No. 19-1221

In the Supreme Court of the United States

DERRICK LUCIUS WILLIAMS, JR., PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE TENTH CIRCUIT

James Patterson McBaine Honors Moot Court Competition

2021 Record

Table of Contents

QUESTION PRESENTED

What is the appropriate legal standard under the Fourth Amendment for government agents to conduct a warrantless forensic search of a digital device at the border?

This excerpt from Petitioner's petition for certiorari is included as an introduction to this year's problem. It is not meant to be an exclusive statement of the relevant law, issues, or cases.

Use of this excerpt is the only permitted exception to the Competition rule prohibiting use of parties' briefs or the case file. You should not attempt to access the full petition.

INTRODUCTION

This case presents an ideal vehicle to resolve a four-way circuit split on an issue of exceptional importance to millions of Americans.

Citizens returning from abroad know that some of their freedoms are curtailed as they cross the border. After all, "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). So travelers may expect routine searches without any suspicion. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

But nearly all Americans carry cell phones—some everywhere they go—and many travel with laptops. Surely they would be surprised that border agents might "rummage through" their electronic devices "in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). Indeed, when British officers took such an approach to the Founding generation's homes, they "helped spark the Revolution itself." *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018). And "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house," because from his digital devices "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions," not to mention the "picture messages, text messages, Internet browsing history," "calendars, tape recorders, libraries, diaries, albums," and more that such devices contain. *Riley*, 573 U.S. at 393–94.

An American flying into Seattle or Los Angeles from a trip abroad can deplane with little worry: Government agents may forensically search his laptop or smartphone only if they reasonably suspect that it contains digital contraband, like child pornography. They may not simply download all his files and scrutinize them for evidence of criminal activity, whether or not related to the government's interest in keeping contraband from crossing the border. *United States v. Cano*, 934 F.3d 1002, 1007, 1020 (9th Cir. 2019).

If the traveler lands at Reagan or BWI, the rules are different. Agents may forensically search his laptop or smartphone if they have reasonable suspicion that it contains evidence of a particular crime with a nexus to the purposes of the border search exception to the Fourth Amendment's usual warrant requirement. In other words, they can look for evidence of particular border-related crimes, not just contraband. *See United States v. Aigbekaen*, 943 F.3d 713, 720–23 (4th Cir. 2019).

If the traveler arrives in Denver or Salt Lake City, the rules are even more lax. In the Tenth Circuit, reasonable suspicion of criminal activity—even if untethered to digital contraband or the border search exception's purposes—is all it takes for officers to copy his digital data and analyze it six ways to Sunday, as Petitioner Derrick Williams discovered here. App. 6a–9a.

But any traveler who values his privacy should really avoid entering the country via Miami or Atlanta. In the Eleventh Circuit, every computer or cell phone is no different than a suitcase. Officers can rummage at will through an individual's private digital life with no suspicion whatsoever. *United States v. Touset*, 890 F.3d 1227, 1229, 1233–34 (11th Cir. 2018).

The courts of appeals disagree vigorously about the correct rule. In twelve opinions—both majority and separate—judges have articulated every conceivable view on the question presented. Given that hundreds of millions of people cross the border each year—most of them with digital devices—this Court should not wait any longer to answer the pressing question presented.

FILED
United States Court of Appeals
Tenth Circuit

November 14, 2019

Elisabeth A. Shumaker
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

DERRICK LUCIUS WILLIAMS, JR.,

Defendant - Appellant.

ELECTRONIC FRONTIER FOUNDATION,

Amicus Curiae.

No. 18-1299

Appeal from the United States District Court
for the District of Colorado
(D.C. No. 1:16-CR-00249-WJM-1)

Josh Lee, Assistant Federal Public Defender (Virginia L. Grady, Federal Public Defender, with him on the brief), Denver, Colorado, for Defendant - Appellant.

Marissa R. Miller, Assistant U.S. Attorney (Jason R. Dunn, United States Attorney, with her on the brief), Denver, Colorado, for Plaintiff - Appellee.

Sophia Cope and Adam Schwartz, Electronic Frontier Foundation, San Francisco, California, filed an Amicus Curiae brief, in support Defendant - Appellant.

Before **BACHARACH**, **KELLY**, and **CARSON**, Circuit Judges.

KELLY, Circuit Judge.

Defendant-Appellant Derrick Williams pled guilty to transportation of child pornography, 18 U.S.C. § 2252A(a)(1) and (b)(1), and possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), reserving his right to appeal the denial of a motion to suppress. He was sentenced to 84 months' imprisonment and five years of supervised release. Our jurisdiction arises under 28 U.S.C. § 1291 and we affirm.

Background

On November 24, 2015, Mr. Williams, an American citizen, boarded an international flight bound for Denver International Airport (DIA). Once on the ground, he proceeded to customs where his passport triggered multiple "lookout" alerts in the U.S. Customs and Border Patrol (CBP) enforcement system. The alerts instructed CBP officers to escort Mr. Williams to DIA's secondary screening area where he was met by Homeland Security Special Agent Kyle Allen.

Agent Allen became aware of Mr. Williams in August 2015 when he received a letter stating that Mr. Williams had been arrested in Germany for violating weapons laws. According to the letter, someone reported seeing Mr. Williams and another man brandishing weapons in a suburban neighborhood. Officers found a crossbow, multiple pistols, and an airsoft gun that resembled an automatic rifle in their possession.

The letter additionally stated that it was unclear how Mr. Williams entered Germany as he was banned from the country in 2011 after being discovered living there

on an expired visa. The ban extended throughout the Schengen Area for a five-year period. However, Mr. Williams admitted to German law enforcement that in 2015 he had already traveled through Belgium, France, Iceland, and the Netherlands — all Schengen member states — and that he would go to Morocco next.

Prompted by this letter, Agent Allen began investigating Mr. Williams and discovered that he had domestic felony convictions for trespass, unlawful use of a financial instrument, fraud, and escape. The escape charge arose when Mr. Williams fled the United States in 2007 while serving a community corrections sentence. Mr. Williams was convicted in 2011 after being deported from Germany to the United States.

On November 13, 2015, terrorist cells operating in France and Belgium launched a large-scale attack in Paris. The terrorists, who claimed allegiance to the Islamic state, were of Moroccan descent. Agent Allen's supervisors asked that he review his open investigations. Agent Allen then reviewed Mr. Williams's file and, though he did not have specific information linking Mr. Williams to terrorist activity, placed a lookout on Mr. Williams in the CBP enforcement system.

