IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

United States of America	)	
	)	
	)	
v.	)	No. 16 CR 296
	)	
	)	
Donald Wanjiku	)	

Memorandum Opinion and Order

On June 2, 2016, a grand jury returned an indictment charging defendant Donald Wanjiku with one count of transportation of child pornography in violation of 18 U.S.C. § 2252A(a)(1). Before me is Mr. Wanjiku's motion to suppress evidence obtained during a search of his electronic devices at O'Hare International Airport on June 9, 2015, as well as all evidence later obtained as a result of that search. On March 21, 2017, I held an evidentiary hearing on the motion. Having closely considered the parties' arguments and the evidence presented, I deny the motion for the reasons explained below.

I.

Unless noted otherwise, the following facts are undisputed. On June 9, 2015, Mr. Wanjiku arrived at O'Hare after a sixty-day trip to the Philippines. At the primary inspection site (i.e., the passport control area through which all international travelers must pass), a Customs and Border Patrol ("CBP")

officer referred Mr. Wanjiku for secondary inspection in an area known as "baggage control hall A," where CBP and Homeland Security Investigations ("HSI") were conducting a special operation dubbed "Operation Culprit." During the secondary inspection, CBP officer Adam Toler discovered and initiated searches of three electronic devices belonging to Mr. Wanjiku—a cell phone, a laptop computer, and an external hard drive. The government's searches of these devices produced photographic and video evidence of suspected child pornography, which led to the charges in this case.

Officer Toler testified at the suppression hearing about Operation Culprit and his inspection of Mr. Wanjiku. He began by describing Operation Culprit as targeting "certain flights that were coming from areas of high sex tourism," specifically, Philippines, Thailand, and Cambodia. H'rg. Tr. at 5:1-3. Four officers, including Officer Toler, participated in the operation. Officer Toler testified that to identify individuals potentially of interest, he and his fellow agents culled the list of all passengers arriving from those countries into a "manageable list" of people who "seem[ed] to match the scope of our operation." *Id*. at 6:14, 8:4. They began by "looking for U.S. citizens, males, returning from one of those countries that were traveling alone," who had a prior criminal history, and who were between the ages of eighteen and fifty or sixty. *Id*. at

5:10-12, 22. The agents used something called the "TECS platform" to search "all databases linked to CBP," including NCIC and ADIS (i.e. Arrival and Departure Information System), for information about the travelers' arrival and departure records, their criminal histories, and the e-mail addresses and telephone numbers they used to book their reservations. *Id*. at 40:18-23; 53:11-18. Because Mr. Wanjiku satisfied each of the initial screening criteria, his name was included on the agents' preliminary list of individuals potentially of interest to Operation Culprit. *Id*. at 7:19-21.

Officer Toler stated that he and his fellow agents then "worked through each individual name to see if we could whittle the list down a little bit more." H'rg. Tr. at 7:23-25. For example, "if you've got a man who is from the Philippines who is traveling to the Philippines where he is originally from and his criminal history is something like a drunk driving arrest, it doesn't seem to match the scope of our operation, so we would remove him from the list." *Id*. at 7:25-8:5. At this stage of screening, which took place prior to Mr. Wanjiku's arrival, agents discovered that Mr. Wanjiku's criminal history included an arrest for contributing to the delinquency of a minor, which Officer Toler testified "heightened our level of suspicion on him because we are dealing with sex tourism where a lot of the victims are minors." *Id*. at 8:15-19. The agents also noticed

that Mr. Wanjiku had made three trips to the Philippines in the preceding two years, *id*. at 10:1-3, which Officer Toler testified "seem[ed] strange" because Mr. Wanjiku had no apparent affiliation with that country, such as a wife who was from there, a record of "people traveling to his address from the Philippines,"[1] employment affiliations, or "something that we could see that he is somehow tied to the Philippines." *Id*. at 9:2-3, 11:3-9.

The agents' pre-arrival investigation of Mr. Wanjiku also revealed that an email address linked to one of his prior trips was "Mr. Dongerous, D-o-n-g-e-r-o-u-s," which Officer Toler testified further heightened their suspicions "because DONG is the name or slang name for male genitalia." *Id*. at 8:22-24. The agents plugged this email address into Facebook and found what they believed to be Mr. Wanjiku's profile, and which showed a picture of him in a mask, as well as "multiple friends who seemed very young." *Id*. at 12:17-23. Officer Toler stated that these factors further increased their interest in Mr. Wanjiku because Operation Culprit "is for sex tourism and exploitation of children, and to see somebody who has multiple young friends on their Facebook seemed a little strange, especially for

[1] Officer Toler explained, "You can run a person's address through TECS and see if anybody has listed on their I94 which is their arrival document...where they're going to be in the United States." H'rg. Tr. at 62:9.

somebody who is in his 40s. Also, to have -- be wearing a mask in your Facebook profile, that seemed a little strange as well." *Id*. at 13:1-6.

