UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------x
UNITED STATES OF AMERICA

MEMORANDUM AND ORDER
22-CR-149 (NRM)

-against-

KURBONALI SULTANOV,

Defendant.

----------x

NINA R. MORRISON, United States District Judge:

Pending before the Court is Defendant Kurbonali Sultanov's motion to suppress evidence obtained by the government (1) during Sultanov's detention and questioning at John F. Kennedy International Airport upon Sultanov's reentry into the United States, and (2) thereafter through a warrant issued for a search of two cell phones seized from Sultanov on the day of his reentry. The Court has considered the parties' written briefs, the testimony adduced and exhibits entered at the suppression hearing held on March 21, 2023, the parties' statements from oral argument held on April 18, 2023, and the supplemental briefs filed by the parties and amici thereafter. For the reasons outlined below, Sultanov's motion is GRANTED IN PART and DENIED IN PART.

OVERVIEW

On March 5, 2022, Kurbonali Sultanov was detained in a secondary inspection area at John F. Kennedy International Airport ("JFK") and directed to turn over his cell phone and passcode. After law enforcement officials manually

searched Sultanov's phone, two Special Agents questioned Sultanov regarding the contents of his device. Relying on information from its search of Sultanov's cell phone and his statements to the Special Agents, the government subsequently obtained a warrant to search two cell phones that were in Sultanov's possession when he reentered the country. Sultanov was subsequently indicted on one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B), 2252(b)(2), and 3551 *et seq*.

Sultanov now seeks to suppress both the contents of his cell phones and the statements he made to law enforcement while in the secondary inspection area. In support of his motion to suppress the physical evidence, Sultanov argues that the Fourth Amendment requires the search of a cellular device at the border to be supported by a warrant and probable cause — neither of which was present here. This raises the unsettled issue — one that is percolating among district courts within this Circuit, but which the Second Circuit has not yet addressed — whether the historical exemption to the warrant requirement at the border must yield to the heightened privacy interests implicated by the search of a modern cell phone. Because "[c]ell phones differ in both a quantitative and a qualitative sense from other objects" a traveler might bring across the border, the Court concludes that it must so yield, and that the government should have obtained a warrant before conducting its search. *Riley v. California*, 573 U.S. 373, 393 (2014). Nevertheless, the Court denies Sultanov's motion to suppress the evidence contained on his phones because the search warrant was issued and executed in good faith.

Sultanov also seeks to suppress the statements he made to the government, including an earlier statement providing his cell phone passcode to a customs official and later statements to the Special Agents. He argues that these statements violate the Fifth Amendment because he did not waive his *Miranda* rights before making them. The Court concludes that, while Sultanov's initial questioning in secondary inspection was not "custodial" (and thus did not trigger the government's duty to read him his *Miranda* rights), the subsequent questioning by the Special Agents constituted a "custodial interrogation." The Court also finds that Sultanov — whose first language is not English, and who expressly told the agents that he only understood the *Miranda* warnings "50/50" — did not knowingly waive his *Miranda* rights before making certain statements during that custodial interrogation, and Sultanov's motion is granted as to those statements.

FACTS AND PROCEDURAL HISTORY

The Court makes the following findings of fact based on the testimony and evidence presented at a suppression hearing held in this case and in exhibits offered by both parties.

I. Background Facts

Kurbonali Sultanov is a United States citizen who was naturalized from Uzbekistan. HSI Tr. dated Mar. 5, 2022 ("HSI Tr.") 5:89–91, Gov't Ex. 4-T.[1] In late

[1] References to "Gov't Ex." are to the exhibits submitted during the Suppression Hearing held on March 21, 2023, and "Oral Arg. Tr." indicates the transcript from argument on Defendant's motion held on April 18, 2023. While these documents are part of the record of the case, they are not filed on the docket.

2021, Sultanov traveled to Uzbekistan through Europe to visit his family, *id.* at 12:233–34, and stayed there for roughly three months, *id.* at 14:288–91. On January 12, 2022, the United States received an alert through the Treasury Enforcement Communications System ("TECS") that Sultanov had been identified as a possible purchaser or possessor of child sexual abuse material. Suppression Hr'g Tr. 25:17–26:5, ECF No. 35. The TECS "is an investigative tool of the Department of Homeland Security that keeps track of individuals entering and exiting the country and of individuals involved in or suspected to be involved in crimes." *United States v. Cotterman*, 709 F.3d 952, 957 n.3 (9th Cir. 2013).