Less than two weeks after the attacks, Agent Allen learned that Mr. Williams had boarded a flight from Paris to Denver with a stopover in Reykjavik. He met Mr. Williams at DIA to interview him. Prior to conducting the interview, however, Agent Allen reviewed Mr. Williams's customs declaration form and noticed that he had not listed Germany as one of the countries visited. Only Belgium, France, and Morocco were included.

During the interview, Mr. Williams was repeatedly asked if he had traveled to other European countries not listed on his customs declaration form. He was evasive and never affirmatively admitted to having been in Germany. He also gave vague answers regarding his time in Belgium and claimed that he split his time there between a hostel and living with a friend. He could not give specific information about the friend other than that his name was Mohammed and they had met near a mosque.

At the close of the interview, Agent Allen explained to Mr. Williams that his electronic devices, a laptop and a smartphone, would be searched. He asked for the devices' passwords, which Mr. Williams refused to give. As a result, two forensic computer specialists attempted to get around the passwords. When they were unsuccessful, Agent Allen told Mr. Williams that his electronics would need to be taken to another site and would be returned to him later. He asked Mr. Williams where the devices should be returned, and he gave his address as 3333 Curtis Street. Agent Allen noticed this address did not match the 2952 Downing Street address that Mr. Williams listed as his home address on both the customs declaration form and his most recent passport application. Mr. Williams was allowed to leave.

The next day, Agent Allen took Mr. Williams's electronics to his office. A computer forensics agent used a software program called "EnCase" to bypass the laptop's password and create a copy of the hard drive, which he was then able to search. Within three minutes, the agent found a folder titled "Issue 15 Little Duchess," which contained child pornography. He immediately stopped his search and notified Agent Allen who

subsequently obtained a search warrant authorizing a full forensic search. The search ultimately yielded thousands of images and videos of child pornography.

Mr. Williams was indicted and moved to suppress the evidence obtained from his laptop on grounds that it was tainted by the three-minute search conducted prior to the issuance of a search warrant. He argued that the agents needed reasonable suspicion for this kind of search and that, because they did not have it, his Fourth Amendment rights were violated. The government countered that the Fourth Amendment allowed for suspicionless searches at the border and that, even if reasonable suspicion were required, they had ample reason to suspect that Mr. Williams was involved in criminal activity. The district court held a hearing on the matter and subsequently denied the motion. The court declined to decide whether reasonable suspicion was necessary to justify the search but found that because the agents had it in this case, Mr. Williams could not prevail either way. On appeal, Mr. Williams argues that the district court erred in holding that the search was supported by reasonable suspicion and that, without reasonable suspicion, the search of his personal electronic devices at the border violated his Fourth Amendment rights.

Discussion

We review a district court's factual findings pertaining to a motion to suppress for clear error, Ornelas v. United States, 517 U.S. 690, 699 (1996), and view evidence in the light most favorable to the prevailing party, United States v. Jones, 523 F.3d 1235, 1239 (10th Cir. 2008). Whether a search was reasonable under the Fourth Amendment is a

question of law reviewed de novo. United States v. Greenspan, 26 F.3d 1001, 1004 (10th Cir. 1994).

Although Mr. Williams asks us to find that searches of personal electronic devices at the border must be supported by reasonable suspicion, we decline to do so. It is well-established that in deciding constitutional questions, courts should strive "never to formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied." Liverpool, N.Y. & Phila. Steam-Ship Co. v. Com'rs of Emigration, 113 U.S. 33, 39 (1885). Moreover, under any interpretation of the Fourth Amendment put forth by Mr. Williams, reasonable suspicion is sufficient to justify a border search of personal electronic devices. As we agree with the district court that reasonable suspicion was present here, Mr. Williams' own arguments preclude him from prevailing.

Law enforcement officers must "have an articulable, individualized, reasonable suspicion that an individual is involved in some criminal activity." United States v. Rascon-Ortiz, 994 F.2d 749, 752 n.3 (10th Cir. 1993). In the Fourth Amendment context, the "reasonable suspicion analysis requires a careful consideration of the 'totality of the circumstances.'" United States v. Esquivel-Rios, 725 F.3d 1231, 1238 (10th Cir. 2013) (quoting United States v. Cortez, 449 U.S. 411, 417 (1981)). Here, the totality of circumstances surrounding the search of Mr. Williams's laptop readily meet the reasonable suspicion standard.

First, Mr. Williams's criminal history concerns border offenses. He fled the United States a fugitive and was convicted after deportation from Germany. Moreover,

German authorities banned Mr. Williams from entering any country in the Schengen Area between 2011 and 2016. Agent Allen knew that Mr. Williams had blatantly contravened this ban in 2015 by traveling undetected through Iceland, the Netherlands, Belgium, France, and Germany.

Second, Agent Allen knew Mr. Williams had been in Germany prior to his return to the United States, yet Mr. Williams did not list Germany as one of the countries visited on his customs declaration form despite attesting via signature that his answers on the form were truthful. Additionally, Mr. Williams evaded all of Agent Allen's questions regarding his time in Germany and claimed that, because of his advanced age of 39, he was unable to recall details regarding his time abroad. See United States v. Himmelwright, 551 F.2d 991, 996 (5th Cir. 1977) (upholding a search as reasonable based in part on defendant's evasive and contradictory statements).

Third, Mr. Williams was returning to the United States on a one-way ticket originating in Paris — the site of devastating terrorist attacks less than two weeks earlier. His travel itinerary included Belgium, France, and Morocco, three countries intimately linked to the attacks. See United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006) (finding a suspicious itinerary relevant under the totality of the circumstances test). Additionally, Mr. Williams had been arrested in Germany for brandishing what appeared to be weapons.

Finally, Mr. Williams appeared to distance himself from his electronic devices. On his customs declaration form, Mr. Williams gave his home address as 2952 Downing Street and yet, when asked where the devices should be returned, gave his address as

3333 Curtis Street. The totality of the circumstances is sufficient to justify a warrantless search of the laptop and cell phone.

Relatedly, Mr. Williams argues that even if the border agents had reasonable suspicion that he was engaged in criminal activity, this suspicion was not particularized enough to justify the search. He suggests that border agents are tasked exclusively with upholding customs laws and rooting out the importation of contraband. He argues that because border agents did not suspect him of either of these types of crimes, they were prevented from searching his laptop and cell phone. We disagree because "[t]he Fourth Amendment does not require [law enforcement] officers to close their eyes to suspicious circumstances." Rascon-Ortiz, 994 F.2d at 753 (quoting United States v. Johnson, 895 F.2d 693, 696 (10th Cir. 1990)).