Based on the factors described above, the agents included Mr. Wanjiku among the individuals flagged in the TECS system with a "one day lookout" to signal to the primary border control officers that the individuals should be sent to baggage hall A for secondary inspection. *Id*. at 16:6-17:5. According to Officer Toler, the primary officer indicated in notes provided to secondary officers that Mr. Wanjiku was "evasive for questioning." *Id*. at 46:21-22.

Officer Toler described the secondary inspection process generally as follows:

> Once the people came in, we were doing the baggage inspections on all the people who were referred based on our operation. And so we would take their bags, we would get a binding declaration from them. Of course, I would get a binding declaration from them. I would ask them about what they were doing out of the United States. Get a story about their trip. Then open up their bags, go through their bags and pretty much make sure that everything in their bags corroborated with what they said about their trip.
>
> *Id*. at 17:20-18:3.

Officer Toler stated that he first saw Mr. Wanjiku while he was waiting in line while Toler and the other officers completed other baggage exams. Then, Mr. Wanjiku did something Officer Toler had never seen before: he left the line before it was his

turn for examination. Indeed, Officer Toler later discovered, after Mr. Wanjiku was escorted back to the line by an ICE agent, that Mr. Wanjiku had gotten out of the general queue in baggage hall A and gone to baggage hall B—an area approximately one to two hundred feet away and across an exit corridor—to use the bathroom.

Officer Toler stated that the first thing he asked Mr. Wanjiku was why he had gone to the other hall, to which Mr. Wanjiku responded that he had heat stroke and needed to use the bathroom. *Id*. at 24:13-15. Officer Toler informed Mr. Wanjiku that there were also bathrooms in baggage hall A.[2] He perceived Mr. Wanjiku as "visibly nervous about the whole situation," noting that he was "sweating profusely" (although the airport is air-conditioned) and that he was "shifting his weight." *Id*. at 24:16-18.

Officer Toler proceeded to question Mr. Wanjiku about his trip, explaining that his purpose was to "get[] his story of his trip," to get "a set of facts" he would then compare with the contents of his luggage to see whether the items corroborated or did not corroborate the story. In Officer Toler's view, several elements of Mr. Wanjiku's story didn't add up. First, Mr. Wanjiku told Officer Toler that he had stayed with friends in

[2] Officer Toler confirmed that the bathrooms in baggage halls A and B are marked identically. *See* H'rg. Tr. at 23:4-11.

the Philippines, and he provided their address. Yet, his luggage contained "a pocket full of receipts" for hotel stays, most of which were for one night. *Id*. at 31:8-11. When Officer Toler asked him about the receipts, Mr. Wanjiku explained that "his friend showed him around the country and those were receipts for going around the country." *Id*. at 31:17-18. But that explanation didn't alleviate Officer Toler's concerns. Two of the receipts were for the same hotel on two different occasions, about a week apart. In Officer Toler's view, "if you're going around the country, usually you move on to a different place. You don't stay at the same hotel a week apart." *Id*. at 31:21-25.

In addition, Officer Toler discovered condoms, needles, and syringes in Mr. Wanjiku's bag. Mr. Wanjiku explained that the needles were for medication he was carrying in another bag. Indeed, a bag being searched by another CBP officer contained injectable testosterone.[3] About this, Officer Toler testified, "I don't know much about medication, I'm not a doctor, but anything with testosterone seems like it's for male genitalia, I don't know. It's sexually specific." *Id*. at 32:23-25.

[3] The prescription was for "Donald Kwiatkowski," which Mr. Wanjiku explained was his name before he had it legally changed. Mr. Wanjiku showed the officers a social security card with that name to prove that it was indeed his previous name. Officer Toler testified that another officer "started doing checks on that other name to see if he had traveled using that name or had a criminal history under that name as well," Hr'g. Tr. at 3-22, but the record does not reflect what information, if any, those checks produced.