On March 5, 2022, approximately two months after the government received the TECS alert, Sultanov reentered the United States at JFK. HSI Tr. 1:1. Upon his arrival, Transportation Security Administration ("TSA") agents at JFK's primary inspection area became aware of the TECS hit for Sultanov and redirected him to a secondary screening area. Suppression Hr'g Tr. 23:22–24:2.

At secondary screening, Sultanov was asked for and provided his cell phone passcode to a United States Customs and Border Protection ("CBP") officer. *Id.* at 28:4–5. The CBP officer conducted a manual search of Sultanov's cell phone, *id.* at 30:2–6, and discovered what he believed to be child pornographic material, *id.* at 32:1–5. The CBP officer had Sultanov wait in secondary screening until agents from Homeland Security Investigations ("HSI") arrived to speak with Sultanov concerning the material on his phone.

Several hours later, two HSI agents arrived at the secondary inspection area of JFK, *id.* at 74:10–17, and conducted their own review of the material on Sultanov's phone, *id.* at 77:12–79:4. After searching Sultanov's phone, the HSI agents sequestered Sultanov in a smaller room within the secondary inspection area and conducted a recorded interview of him. *Id.* at 79:9–18.

Before questioning Sultanov, the HSI agents administered *Miranda* warnings. HSI Tr. 2:15–3:26. In response to the *Miranda* warnings, Sultanov told the agents that he understood the warnings "50/50." *Id.* at 3:27. Sultanov then proceeded to speak at length with the HSI agents, who continued questioning him about the contents of his phone without further clarifying the *Miranda* warnings. *Id.* at 3:40–41. After the HSI agents finished questioning Sultanov, they arrested him and took possession of the cell phone the CBP officer and HSI agents had searched and an additional cell phone that was turned off and stored in Sultanov's luggage. Suppression Hr'g Tr. 94:20–95:7.

On March 17, 2022, the government obtained a warrant from Magistrate Judge James R. Cho, authorizing the forensic examination of both of the cell phones seized from Sultanov two weeks earlier. *See* Appl. for Search Warrant at 23, ECF No. 33-1. Shortly thereafter, on April 1, 2022, Sultanov was indicted on one count of possession of child pornography under 18 U.S.C. § 2252(a)(4)(B), 2252(b)(2) and 3551 *et seq*. Indictment 2, ECF No. 6.

On October 31, 2022, this action was reassigned to the undersigned. *See* Text Order dated Oct. 31, 2022. The Court held a status conference on December 13,

2022, at which Sultanov stated his intention to move to suppress the statements that he made to law enforcement as violative of his Fifth Amendment right against self-incrimination, as well as the videos seized from his cell phones as violative of his Fourth Amendment right to be free from unreasonable, warrantless searches. *See* Min. Entry dated Dec. 13, 2022. After the parties filed their initial briefs on the motion, *see* Mot. to Suppress, ECF No. 21; Response in Opp'n, ECF No. 22, the Court held a suppression hearing on March 21, 2023, Min. Entry dated Mar. 21, 2023.

II. The Suppression Hearing

The Court first heard testimony from CBP Officer Marves Pichardo, who was the first official to examine Sultanov's cell phone and obtain his passcode. Suppression Hr'g Tr. 3:21–69:3. The government then presented testimony from HSI Agent Joshua Croft, who examined Sultanov's cell phone at JFK, questioned Sultanov concerning the material on his phone in a lengthy recorded interview, seized Sultanov's cell phones, and arrested him. *Id.* at 69:14–122:22.

A. CBP's Practices for Questioning Travelers Entering the United States at JFK and Searching Their Electronic Devices

i. Primary Inspections

Pichardo testified that all travelers entering the United States from another country through JFK must pass through "primary inspection" by CBP before being admitted into the United States. *Id.* at 6:3–7. During primary inspection, CBP officers review a traveler's identification and customs declaration form and may ask limited questions concerning, for example, the reason for a person's travel and

whether they have anything to declare to customs. *Id.* at 7:4–12. The CBP officer conducting the primary inspection has discretion to refer the traveler for further evaluation by CBP in a secondary inspection area. *Id.* at 7:17–23.