Finally, Mr. Williams argues that the scope and duration of his laptop search was unreasonable under the Fourth Amendment. This argument has been waived as it was not raised in the motion to suppress and Mr. Williams did not show good cause for his untimeliness in this regard. United States v. Bowline, 917 F.3d 1227, 1234 (10th Cir. 2019) ("[A]n untimely argument . . . is not reviewable either in district court or in any subsequent proceedings absent a showing of an excuse for being untimely.").

AFFIRMED.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge William J. Martínez

Criminal Case No. 16-cr-249-WJM

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. DERRICK LUCIUS WILLIAMS JR.,

Defendant.

ORDER DENYING MOTION TO SUPPRESS

The Government has charged Defendant Derrick Lucius Williams Jr. ("Williams") with one count of transporting child pornography and one count of possessing child pornography. (ECF No. 1.) Williams moves to suppress the relevant evidence against him, given that it was gathered when federal customs agents seized and forensically examined his laptop upon his reentry to the United States at Denver International Airport ("DIA"). (ECF No. 19.) Williams argues that the search required reasonable suspicion, and that such suspicion was lacking. The Government counters that it has plenary authority at the border to search digital devices. For the reasons explained below, the Court does not reach the Government's plenary-authority argument because the Court finds that reasonable suspicion existed to search Williams's laptop. Williams's motion is therefore denied.

I. FACTS

Homeland Security Special Agent Kyle Allen ("Allen") is a Denver-based federal

law enforcement officer who investigates, among other things, possible legal violations by persons entering the country at DIA. In August 2015, Allen received a letter from the FBI's Denver field office about a law enforcement report that German officials had recently shared with United States officials. The letter read in relevant part as follows:

> Denver FBI was notified by the Office Legal Attach[é], Frankfurt[,] Germany [i]n July 2015 that the Polizei Präsidium South Hessen (PPSH) had arrested Derrick Williams, a resident of Colorado at the time.
>
> In May 2015, PPSH arrested Derrick Williams for violating weapons laws. (Note: weapons were bow/arrow and air gun, not permitted to be used in public spaces.) At the time of the arrest, a brief interview was conducted with Williams. Williams provided his travel itinerary, documenting his travel to Mainz, Germany via Reykjavik, Iceland and Amsterdam. Williams flew from Denver to Reykjavik, then on to Amsterdam. He spent seven days in Amsterdam before taking a train to Mainz, Germany. He had an open-ended bus ticket from Mainz to Brussels, Belgium and advised arresting officers he would be traveling from Brussels to Morocco. PPSH did not collect further intelligence from Williams during the interview and advised him he had three days to leave Germany.
>
> Upon further investigation, PPSH advised [that] Williams was in Germany from November 2007 until October 2011. Most of that time, he was [t]here illegally (his passport or visa expired 4/2/2008). On 10/17/2011, upon discovering [that] Williams was there illegally, German authorities put a Schengen alert on him, which banned him from entering any Schengen member state[1] from 10/17/2011 until 10/16/2016 (NFI).[2] It is unclear how Williams entered Iceland and the Netherlands with this ban in place. PPSH had no further information on Williams or his travel after leaving Germany in

[1] The Schengen Area is a group of European countries (not precisely coterminous with the European Union) where free travel across their various borders is permitted once a traveler is lawfully admitted to one of them. As relevant to the present proceeding, member states include Belgium, France, Germany, Iceland, and the Netherlands. *See* https://travel.state.gov/content/passports/en/go/schengen-fact-sheet.html (last accessed Sept. 20, 2017).

[2] The meaning of "NFI" is unknown. One possible meaning relevant to this context is "not formally invited."

May 2015.

(Defendant's Exhibit ("DX") G.)

This letter prompted Allen to begin an investigation into Williams. This investigation included Williams's most recent passport application, from which Allen obtained Williams's permanent address of 2952 Downing Street, Denver—a detail that would become important later. Allen also looked at Williams's travel history, to the extent it was known by United States databases, and it showed that he had departed the country in May 2015 on a one-way ticket to Reykjavik.

In addition to the foregoing, Allen checked Williams's criminal history, which included felony convictions for trespass, use of a financial instrument, fraud, and escape. The escape conviction shed light on Williams's presence in Germany from 2007 to 2011. Williams had been serving a community corrections sentence in 2007. One night, instead of going to work as authorized by his parole officer, Williams headed to DIA and fled the country—hence the charge of felony escape. When Williams returned to the United States in 2011 (upon his deportation from Germany), he was convicted in Colorado state court on that escape charge.

Allen apparently did little else with respect to Williams until November 2015. As is well known, terrorists attacked civilians in various locations in and around Paris on November 13, 2015. Parts of France and Belgium (where the terrorist cell was based) were "on lockdown" for several days thereafter. Authorities were searching for suspects in those countries, as well as in Germany.

Prompted by this event, Allen's supervisors requested that he and his fellow officers review their current investigations to determine if any persons might be "of interest." Allen had no information specifically linking Williams to the Paris attacks.

Nonetheless, on November 18, 2015 he created a "lookout" in what U.S. Customs and Border Patrol ("CBP") refers to as the "TECS" database. This lookout would ensure that Allen would receive notification if Williams sought to reenter the United States through a regular port of entry. Allen's lookout also instructed Customs and Border Patrol officials to escort Williams to "secondary" if he presented himself at a port of entry—meaning that Williams should not be allowed to pass into the country solely based on the "primary" interview with the CBP officer that inspects travelers' passports and customs declarations, but should instead be taken to a side room for further questioning.

Allen's lookout was well-timed (or ill-timed, from Williams's perspective). Six days later (November 24, 2015), Allen received word that Williams had boarded a flight in Paris on a one-way ticket bound for Reykjavík and then Denver, meaning Williams would likely arrive at DIA that evening.

Allen arranged to be present at the DIA port of entry around the time of Williams's expected arrival. At Allen's request, two Homeland Security computer forensic agents also arranged to be there, in case Williams was carrying electronic devices that could not be searched without special tools.