Officer Toler then asked Mr. Wanjiku to unlock his cell phone, i.e., to put in the password so that it could be operated. Mr. Wanjiku asked several times why he had to unlock his cell phone, and Officer Toler explained that "if he chose not to unlock it, that [he] would detain the phone and send it to the lab to be unlocked pursuant to [the government's] border search authority." *Id*. at 65:22-66:1. Mr. Wanjiku was "upset," but he unlocked the phone. *Id*. at 66:4-8. Officer Toler began manually "scrolling through pictures" and discovered several depicting Mr. Wanjiku "laying (sic) in bed with a man who is in his underwear." *Id*. at 34:7, 36:12-13. Although Officer Toler described the other individual as a man, he said "I don't know how old this person is, so I asked for ICE to look through it."[4]

Officer Toler testified that Mr. Wanjiku's secondary examination lasted approximately an hour to an hour and a half. And the end of the inspection, his devices were seized, and he was released into the public area of the airport. *Id*. at 38:11-25.

On cross-examination, defense counsel challenged the reliability of the facts the CBP agents used to screen for potential targets and questioned the inferences Officer Toler

[4] The photos Officer Toler viewed were submitted into evidence. I have reviewed them, and I find Officer Toler's testimony that he did not know the approximate age of the individual pictured with Mr. Wanjiku to be credible.

claims to have drawn for them. For example, counsel asked Officer Toler whether he knew the date, state, or circumstances of Mr. Wanjiku's arrest for contributing to the delinquency of a minor. Officer Toler admitted that he did not, nor did he know the disposition of that case. H'rg. Tr. at 17:21-18:23. Officer Toler also admitted that his basis for believing that Mr. Wanjiku had traveled alone to the Philippines was not iron-clad: if, for example, a friend had booked a ticket for the same itinerary on a separate reservation, agents would not be able to verify that. *Id*. at 46:2-5. Counsel also challenged Officer Toler's conclusion that the "Mr. Dongerous" email referred to male genitalia, observing that "Don" could also refer to Mr. Wanjiku's first name, Donald. *Id*. at 54:20-55-5. Officer Toler also acknowledged that nothing on the Facebook page he believed to be Mr. Wanjiku's suggested sex tourism, child pornography, or sex trafficking. *Id*. at 52:23-53:5.

The government then called Special Agent Kevin Gerlock, an expert in digital forensic examinations, to testify about the searches that were conducted on Mr. Wanjiku's electronic devices after Mr. Wanjiku himself was admitted into the United States. A detailed discussion of the technical processes that Agent Gerlock testified the government used to search Mr. Wanjiku's devices is unnecessary. In broad brushstrokes, Agent Gerlock explained that at the airport, HSI Special Agent Mark Bowers

performed a forensic "preview" of Mr. Wanjiku's external hard drive using software called "enCase." The preview allowed Agent Bowers to see a "gallery view" of all of the images and videos stored on the device. He then viewed a few of the videos. The search took under an hour and was performed while Mr. Wanjiku was still at the airport. The search revealed six videos of suspected child pornography, which Agent Bowers copied to a CD and gave to the case agent. Agent Bowers did not search "unallocated space" in the drive, meaning he did not view any items that the user had deleted. H'rg. Tr. at 84:1-86:1.

HSI agents also performed a "preview" of Mr. Wanjiku's cell phone at O'Hare on June 9, 2015. Agent Gerlock explained that to preview a cell phone, agents typically use special software to extract data and create an HTML report. He explained, "you can't just go on a phone and start tapping around and going through things because you affect the phone." *Id*. at 92:16-18. The data extracted in a preview does not get deleted or hidden files, but only "images and videos in files that [the software] can see." *Id*. at 92:24-25. The agents' phone preview in this case took a little over an hour. The search was confined to photographs; the agents did not search text messages, emails, or anything else on the phone. *Id*. at 95:21-96:5. The preview continued the following morning, when the same process was used to search videos. The video search also took approximately an hour. *Id*. at

98:1-22. In total, the phone previews uncovered fourteen images of suspected child pornography. *Id*. at 99:23-100:12.

Finally, the agents searched Mr. Wanjiku's laptop computer, although no preview was conducted at O'Hare because the agents lacked the necessary equipment. The agent who conducted the search, Rodney Hart, "looked for images, videos, and basically any attributes that dealt with the other videos that were found on the external hard drive. In other words, we already had the videos from the external hard drive. He was just looking to see the connectivity between the two." *Id*. at 104:20-24. The search did not re-create files or restore any deleted items. It lasted under three hours. Additional suspected child pornography was found. *Id*. at 105:17-20.