A traveler may also be directed into secondary inspection for additional screening if the CBP officer conducting the primary inspection sees a "hit or a lookout on that specific person" in a database called TECS, or Treasury Enforcement Communications System. *Id.* at 7:20–23. A hit or lookout may be entered by another government agency into TECS for a variety of reasons. For a noncitizen traveler, the Department of State might enter a lookout in TECS to ensure that a noncitizen who was previously denied a visa is traveling with a new, valid visa. *Id.* at 8:8–11. For U.S. citizens, a hit might be entered because "their travel is a little inconsistent," they are "coming from any source countries," and/or an agency wants to ensure they are "abiding by [U.S.] laws and regulations." *Id.* at 8:12–17. Regardless of the particular reason for the hit, a hit is "typically derogatory" and signals that a government agency has determined that "something that has happened in the past" may "require[] additional screening or a more in-depth look into that person coming from abroad." *Id.* at 8:1–5.

ii. Secondary Inspections

When a CBP officer conducting a primary inspection determines that a traveler requires additional screening, the traveler must be escorted to the secondary inspection area of the airport. *Id.* at 7:20–23. Upon arrival to the secondary inspection area, the CBP officer who conducted the primary inspection places the traveler's passport in the possession of the CBP officers conducting the

secondary inspection and directs the traveler to take a seat. *Id.* at 13:7–12. At JFK, the secondary inspection area, which is "adjacent" to the primary inspection area, is roughly 60 feet by 40 feet in size and can seat 30 to 40 people at a time. *Id.* at 10:14–11:8. The secondary inspection area is connected to an overflow room with additional seating, holding cells, and interview rooms. *Id.* at 22:14–19.

Pichardo testified that the doors to the secondary inspection area "always remain open," *id.* at 14:10–12, but that the officers processing secondary inspections "keep eyes . . . on the travelers" to "mak[e] sure that no one tries to leave the area," *id.* at 11:13–20. Travelers detained in secondary inspection are not free to leave that area. *Id.* at 39:11–40:25, 42:17–43:3, 52:16–20.

Some, but not all, travelers may also be shackled by their feet, especially if they are subject to expedited deportation. *Id.* at 62:3–9. While water fountains and bathroom facilities are present in the secondary inspection area, *id.* at 22:8–11, any traveler who wishes to use the restroom must be escorted to the restroom by an officer, *id.* at 41:21–42:2. Travelers held in the secondary inspection area are not allowed to use the restroom privately; instead, the escorting officer requires them to keep the door open and "watch[es] them, from a distance, use the restroom." *Id.*

Pichardo testified that, pursuant to "our laws and regulations," as part of conducting a secondary inspection, he sometimes asks travelers to give him their cell phones. *Id.* at 14:13–17. Such interactions are "generally" one-on-one, but "if need be, you do have your officers there to back you up." *Id.* at 15:4–9. Pichardo, who has performed "over a thousand" secondary inspections and has received

training on how to conduct such inspections, *id.* at 9:9–22, testified that it "would be hard" to estimate the number of times he has asked to search a traveler's cell phone and that he asks on a "case-by-case basis" depending on "travel history" and "background information that we get from our system checks," *id.* at 15:17–23.

Under current CBP protocols, a traveler can, in theory, refuse to turn over her phone or passcode. *Id.* at 46:10–13. However, doing so would subject the phone to temporary seizure, even if the traveler is allowed to leave the airport — that is, if a traveler refused to provide his passcode and allow the phone to be searched by officers at the screening area, CBP would take custody of the phone, and the traveler would have to leave it behind. *Id.* at 45:19–46:5.

Pichardo testified that he has never had a single traveler refuse to surrender her phone or passcode when asked. *Id.* at 44:19–45:12, 57:2–12, 61:8–21, 63:5–13. And because no traveler has ever declined to allow CBP to inspect the contents of her cell phone, he has never requested a supervisor's assistance, nor has he ever seen one of his fellow officers do so. *Id.* at 63:5–13. Pichardo explained, "[t]ypically, passengers are very compliant, they are very giving, and they will provide passwords, so — in all my time in secondary, I have never seen that happen." *Id.*

Upon direct inquiry from the Court, Pichardo explained that, subject to approval from their supervisors, secondary inspection officers have discretion to decide whether to search a traveler's cell phone. *Id.* at 18:12–15. His own practice is to decide whether to search someone's cell phone "based off of the story that [the traveler] is giving me." *Id.* at 18:16–21. He continued:

THE WITNESS: If it's a noncitizen, it's basically to determine the admissibility into the United States. If it is a citizen of the country, typically, we need more than just, you know — it might be their travel history, it might be related to terrorism, it might be related to other different factors that — or laws that we enforce that may require some — us to check electronic devices.

THE COURT: And when you say "related to a citizen's travel history," what about a citizen's travel history would give you a reason to ask for their phone and their passcode?