Williams indeed arrived at the DIA port of entry a little before 7:00 PM. At the primary inspection point, Williams presented his signed customs declaration form (the standard CBP Form 6059B) to a CBP officer, who then relayed the declaration form to Allen. On that form, Allen saw that Williams had given 2952 Downing Street, Denver, as his address—the same permanent address listed on his passport application. (*See* Government's Exhibit ("GX") 9.) However, on the line for "Countries visited on this trip prior to U.S. arrival," Allen noticed that Williams had written "Belgium, France, Morocco"

but not Germany. (*Id*.) Allen concluded that Williams's answer was an intentional omission, or in other words, that Williams could not have innocently forgotten his time in Germany, given that he had been arrested there.

Per Allen's TECS lookout, the primary CBP officer referred Williams to the secondary inspection area, where Williams spoke with another CBP officer. While speaking with that officer, still other CBP officers searched Williams's luggage and found nothing of immediate concern, although they located a laptop and a smartphone that they could not access due to password protection.

The Homeland Security computer forensic agents went to work on these devices. Those agents brought only "light-weight forensic equipment" (as compared to the "larger forensic workstations" they have at their offices). If that equipment had been able to bypass the password on the laptop and/or smartphone, the agents planned to quickly browse through the files and records immediately available on the device in question, not to run a full forensic scan. However, the agents could not crack the password on either device.

While the forensic agents were working on those devices, Williams was escorted into an interview room where he met Allen and Aurora Police Detective Craig Appel ("Appel"), who was at that time a deputized FBI "task force officer" as part of a joint counterterrorism task force. Allen and Appel (together, "the Agents") interviewed Williams for approximately the next thirty minutes, with an audio recorder running. (*See* GX 10 (audio recording of the interview).)

For roughly the first ten minutes of the interview, Williams and the Agents discussed his purpose for spending close to six months abroad. Williams explained that

he had been engaged to marry a Moroccan woman in Morocco, but the process by which a foreigner can marry a Moroccan in Morocco is lengthy and paperwork-laden. Moreover, he was only permitted to stay in Morocco for three months at a time, which was not long enough to complete the paperwork. Rather than incur the expense of flying back to the United States after those three months, he adopted a less expensive alternative: fly to Brussels and spend three weeks there in a hostel, or with a friend, and then return to Morocco to continue the marriage approval process. During his second trip to Morocco, he finally married his fiancée, and he now planned to apply to bring her to the United States. (*Id*. at 2:35–10:00.)

During this portion of the interview, the Agents asked Williams for the name of the friend with whom he stayed in Brussels. Williams identified the friend as "Mohammed," whose last name Williams did not know. Williams had met Mohammed at a restaurant near a mosque in Brussels, although he could not remember the name of the mosque. Williams said that Mohammed recognized him as a stranger to the city and also a Muslim, and invited him to stay at Mohammed's place. (*Id*. at 7:00–8:30.)

Roughly the second ten minutes of the interview were dominated by discussion of Williams' laptop and smartphone. By this time, someone had informed Allen that those devices were password-protected, and that the forensic agents had failed to bypass the passwords. The Agents therefore tried to convince Williams to divulge his laptop password and smartphone swipe code. Allen informed Williams that "border search authority" gave him power to inspect all items entering the United States, including the contents of Williams's digital devices, and that those devices would be

searched one way or the other.[3] However, the process would be much quicker if Williams would help them to access his devices.

Williams refused to disclose his password and swipe code, explaining that he believed it was an invasion of his constitutional rights generally, and also that he was being targeted because he is Muslim. (*Id*. at 10:00–20:50.) The Agents therefore had Williams fill out two claim forms for his electronic devices (one for the laptop, one for the smartphone). On both forms, Williams gave his address as 3333 Curtis Street, Denver. (GX 11.) Allen noticed that this address differed from the one Williams had just given on his customs declaration, and the one that had been on his passport application, but did not ask Williams about the discrepancy.

For roughly the last ten minutes of the interview, the Agents repeatedly asked Williams if he had been to Germany during the last six months, and Williams repeatedly avoided answering. For example:

- In one instance Williams responded, "You have the information where I was at . . . from my passport." Allen observed, however, that not every European country would stamp a traveler's passport, apparently referring to the Schengen Area protocol.
- In another instance Williams directed the Agents to speak with the United States consulate in Casablanca, whose officials (according to Williams) had also asked him if he had been in Germany. "They know better,"

[3] Allen believed, although he did not explain as much to Williams, that border search authority was essentially unfettered with respect to travelers' belongings. Allen obtained this belief from ICE Directive 7-6.1, § 6.1, which states that "ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion . . . ." (DX H at 2.)

Williams said. But in response to Allen's question, "They know—so you told them?", Williams answered, "No, they asked me the same question like you did, was I in Germany?"

- In yet another instance, Williams simply responded, "What do you think?"
- Williams claimed that the fatigue of travel, and aging generally, were affecting his memory.

Williams eventually volunteered that he had lived in Germany "a long time ago" on an expired visa because he had traveled there but run out of money to return, and admitted that he had been deported and banned from Germany. Understanding Williams to be referring to his time from 2007 to 2011, Allen asked, "What about this trip?" Williams returned to his previous evasiveness, implying that the Agents were being dishonest by asking him a question to which they already knew the answer. (GX 10 at 20:50–28:20.)

With matters essentially at a stalemate, Williams stated that he wanted to go home, and the agents did not hold him up with any more questions. They explained, however, that his unwillingness to provide his password and swipe code would "greatly increase" the time it would take for them to return his laptop and smartphone. Williams stated that he understood but was going to stand on principle. He then left the airport with his belongings, minus the laptop and smartphone. Those two items were placed in a secure locker at the port of entry.

The following morning (November 25, 2015), Allen returned to DIA, retrieved the laptop and smartphone, and drove them to a Homeland Security office in Greenwood Village. There, he handed off the devices to one of the computer forensic agents that had come to the airport the previous evening, Christopher McGuckin ("McGuckin").