On July 7, 2015, the government obtained a search warrant authorizing full forensic examinations of Mr. Wanjiku's cell phone, laptop, and external hard drive. Agent Gerlock explained that a full forensic examination is a different process from a forensic preview. It takes substantially longer (anywhere from a day to three or four months), and "allows you to process information," recover deleted files, and correlate data. *Id*. at 81:10-21. Agent Gerlock acknowledged on cross-examination, however, that the same software the agents used to preview the hard drive was also used for the full forensic examination. In fact, all of the processes used at O'Hare "would have recovered

the evidence that's being introduced in this case." *Id*. at 114:5-6. Indeed, it does not appear that the full forensic searches uncovered any additional evidence of child pornography.

II.

> This case stands, as another court recently put it,
>
> > at the intersection of two avenues of law. Heading in one direction is the Supreme Court's bright line rule in *Riley [v. California*, 134 S. Ct. 2473 (2014)]: law enforcement officers must obtain a warrant to search a cell phone incident to an arrest. Heading on a different course is the border search exception. The border search exception describes an exception to general Fourth Amendment principles. It is the notion that the government may search without a warrant anyone and anything coming across its border to protect its national sovereignty.

United States v. Caballero, 178 F. Supp. 3d 1008, 1014 (S.D. Cal. 2016). Indeed, on the one hand, courts around the country, including the Seventh Circuit, have uniformly acknowledged that the government may conduct routine border searches without any level of suspicion. *United States v. Johnson*, 991 F.2d 1287, 1291 (7th Cir. 1993) (citing *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985)). And while "non-routine" border searches—such as the alimentary canal search at issue in *Montoya de Hernandez,* and the forensic digital search conducted in *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013)—have been held to require reasonable suspicion, no court has held that the government must obtain a warrant before searching a traveler's electronic devices at the border. On the other hand,

the Court recognized in *Riley* that because "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated" when the government conducts searches of physical items such as an individual's wallet or purse, the factors that support warrantless searches of the latter in certain circumstances do not necessarily justify warrantless searches of an individual's "digital data." *Id*. at 2488-89.

Acknowledging that the Seventh Circuit has not defined the level of suspicion required to conduct an electronics search at the border, the government asks me to hold that brief manual or software-supported border searches of electronic devices are equivalent to routine border searches of physical items, and thus require no individualized suspicion. *See, e.g., U.S. v. Stewart,* 729 F.3d 517, 525 (6th Cir. 2013) (no reasonable suspicion required for non-forensic examination of laptop); *United States v. Arnold*, 533 F.3d 1003, 1008 (9th Cir. 2008) ("reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border"); *United States v. Feiten*, No. 15-20631, 2016 WL 894452, at *4 (E.D. Mich. Mar. 9, 2016) (a "forensic preview search of three different electronic devices" was a routine border search requiring no individualized suspicion). Alternatively, the government argues that even if the government's pre-warrant searches of Mr. Wanjiku's devices were

non-routine and thus required reasonable suspicion, the information known to Officer Toler at the time he initiated the searches was adequate to satisfy this standard.

Mr. Wanjiku, for his part, urges me to reject an analytical framework premised on the distinction between routine and "forensic" electronics searches, emphasizing the evanescence of this distinction in today's rapidly changing technological environment as well as its insensitivity to the significance of the privacy interests at stake when digital searches are at issue. Indeed, as the Court recognized in *Riley*, even cursory border searches are capable of revealing troves of the kind of personal and private information the Fourth Amendment is intended to protect. *See* 134 S. Ct. at 2491 (observing that cell phones can access information stored remotely "at the tap of a screen."). On these grounds, Mr. Wanjiku argues that even at the border, the government should be required to obtain a warrant before conducting any type of search of a cell phone or other personal electronic device, and that at a minimum, it must establish reasonable suspicion for such a search. Mr. Wanjiku goes on to argue that the government did not have reasonable suspicion to search his electronic devices in this case, particularly since it was clear from the moment he was "flagged" for secondary inspection that his devices would be searched.

While I am inclined to agree with defendant, and with the court's conclusion in *United States v. Kim*, 103 F. Supp. 3d 32 (D.D.C. 2015), that construing the border search doctrine to allow the government unfettered access to information contained on (or accessible by) an individual's personal electronic devices without any suspicion at all, so long as the search is reasonably brief, is not physically invasive or embarrassing, and does not damage the individual's property, would "untether" the rule from the justifications underlying it, *see id*. at 55-56; and I further agree that the Court's decision in *Riley* rejects the government's claim that searches of cell phones or other electronic devices are analytically equivalent to searches of physical items, and may indeed suggest the Court's willingness to reevaluate, in the age of modern cell phones, whether the balance of interests should continue to be "struck much more favorably to the Government at the border" where digital searches are concerned, cf. *Montoya de Hernandez*, 473 U.S. at 540, I conclude that this is not the appropriate case in which to wrestle these difficult issues to the ground. Instead, I deny defendant's motion on the ground that the information available to the government at the time it initiated the searches of Mr. Wanjiku's electronic devices was sufficient to trigger a reasonable suspicion that he was involved in the kind of criminal activity targeted by Operation Culprit.