THE WITNESS: If they're coming from source countries, so Europe and — anyone from Europe, and they're — they're traveling there often or they've been away from the United States for a certain amount of time, it kind of draws questions to why were they away, what information are they bringing back with them, what kind of baggage are they bringing back with them. Just things to clarify their reasons for them going abroad and coming back into the United States.

THE COURT: And what's a source country?

THE WITNESS: A source country is typically related to terrorism. So it can be Yemen, for — to give you an example, Syria. Just countries that have political difficulties at this point in time and that we're — we're currently looking at for intelligence and stuff like that.

Id. at 18:21–19:19. Pichardo also detailed the scope of the search that a secondary inspection officer at JFK can conduct on a traveler's cell phone:

THE COURT: [W]hat is your understanding about how much information on a phone you can look at during that manual search? What categories of information can you look at? How long can you spend on it? What's the general[] parameters, or does it depend on the case?

THE WITNESS: . . . What [we can] look at is we have to put the media device in airplane mode, so it doesn't acquire any more information, so it needs to be present at that point, so that's why we put it on airplane mode. Also, anything that's in the phone at that point, so if I click on something and it's present, then that's — that's subject to inspection —

THE COURT: Sorry, say that again. When you click on anything in the phone —

THE WITNESS: It's subject to inspection, so we could look at pretty much anything that's stored on the phone. We can't like gain access to something and put it on the phone.

THE COURT: I see. So . . . you can look at anything they have saved on their phone.

THE WITNESS: That's correct.

THE COURT: And that would include text messages, emails, photos, videos, files, that sort of thing?

THE WITNESS: Yes, that's correct.

Id. at 19:22–20:22. Pichardo elaborated on cross examination by defense counsel:

QUESTION: Now, you stated that you have — that you can look at anything that is stored on the phone; is that correct?

ANSWER: Yes, that is correct.

QUESTION: So, for example, if an individual has a private photo of his, or his family, you're allowed to look at these photos?

ANSWER: Anything that is on that phone on that given day, we can examine.

QUESTION: And that may include something like a banking app?

ANSWER: Yes. It's not limited to anything. Anything that's on that particular phone.

QUESTION: So, essentially, even if the person has a banking app, you may ask for [a] password for his banking app account?

ANSWER: Yes, we may.

QUESTION: Or any other app device?

ANSWER: Yes, that's fair.

QUESTION: And that may be done even if the person, for example, is being detained subject to a hit with respect to child pornography, you can look into other apps for other information; correct?

ANSWER: Yes, that's correct.

QUESTION: And when you're saying that, for example, that you can read SMS messages, you can read the private contents of the SMS messages?

ANSWER: That is correct.

Id. at 52:21–53:19.

When CBP elects to search a person's electronic device, it is CBP's practice to provide the traveler whose device is being searched with an "electronic media tear sheet, just to notify the traveler that an inspection of their [] device . . . is going to be conduct[ed]." *Id.* at 16:23–17:3. The tear sheet is "basically a flyer giving basic information of why they may be selected for an electronic media device search and how to give us a basis — give them a basis of the laws behind why we conduct electronic media device searches at the border." *Id.* at 17:7–10.

B. Sultanov's Interactions with CBP

On March 5, 2022, Sultanov, a United States citizen, arrived at JFK after visiting family in Uzbekistan. HSI Tr. 2:1–4, 12:239–45. According to Sultanov, he was questioned about his recent travel during primary inspection. *See* First Aff. in Supp. of Mot. ¶ 4, ECF No. 21-1. Sultanov told the CBP officer conducting the primary inspection that he had been in Uzbekistan, and the officer returned his passport. *Id.* ¶ 5. While Sultanov waited for his luggage at baggage claim, "two officers approached [him] and asked [him] to follow them." *Id.* ¶ 6. Sultanov was brought to the airport's secondary screening area, where Pichardo was stationed. Suppression Hr'g Tr. 22:23–23:14.

According to Pichardo, Sultanov arrived at the secondary inspection area at approximately 12:17 p.m. *Id.* at 27:7–10. Sultanov was not escorted in handcuffs, though Pichardo could not recall whether other travelers waiting in the secondary inspection area were in handcuffs. *Id.* at 59:3–7, 62:10–18. When Pichardo scanned Sultanov's passport roughly twenty minutes later, *id.* at 27:4–10, he learned that Sultanov's passport was tied to what he described as a "lookout" alert, indicating that Sultanov had "been identified as a possible purchaser/possessor of child sexual exploitation material," TECS R. 1, Gov't Ex. 1, and that an "electronic media search" of Sultanov's devices should be conducted, *id.*; Suppression Hr'g Tr. 23:20–24:2. After reviewing the "lookout" and ensuring through "system checks" that Sultanov "didn't have any other criminality," he sought and obtained permission from his supervisors to "conduct a[n] electronic media device" search. *Id.* at 26:11–18.