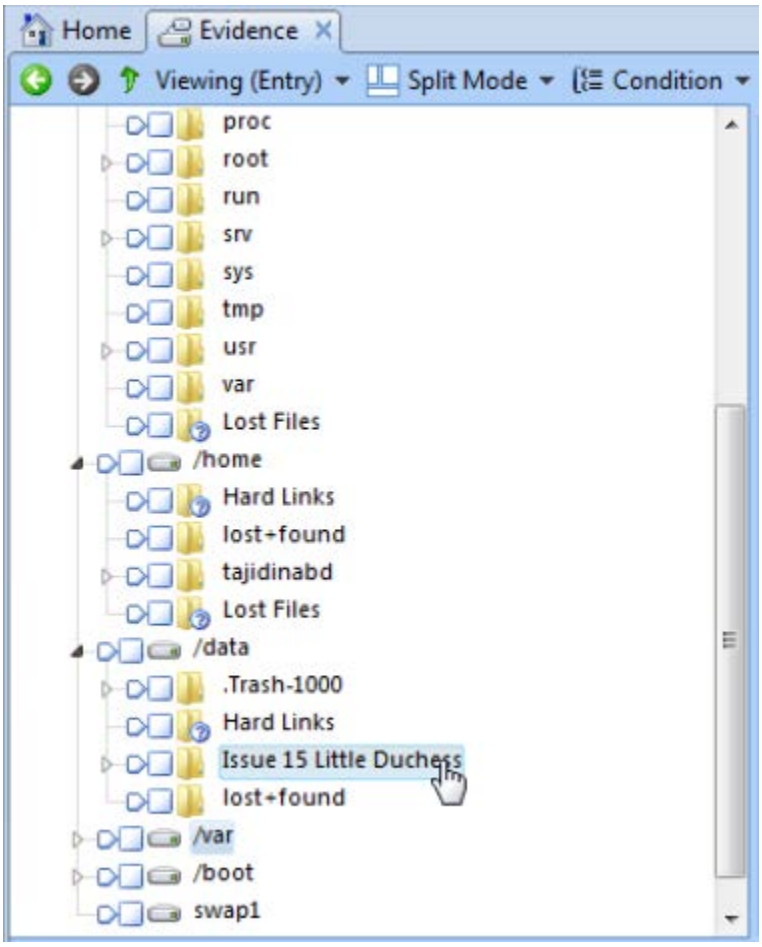
Allen then attempted to e-mail Williams at an e-mail address Williams provided on the customs claim form the previous evening. Allen understood from Williams that the only phone number that could reach him was the one associated with Williams's smartphone, and since Allen was detaining the smartphone, he wanted to make sure that at least the e-mail address was valid. Thus, he asked Williams, "[C]an you please respond to this e-mail so I know this account is checked[?]" (GX 12.) The e-mail also contained Allen's phone number. (*Id.*) Williams never replied to this e-mail, either that day or later.

While Allen was e-mailing Williams, McGuckin and a subordinate began working on the laptop and smartphone. They first removed the laptop's hard drive and made a bit-for-bit copy, so they could work on the copy and avoid potentially altering the original. They completed the copy that day but did not inspect any of the copied data.

The next day (November 26, 2015) was Thanksgiving and McGuckin was not in the office for the remainder of that week. He finally began examining the hard drive image on December 1, 2015. He loaded the image into EnCase, a computer program used for forensic examination of digital media. EnCase's initial processing included recovery of "lost folders," which McGuckin described as follows: "if a folder or file's parent folder is deleted then a—the link to that, to its location, is lost, so recovering the lost folders attempts to reconstruct that." No party has explained the difference, if any, between recovering lost folders and recovering deleted files. In any event, at this time McGuckin did not inspect whatever EnCase had managed to recover, nor did he direct EnCase to index the hard drive for ease of searching.

When EnCase had finished preparing the data, it displayed the contents of

Williams's hard drive image through a graphical user interface similar to what one would see if accessing the hard drive through the laptop, as shown in the following excerpt from a screencast video McGuckin created to document the process he followed:



(GX 15 at 4:33.) As can be seen by the location of the cursor, a folder named "Issue 15 Little Duchess" quickly drew McGuckin's attention. He began browsing that folder, as one could do if accessing it directly through the laptop, and soon discovered child pornography.

McGuckin did not go any further in his examination that day. Allen instead applied for a search warrant to examine the entire laptop. That warrant issued on December 4, 2015, at which point McGuckin began a detailed forensic analysis of the

hard drive image, including keyword searches and file type searches, as well as retrieval of e-mails, Internet browsing and search history, and BitTorrent history.

It took McGuckin until June 2016 to complete his forensic report of the hard drive image. By that time, he had "discovered several thousand images and videos consistent with child pornography." (DX F at 4.) As for Williams's smartphone, McGuckin could not crack it with his equipment and therefore sent it to another lab. That lab was finally able to access the smartphone's contents several months later. No contraband files were found on the smartphone, however.

On July 27, 2016, a grand jury indicted Williams with the offenses of transportation and possession of child pornography. (ECF No. 1.) Williams was arrested on September 26, 2016. (ECF No. 4.)

II. BURDEN OF PROOF

On a motion to suppress evidence derived from a warrantless search, the defendant bears the burden of presenting a *prima facie* case that the Fourth Amendment has been "implicated," at which point the burden shifts to the Government to prove "that its warrantless actions were justified (*i.e.*, as a lawful investigatory stop, or under some other exception to the warrant requirement)." *United States v. Carhee*, 27 F.3d 1493, 1496 (10th Cir. 1994); *see also id*. at nn.1–2 (citing authorities); 6 Wayne R. LaFave, *Search & Seizure* § 11.2(b), at n.35 and accompanying text (5th ed., Oct. 2016 update) ("*Search & Seizure*").

Williams's motion reveals that his personal Fourth Amendment rights are implicated here. He has therefore raised a *prima facie* case of a potential Fourth Amendment violation through a warrantless search, thus shifting the burden to the

Government to justify the search.

III. ANALYSIS

A. Border Search Authority

As noted above, Allen invoked "border search authority" to seize and search Williams's laptop and smartphone. Although it is not clear precisely what Allen meant by the phrase "border search authority," it is nonetheless a recognized concept—or, more specifically, an established application of the Fourth Amendment's guarantee against unreasonable searches and seizures. In general, "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable [under the Fourth Amendment] simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). But narrow exceptions exist to this otherwise broad pronouncement of *per se* reasonableness.

1. *Montoya de Hernandez* (1985)

Apparently the first Supreme Court decision to deviate from this blanket pronouncement of reasonableness was *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985). In *Montoya de Hernandez*, the suspect was detained at Los Angeles International Airport upon her arrival from Bogotá, Colombia. *Id*. at 533. A customs inspector noticed that she had recently made at least eight trips from Bogotá either to Miami or Los Angeles. *Id*. When she provided a fairly implausible account of why she had traveled to the United States again, she was referred to a female officer for a strip search. *Id*. at 533–34. The female officer noticed that the suspect's abdomen was unusually firm, among other things. *Id*. at 534.