To review basic principles: Reasonable suspicion exists where an officer can "point to specific and articulable facts which, taken together with rational inferences from those facts," cause the officer to conclude that "criminal activity may be afoot." *Terry v. Ohio*, 392 U.S. 1, 21, 30 (1968). The standard takes into account "the totality of the circumstances—the whole picture," *Navarette v. California*, 134 S. Ct. 1683, 1687 (2014), and while it requires more than a mere "hunch," the level of suspicion necessary is "considerably less than proof of wrongdoing by a preponderance of the evidence, and obviously less than is necessary for probable cause." *Id.* at 1687 (internal quotation marks and citations omitted).

By the time Officer Toler began searching Mr. Wanjiku's belongings, the facts available to him included: 1) that Mr. Wanjiku was a U.S. citizen male in his 40's returning from an extended trip by himself to the Philippines, a country with which he had no obvious connection, to which he had traveled several times in the preceding two years, and which was a known destination for sex tourism; 2) that Mr. Wanjiku had been arrested for contributing to the delinquency of a minor, a crime that, like child pornography, involved a minor victim; 3) that Mr. Wanjiku used an email address that Officer Toler construed as a possible reference to male genitalia; 4) that Mr. Wanjiku's Facebook page included a profile picture of him in a mask and

showed that he had multiple friends who seemed very young; 5) that the primary border officer's notes stated that Mr. Wanjiku had been "evasive for questioning" during primary inspection; 5) that Mr. Wanjiku left the secondary inspection line prior to his inspection—something Officer Toler stated he had never seen before—and offered a questionable explanation for his departure after being escorted back to the line by an ICE agent; and 6) that Mr. Wanjiku appeared visibly nervous during inspection, sweating profusely and shifting his weight.

In addition, upon examining the contents of Mr. Wanjiku's bag, Officer Toler found hotel receipts that called into question his previous account of where he had stayed during his trip. Officer Toler also found condoms, syringes, and injectable testosterone. While none of these bits of evidence, taken alone, gives rise to a reasonable suspicion of wronging, "reasonable suspicion need not rule out the possibility of innocent conduct." *U.S. v. Navarette*, 134 S.Ct. 1683, 1691 (2014) (quotation marks and citation omitted). Indeed, while any of the above "flags" might have had an innocent explanation, Officer Toler could conclude that collectively, they raised a reasonable suspicion that a search of Mr. Wanjiku's electronic devices would reveal evidence of criminal activity involving minors. *See Cotterman*, 709 F.3d at 968 ("[E]ven when factors considered in isolation from each other are susceptible to an innocent

explanation, they may collectively amount to a reasonable suspicion.") (alteration in original) (citation omitted)).

Moreover, I disagree with Mr. Wanjiku that "the clock for reasonable suspicion should stop" at the time he was targeted for secondary inspection. H'rg. Tr. at 123:25-124:9. The reasonable suspicion determination considers whether "the facts available to the officer *at the moment of the seizure*" support an objective conclusion that the search was reasonable. *Terry*, 392 U.S. at 21-22 (emphasis added). Although Officer Toler acknowledged that he knew he would search Mr. Wanjiku's electronic devices as soon as he was referred for secondary inspection, H'rg. Tr. 56:10-23, an officer's subjective reasons for initiating a search are irrelevant. *United States v. Williams*, 627 F.3d 247, 254 (7th Cir. 2010) (citing *Whren v. United States*, 517 U.S. 806, 813 (1996)).

In short, the record reflects that the agents involved in the searches based their decision to search Mr. Wanjiku's electronic devices on particularized, objective facts that caused them to suspect he was involved in criminal activity. Moreover, even if their understanding of those facts was mistaken—for example, if Mr. Wanjiku was not traveling alone, or if he was sweating not out of nervousness but because of heat stroke—it no less supported reasonable suspicion. *Cotterman*, 709 F.3d at 968 ("the agents' *understanding* of the objective

facts, albeit mistaken, is the baseline for determining reasonable suspicion.") (original emphasis). Accordingly, the searches did not violate the Fourth Amendment.

III.

For the foregoing reasons, I deny defendant's motion to suppress.

ENTER ORDER:

Elaine E. Bucklo
United States District Judge

Dated: April 7, 2017