the laptops. *Id.* A further search of the password-protected files revealed an extensive collection of additional images of child pornography, including images of the defendant himself repeatedly molesting a child over a two-to-three-year period. *Id.* at 959.

9 Given the prevalence of laptops, tablets, cell phones, e-readers, and digital cameras, carried in combination by travelers ranging from elementary school students to senior citizens, and the availability of myriad electronic applications for news, sports, music, games, fitness, banking, personal organization, and travel, this Court is not necessarily persuaded that being equipped with multiple electronic devices is a strong indicator of business activity. But it notes that this factor was absent in this case in any event.

10 In *United States v. Saboonchi,* 990 F.Supp.2d 536, the court devoted only one page of its lengthy decision holding that reasonable suspicion was needed to its finding that the standard had been satisfied. *Id.* at 571. The opinion recounts that when Saboonchi, a dual citizen of the United States and Iran, arrived at the border, he was already the subject of ongoing investigations into export violations, and that evidence had already been gathered in response to several subpoenas. *Id.* There was information gleaned from both the subpoenas and witness interviews that the defendant had purchased two cyclone separators after representing that they would be used domestically, and that he had shipped them overseas, understating their value in a manner that suggested to the agent that he was seeking to avoid scrutiny. *Id.* at 542–43, 571. Also, it had already been determined that the recipient of the shipment was linked to a company in Iran. *Id.* at 571. But while it is true that this case also involves an investigation into a completed export violation, with little evidence that anything was ongoing at the border, the *Saboonchi* investigation was much further along than Special Agent Hamako's, which at that point consisted primarily of Yang's accusation. And the opinion, while it may be instructive on certain points, is not binding on this Court in any event.

11 Such an analysis may have been necessary in that case since the *Saboonchi* court was otherwise constrained by the Fourth Circuit precedent in *Ickes.*

12 The First Circuit has proposed that the following non-exhaustive list of factors may be relevant when determining whether a search can be characterized as routine: "(i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe; (ii) whether physical contact between Customs officials and the suspect occurs during the search; (iii) whether force is used to effect the search; (iv) whether the type of search exposes the suspect to pain or danger; (v) the overall manner in which the search is conducted; and (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search." *United States v. Braks,* 842 F.2d 509, 512 (1st Cir.1988) (footnotes omitted).

13 The government, which had not even planned to call the forensic specialist until the Court indicated his testimony would be necessary, *see* 4/7 Tr. at 98, submitted that the search here did not meet the *Cotterman* test for a "forensic" examination, but it was not prepared to articulate why. 4/8 Tr. at 81–82.

14 The fact that *Riley* involved a cellular telephone rather than a laptop is of little moment; indeed, it was the fact that a cellular telephone is, for all intents and purposes, a small computer, that led that Court to find that the usual rules governing a search incident to arrest should not apply. 134 S.Ct. at 2489.

15 The level of concern expressed by the Supreme Court regarding the volume of personal data saved on an electronic device leads the Court to conclude that the decision in *House v. Napolitano,* 2012 WL 1038816 (D.Mass.2012), which was decided before *Riley* and is not binding in any event, is not instructive here. In that case, the District Court found that "the search of one's personal information on a laptop computer, a container that stores information, even personal information, does not invade one's dignity and privacy in the same way as an involuntary x-ray, body cavity, or strip search of a person's body or the type of search that has been held to be non-routine and require the government to assert some level of suspicion." *Id.* at *7.

16 For that reason, the Court does not feel compelled to follow the decision of the Fourth Circuit in *Ickes,* 393 F.3d at 501, which preceded *Riley* and is also distinguishable on other grounds. In that case, the border agents searched the defendant's computer only after finding other incriminating items during a physical search of the defendant's vehicle at a border crossing. *Id.* at 502–03, 506. In addition, the defendant's computer was seized and searched at the border, while the defendant was in the agents' custody. *Id.* at 503.

17 The Court need not determine whether the agent could have articulated probable cause to believe that Kim had participated in a criminal conspiracy in the past and that the laptop would contain evidence of that alleged conspiracy, because "[i]n cases where searches are made without warrants, the Supreme Court has decreed that the existence of probable cause must be accompanied by

circumstances rendering the warrant procedure impracticable." *Brennan,* 538 F.2d at 721, citing *Warden v. Hayden,* 387 U.S. 294, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967). Since there were no exigent circumstances present in this case, if the search was not a "border" search within the meaning of *Ramsey* and other Supreme Court precedent, then the failure to obtain a warrant requires suppression.

18 The government did not even attempt to advance the argument that the issuance of the warrant, in which probable cause was predicated almost exclusively on the emails themselves, somehow cured the underlying illegality and provides grounds for denying the motion to suppress.

End of Document