The inspectors formed a belief that the suspect "was a 'balloon swallower,' one

who attempts to smuggle narcotics into this country hidden in her alimentary canal." *Id*. After detaining her for several hours while "she exhibited symptoms of discomfort consistent with heroic efforts to resist the usual calls of nature," they subjected her to a pregnancy test (because she claimed she was pregnant and so could not be x-rayed), which turned out negative; and then a rectal examination, which recovered "a balloon containing a foreign substance." *Id*. at 535. Over the next four days, she passed a total of eighty-eight balloons, all containing cocaine. *Id*. at 536.

The Ninth Circuit ruled that such an invasive search required "a 'clear indication' or 'plain suggestion' that the traveler was an alimentary canal smuggler." *Id*. at 536. The Supreme Court held that this standard was too high, but it did *not* fall back on its prior pronouncements that effectively eliminated the Fourth Amendment at the border. It instead summarized its prior cases by noting that "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant," *id*. at 538, and then pivoted to the facts at hand by stating, "We have not previously decided what level of suspicion would justify a seizure of an incoming traveler for purposes other than a routine border search," *id*. at 540. In other words, the Supreme Court seemed to be saying that its prior cases involved "routine" border searches, whereas the case *sub judice* did not.

Continuing this routine/nonroutine distinction, the Court eventually announced a holding specific to the alimentary canal smuggling context: "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection, is justified at its inception if customs agents, considering all the facts surrounding the traveler and her trip, reasonably suspect that the traveler is smuggling contraband in her alimentary

canal." *Id*. at 541. The Court found that this "'reasonable suspicion' standard has been applied in a number of contexts and effects a needed balance between private and public interests when law enforcement officials must make a limited intrusion on less than probable cause." *Id*. It emphasized, however, that this standard requires "a particularized and objective basis for suspecting the particular person of alimentary canal smuggling." *Id*. at 541–42 (internal quotation marks omitted).

The Supreme Court did not explain if this level of specificity was generally required in any nonroutine border search, or only required specifically in the "balloon swallowing" context because of the intrusiveness of the methods used to detect it. In any event, *Montoya de Hernandez* was the first and—so far—only time the Supreme Court has declared that a particular border search required any amount of suspicion.

On the facts of the case itself, the Supreme Court found that the border officers were justified by reasonable suspicion to take the various actions they took to confirm their suspicions, including the prolonged detention needed to ensure that the suspect passed all of the balloons. *Id*. at 542–44.

2. *Uribe-Galindo* (10th Cir. 1993)

Following *Montoya de Hernandez*, the Tenth Circuit has held that "the distinction between 'routine' and 'nonroutine' turns to a large extent upon the degree of intrusiveness of the particular type of search." *United States v. Uribe-Galindo*, 990 F.2d 522, 525 (10th Cir. 1993). *Uribe-Galindo* specifically involved a border search in which: (1) border patrol agents crawled under a vehicle and noticed numerous signs that the fuel tank had recently been worked on; (2) the agents then inspected the interior of the fuel tank with a fiber optic scope and saw fresh welding marks and some sort of unusual compartment within the tank; and finally (3) agents removed and disassembled the gas

tank, and thereby discovered marijuana. *Id*. at 523–24. The Tenth Circuit held that the initial action—crawling under the vehicle to inspect its undercarriage—was a "routine" border search. *Id*. at 525–26. And, once the agents saw the exterior of the fuel tank with their own eyes, including the signs of recent work on the tank, they possessed reasonable suspicion to employ the fiber optic scope and then to disassemble the tank. *Id*. at 524.

3. *Flores-Montano* (2004)

A very similar fuel tank search prompted one of the Supreme Court's more recent border search cases. In *United States v. Flores-Montano*, 541 U.S. 149 (2004), the defendant's car was detained at the border and an inspection agent noticed that the fuel tank sounded solid. *Id*. at 151. The inspection agent then ordered a mechanic contractor to remove and inspect the fuel tank, and that process revealed marijuana. *Id*. The Ninth Circuit, relying on the same "degree of intrusiveness" test followed by the Tenth Circuit since *Uribe-Galindo*, determined that removing a fuel tank was particularly intrusive, and therefore required reasonable suspicion, which was apparently lacking. *Id*. at 151–52. The Supreme Court rejected this reasoning, finding that there was no "degree of intrusiveness" test generically applicable both to persons and property:

> The Court of Appeals seized on language from our opinion in [*Montoya de Hernandez*—the "balloon swallower" case]. The Court of Appeals took the term "routine," fashioned a new balancing test, and extended it to searches of vehicles. But the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border searches of vehicles.

Id. at 152 (citations omitted). The Supreme Court rejected the defendant's argument

"that the disassembly and reassembly of his gas tank is a significant deprivation of his property interest because it may damage the vehicle." *Id*. at 154. The Court cited statistics of how frequently the Government disassembles and reassembles fuel tanks at the border, and those statistics showed no ensuing accidents or destruction. *Id*. at 154–55. Thus, "the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank. While it may be true that some searches of property are so destructive as to require a different result, this was not one of them." *Id*. at 155–56.

Williams summarizes *Flores-Montano*'s holding as follows: "the government's removal, disassembling, and reassembling of a vehicle's fuel tank was 'routine' and did not need to be based on reasonable suspicion." (ECF No. 19 at 9.) This is inaccurate in an important respect. The Supreme Court did *not* announce this holding in terms of the routine/nonroutine distinction seemingly established by *Montoya de Hernandez*. Indeed, it criticized the Ninth Circuit for having established such a distinction (although such a distinction seems obvious in *Montoya de Hernandez* itself). After summarizing and criticizing the Ninth Circuit's reasoning, the words "routine" or "nonroutine" do not again appear in the Supreme Court's opinion. The Court simply placed fuel tank inspections in the category of permissible "suspicionless" searches. *See also United States v. Cortez-Rocha*, 394 F.3d 1115, 1119 (9th Cir. 2005) ("the application of the routine/non-routine balancing test in these cases was specifically refuted in *Flores-Montano*"). Nonetheless, most courts after *Flores-Montano* still invoke the distinction between routine and nonroutine seemingly set up in *Montoya de Hernandez*.

4. Synthesis

The foregoing case law shows the general contours of the legal landscape: the

Government may conduct some searches at the border entirely without suspicion of criminal wrongdoing, while some other set of searches must be justified by reasonable suspicion. Notably, these appear to be the only two options—no party argues that there is a point when suspicion must rise to the level of probable cause, for example.