Pichardo then directed Sultanov to approach his desk. *Id.* at 26:24–25. Pichardo testified that first he asked Sultanov simple questions, like "how long were you away, what were you doing while you are [sic] away," and then he asked Sultanov to hand over his cell phone.[2] *Id.* at 27:1–3. Pichardo recalled that Sultanov "seemed a little confused of why I was asking for his cellular device." *Id.* at 27:13–14. Pichardo testified that he then directly asked Sultanov whether he had a cell phone and Sultanov produced his phone. *Id.* at 27:14–15.

Pichardo recalled that Sultanov's cell phone was passcode-protected and that he had to ask Sultanov for the passcode to his phone "like two times." *Id.* at 28:2–5. Pichardo could not remember whether Sultanov initially refused to turn over his phone's passcode, though he "may have." *Id.* at 48:11–21. When Sultanov asked Pichardo, one or two times, why he needed his cell phone and passcode, Pichardo responded, "I just need your passcode and I need you to have a seat." *Id.* at 50:13–18, 54:18–23, 66:6–15.[3] Pichardo testified that, while it is his understanding that a

[2] In his affidavit, Sultanov alleges that multiple officers asked him for his phone and passcode in the secondary inspection area. First Aff. in Supp. of Mot. ¶ 8. Sultanov also alleges that he was asked for his U.S. passport at the same time that he was asked for his phone and passcode. *Id.* It is unclear from the record whether CBP already had taken possession of Sultanov's Uzbek passport and Pichardo further requested Sultanov's U.S. passport when he asked for Sultanov's cell phone and passcode or whether Sultanov's memory is mistaken and CBP already had possession of both of his passports when Pichardo asked him for his cell phone and passcode. *See* Suppression Hr'g Tr. 44:10–13 (Pichardo testifying that as he recalls, he already had possession of Sultanov's passport when he asked Sultanov for his cell phone).

[3] Pichardo's testimony concerning his statements to Sultanov regarding the search of Sultanov's phone was at times inconsistent. Pichardo initially denied telling Sultanov that he needed to search his phone to complete an investigation.

citizen does have a right to refuse to turn over her cell phone or passcode without forfeiting her ability to enter the United States, he did not inform Sultanov of his right to do so. *Id.* at 46:6–48:1.

Although Sultanov seemed "confused" by and "a little weary [sic] of" Pichardo's request, *id.* at 29:1–4, and appeared not to understand why Pichardo was asking him for his passcode or his cell phone, Sultanov ultimately provided his cell phone to Pichardo for inspection, *id.* at 27:11–28:13. It is unclear whether Pichardo obtained the passcode from Sultanov or whether Sultanov entered the passcode and provided Pichardo with the cell phone unlocked. *Id.* at 28:6–9.

Either immediately after Sultanov unlocked his cell phone or immediately beforehand, Pichardo provided Sultanov with a "tear sheet": a pre-printed form that explains, in general terms, why the government may search travelers' phones. *Id.* at 49:9–12 (testifying that after he gave Sultanov the tear sheet, Sultanov looked at it and then provided his passcode); *id.* at 67:11–17 (testifying that he provided Sultanov with the tear sheet only after Sultanov provided the passcode). Secondary inspection officers provide this form to travelers as a matter of course when conducting a cell phone search, *id.* at 16:23–17:10, 29:16–22, 64:3–65:14, but the form does not advise travelers that they may refuse to surrender their cell phone or passcode, *id.* at 50:23–51:6; *see also* CBP Tear Sheet, Gov't Ex. 2. The form

---

Suppression Hr'g Tr. 49:19–22. On cross-examination, he agreed that he did tell Sultanov, "I need your password to perform a search," *id.* at 54:24–55:1, that he told Sultanov that he needed Sultanov's password "to conduct an exam," *id.* at 65:18–25, and that he told Sultanov once, but possibly twice, "I need your pass code to complete . . . the inspection," *id.* at 67:2–5.

provided to travelers at JFK is in English, and as far as Pichardo is aware, it is not available in any other languages. Suppression Hr'g Tr. 61:22–25. Pichardo could not recall whether Sultanov asked him any questions about the tear sheet. *Id.* at 30:19–21.

