

**PUBLISH**

**UNITED STATES COURT OF APPEALS**  
**FOR THE TENTH CIRCUIT**

**November 14, 2019**

**Elisabeth A. Shumaker**  
**Clerk of Court**

---

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

No. 18-1299

DERRICK LUCIUS WILLIAMS, JR.,

Defendant - Appellant.

-----

ELECTRONIC FRONTIER  
FOUNDATION,

Amicus Curiae.

---

**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.**