Once reasonable suspicion exists, the Government can resort to intrusive measures to determine whether a customs violation is present. In *Montoya de Hernandez*, for example, the presence of reasonable suspicion permitted Government officials to perform a pregnancy test and a rectal exam, and then to detain the suspected smuggler until nature took its course. And in *Uribe-Galindo*, reasonable suspicion permitted removal and disassembly of a gas tank (although *Flores-Montano* shows that the Government probably did not need reasonable suspicion in that instance).

5. Potential Application to Digital Devices

The parties' briefs largely focus on whether complete forensic searches of laptops and smartphones fall into the "suspicionless" category (Williams names this the "routine" category) or the "reasonable suspicion" category ("nonroutine," according to Williams). This question is not easily resolved. Some courts have held that digital devices are basically large briefcases and may be searched as routinely as real briefcases—which is to say, without suspicion. *See, e.g.*, *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005); *United States v. McAuley*, 563 F. Supp. 2d 672, 678 (W.D. Tex. 2008), *aff'd*, 420 F. App'x 400 (5th Cir. 2011); *United States v. Feiten*, 2016 WL 894452, at *5–6 (E.D. Mich. Mar. 9, 2016); *People v. Endacott*, 79 Cal. Rptr. 3d 907, 909 (Ct. App. 2008).

Most of these cases, however, predate the point when smartphone ownership

became nearly ubiquitous. Recognizing that digital devices can (and usually do) hold the equivalent of warehouses worth of private information about their owners, and that cloud computing may augment this by many orders of magnitude, various courts have quite naturally come to see searches of personal digital devices as highly intrusive. These courts have largely settled on a distinction between (1) a "manual" border search of a laptop or smartphone (examining a non-password-protected device by browsing through immediately available directories and files, akin to rummaging through luggage), which requires no suspicion; and (2) a forensic search that creates an easily searchable image of all data on the device, potentially including deleted data, and which can be preserved and examined at the Government's leisure, and accordingly requires reasonable suspicion. *See, e.g.*, *United States v. Cotterman*, 709 F.3d 952, 960–66 (9th Cir. 2013) (*en banc*); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 547–58 (D. Md. 2014).[4]

Under the facts of this case, the Court need not choose sides between the body of case law allowing unfettered border searches of digital devices and the competing body of case law distinguishing between manual and forensic searches. The Court likewise need not decide whether McGuckin's search was more like a manual search (because a password is like a luggage lock, which CBP may cut to inspect a suitcase, and McGuckin then browsed through active files and directories only) or a forensic

[4] Although addressing search-incident-to-arrest authority, not border search authority, the Supreme Court has endorsed the general principle that smartphones are *sui generis*, "differ[ing] in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). Thus, under most circumstances the Government must have a warrant to search a smartphone. *Id*. at 2495. *Riley* specifically discussed smartphones, not laptops, but a laptop often surpasses the data storage and cloud computing capacity of a smartphone. Moreover, the distinction between a laptop and a smartphone is becoming increasingly blurred through tablet computers that intentionally bear similarities to each.

search (because he used forensic software to bypass the password and to re-create the file structure, and he could then search the data at will, including deleted data if desired). If reasonable suspicion existed (regardless of whether the Supreme Court would require it to exist), then under all of the authorities all parties have cited, the border search doctrine would permit the search that McGuckin conducted before Allen obtained the search warrant.

The Court finds that reasonable suspicion existed, as explained below.[5]

B. Reasonable Suspicion

1. The Reasonable Suspicion Standard Generally

The Tenth Circuit has explained reasonable suspicion as follows:

> Reasonable suspicion is a less demanding standard than probable cause. Specifically, reasonable suspicion is merely a particularized and objective basis for suspecting criminal activity. To determine whether investigating officers had reasonable suspicion, we consider both the quantity of information possessed by law enforcement and its reliability, viewing both factors under the totality of the circumstances.

United States v. Mabry, 728 F.3d 1163, 1167 (10th Cir. 2013) (internal quotation marks, citations, and ellipses omitted). Reasonable suspicion, "does not deal with hard certainties, but with probabilities. Long before the law of probabilities was articulated as such, practical people formulated certain common sense conclusions about human behavior; jurors as factfinders are permitted to do the same—and so are law

[5] To be clear, Allen believed he could search Williams's laptop (or cause it to be searched) without any suspicion of any type, simply because Williams was trying to bring it through an international port of entry. Indeed, Allen directed McGuckin to come to the airport because Allen had already made up his mind to search any devices Williams might have brought with him. Allen's actions were motivated by the ICE Directive discussed at n.3, *supra*. But, as explained below, Allen's subjective state of mind is not relevant; and because objective reasonable suspicion existed, the Court need not and expressly does not rule on the validity of the ICE Directive.

enforcement officers." *United States v. Cortez*, 449 U.S. 411, 418 (1981).

The Government and Williams have debated precisely what Allen needed to suspect to have reasonable suspicion. However, Allen's "subjective beliefs and intentions are, quite simply, irrelevant." *United States v. McHugh*, 639 F.3d 1250, 1256 (10th Cir. 2011) (internal quotation marks omitted). Reasonable suspicion is an objective standard, asking only "whether the facts available to the detaining officer, at the time, warranted an officer of reasonable caution in believing the action taken was appropriate." *Id*. (internal quotation marks omitted).

Consistent with this objective standard, the Tenth Circuit does not require an officer to have a particular penal offense in mind. *United States v. Guardado*, 699 F.3d 1220, 1225 (10th Cir. 2012) ("[W]e reject the argument that the officers were required to have evidence linking [the defendant] to . . . particular criminal activity. Direct evidence of a specific, particular crime is unnecessary."); *see also United States v. Harmon*, 871 F. Supp. 2d 1125, 1160 (D.N.M. 2012) ("to establish that reasonable suspicion exists, officers have no obligation to articulate a specific offense which they believe the suspect may have committed"). It is generally sufficient if the facts known to the officer would reasonably, objectively suggest "some particular variety of criminal activity." 4 *Search & Seizure* § 9.5(c), text following n.122.[6]

[6] Williams argues, "[T]he Supreme Court has made clear that the reasonable suspicion standard relates to ongoing or imminent criminal activity, not historic acts," and for support, cites *Cortez*, 449 U.S. at 417, for the proposition that "[a]n investigatory stop must be justified by some objective manifestation that the person stopped is, or is about to be, engaged in criminal activity." (ECF No. 19 at 13.) The Court's analysis below demonstrates reasonable suspicion of an ongoing crime, so this distinction is immaterial here. Nonetheless, for clarity, the Court notes that Williams is wrong. Williams apparently failed to read the footnote attached to the quoted sentence from *Cortez*: "Of course, an officer may stop and question a person if there are reasonable grounds to believe that person is wanted for past criminal conduct." 449 U.S. at 417 n.2. The Supreme Court later made this footnote into a holding, at least with respect to felonies. *United States v. Hensley*, 469 U.S. 221, 229 (1985). The Supreme Court has since avoided the

2. Application to this Case

With these standards in mind, the Court turns to the facts of this case.

From the moment Allen examined Williams's customs declaration form and noticed that it omitted Germany from the list of countries visited, Allen had reasonable suspicion—and perhaps even probable cause—to suspect a violation of 18 U.S.C. § 1001, which criminalizes the act of making a false statement to a federal officer. *See, e.g.*, *United States v. Masters*, 612 F.2d 1117, 1121 (9th Cir. 1979) (affirming the false statements conviction based on customs declaration); *United States v. Parten*, 462 F.2d 430, 432 (5th Cir. 1972) (same).

Williams counters that he never made a false statement on his customs form. (ECF No. 32 at 9–10.) Williams seems to be saying that Allen had no evidence that Williams did anything but forget to list Germany on that form. However, an officer "need not rule out the possibility of innocent conduct, and reasonable suspicion may exist even if it is more likely than not that the individual is not involved in any illegality." *McHugh*, 639 F.3d at 1256 (citations and internal quotation marks omitted). Moreover, objectively speaking, a law enforcement officer would be more than justified in presuming that a person would not likely forget traveling to a country where he or she had been arrested in the last six months, and the law enforcement officer could therefore reasonably conclude that the omission was intentional and material.

Apart from this, Allen gained further reasonable suspicion of criminal wrongdoing during the interview with Williams. Allen knew Williams had been in Germany in the past six months, and in fact had been arrested there. Allen knew that Williams had

---

question as to lesser crimes. *See Navarette v. California*, 134 S. Ct. 1683, 1690 n.2 (2014).

omitted Germany from his customs declaration. Allen also witnessed Williams repeatedly evade questions about whether he had traveled to Germany.[7] Finally, on the claim forms for his laptop and smartphone, Williams listed an address that Allen knew to be different from the permanent address on his passport application and the address Williams had listed earlier that day on his customs declaration.

Considering all of the foregoing together, a reasonable official could suspect that Williams was attempting to conceal something about his travels abroad and also attempting to distance himself from his digital devices. A reasonable official could therefore conclude that Williams's digital devices contained evidence of an ongoing crime, such as materials whose importation into or possession in the United States would be a violation of customs or other laws.

3. Scope of the Subsequent Search

Williams argues that whatever reasonable suspicion may have existed did not justify detaining the laptop for several days beyond the initial border crossing and conducting a forensic search. (ECF No. 40 at 9–15.) Williams argues from case law about *Terry* stops (*see Terry v. Ohio*, 392 U.S. 1 (1968)), and the need for such stops to be limited in scope and length. But border searches with reasonable suspicion are not *Terry* stops, even though they both share the reasonable suspicion requirement. Once reasonable suspicion exists during a border search, Government officials have broad power to detain individuals and subject them to certain medical procedures, *see*

[7] Williams suggests he was not evading the Agents' questions about his travels to Germany, but instead "properly invoking his Fifth Amendment right against compulsory self-incrimination." (ECF No. 32 at 10.) The Court disagrees. Williams has not moved to suppress any of these statements. Moreover, a suspect invoking a Fifth Amendment right to remain silent must do so unambiguously. *Berghuis v. Thompkins*, 560 U.S. 370, 381–82 (2010). Telling the investigating officers where to find the answers (*e.g.*, "look in my passport," "ask the consulate in Casablanca") does not meet that standard.

Montoya de Hernandez, *supra*, and to disassemble physical objects, *see Uribe-Galindo supra*. Indeed, the cases on which Williams relies for the proposition that reasonable suspicion is a requirement also hold that once it exists, an away-from-the-border, days-later, full forensic search of digital devices is permissible. See *Cotterman*, *supra*; *Saboonchi*, *supra*.[8]

Williams also argues that whatever reasonable suspicion Allen may have had must be judged as of the time Williams's electronic devices were seized (*i.e.*, at the secondary inspection location, before the interview with Allen and Appel). (ECF No. 40 at 10.) The Court has already concluded that a law enforcement official could reasonably suspect a violation of 18 U.S.C. § 1001 by this point. But even if that were not the case, Williams's argument is incorrect. All that the various officers had successfully done prior to Williams's interview was seize Williams's luggage and digital devices, search the luggage, and unsuccessfully attempt to access the laptop and smartphone. CBP has extremely broad authority to visually inspect a traveler's belongings, with or without suspicion, *see Ramsey*, *supra*, and that is all that CBP officers had done before the interview.[9]

[8] The Court emphasizes strongly the effect that border search authority has on the foregoing analysis. If Williams had cleared customs without incident and had been stopped on the street a day later by a Denver Police Officer acting purely on reasonable suspicion, that almost certainly *would* be a *Terry* stop, and no amount of reasonable suspicion alone would permit a search of Williams's digital devices. Indeed, full probable cause supported by a search warrant would in all likelihood be necessary in that very different setting. *See Riley*, *supra*. But, as the above discussion sets out, current controlling authority makes plain that, at the border, reasonable suspicion gives border officials much more authority.

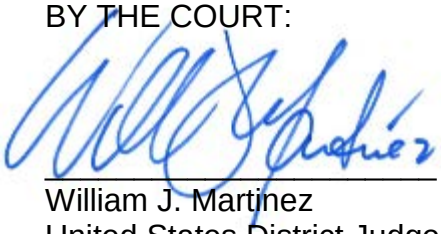
[9] Williams has not pointed the Court to any decision in which it was significant that the government succeeded in lawfully searching property only after a previous failed attempt to search the property in an unlawful way. Thus, the Court finds it of no significance that McGuckin tried and failed to access the laptop and smartphone at the airport, allegedly before Allen possessed reasonable suspicion.

IV. CONCLUSION

For the reasons set forth above, Williams's Motion to Suppress (ECF No. 19) is DENIED. A new trial setting will enter by separate order.

Dated this 25th day of September, 2017.

BY THE COURT:



William J. Martínez
United States District Judge