Sultanov's account of his interaction with Pichardo, as memorialized in an affidavit he submitted in support of his motion to suppress, differs in certain respects from Pichardo's testimony. Sultanov alleges that he "refused to provide the phone and the phone's password" to the officers in the secondary inspection area. First Aff. in Supp. of Mot. ¶ 9. Once he refused, he was provided with a computer printout that looked like a flyer (presumably the "tear sheet" Pichardo described). *Id.* at ¶ 10. Sultanov alleges that he could not understand the printout and asked for clarification. *Id.* at ¶ 11. In response, the CBP officers told Sultanov that the "printout states that [he has] to provide them [his] phone's password and the phone and [he doesn't] have a choice or right to refuse to provide it." *Id.*

Pichardo testified that after obtaining Sultanov's unlocked cell phone, he then proceeded to conduct an "examination" of the phone, Suppression Hr'g Tr. 30:22–23, otherwise known as a "manual search," *id.* at 19:24, 53:20–23. Before beginning the search, Pichardo placed Sultanov's cell phone on "airplane mode." *Id.* at 31:2. Although Pichardo explained that in this instance, his search was limited to examination of "different applications where any photos or videos" might be located on Sultanov's phone, *id.* at 31:2–6, as a general matter such searches are not

categorically limited, *id.* at 31:1–10. Instead, "anything derogatory that would have been on the phone could have been . . . searched as well." *Id.* 31:9–10.

After conducting a search that lasted approximately ten minutes, *id.* at 31:23–24, Pichardo found "approximately four videos" that were "suspect" regarding potential depictions of child pornography, *id.* at 32:3–5. These four videos included what appeared to be images of teenagers and young children engaging in sexual activity. *Id.* at 31:25–32:2.

After discussing the videos with his supervisors, Pichardo then contacted agents from CBP. *Id.* at 32:19–23. However, the CBP unit "denied interest in coming and seeing what [he had] discovered." *Id.* at 32:23–24. Pichardo then called "the HSI on duty agent," who informed Pichardo that he would "tak[e] interest in the case." *Id.* at 32:25–33:1.

Sultanov was required to remain in the secondary inspection area, awaiting the arrival of an HSI agent, for approximately three to four more hours. *Id.* at 52:5–9. During that time, Pichardo allowed Sultanov to call his family to inform them of his whereabouts, and Sultanov expressed that he was experiencing back pain but declined medical attention when offered. *Id.* at 33:2–33:13, 52:10–15. Pichardo also testified that, while he did not personally escort Sultanov to the restroom, Sultanov "probably" asked another officer to use the restroom, who, pursuant to the agency's policy, "had to be there with him using the restroom — watching him." *Id.* at 42:6–15. Pichardo recalled that Sultanov moved freely around the secondary inspection area and that the doors to the area were open. *Id.*

at 34:1–6. Although he could not remember specifically, Pichardo testified that Sultanov "probably asked [him] . . . why was it taking so long," and that Pichardo said, "there's someone that's going to come and speak to you, like an agent, another officer is going to come and talk to you." *Id.* at 34:7–12. Pichardo did not tell Sultanov the reason he was required to remain in the secondary inspection area: that he had found what appeared to be child pornography on Sultanov's cell phone. *Id.* at 33:14–16. Pichardo testified that his conversations with Sultanov were in English, that the two generally communicated easily in that language, and that, in other instances, he has enlisted the aid of a language service if a traveler is unable to communicate in English. *Id.* at 34:13–20, 51:11–52:4, 59:8–24.

Sultanov recalls the period of time he spent waiting for additional agents to arrive differently. In particular, Sultanov alleges that while he was waiting in the secondary inspection area, he asked whether he could leave and he was told he could not, that CBP officers reminded him that they had his cell phone and U.S. passport, and that the doors to the secondary inspection area were closed and locked from the inside. First Aff. in Supp. of Mot. ¶ 13. Additionally, Sultanov recalls that "[a]fter an hour or two the chief CBP officer" told him that CBP "had found child pornography on [his] phone and that someone else" would come speak to him. *Id.* at ¶ 14. Approximately one hour later, additional agents arrived to question him. *Id.* at ¶ 15.

C. Sultanov's Interactions with HSI

The Court then heard testimony from Special Agent Joshua Croft of the HSI Child Exploitation Investigation team. Suppression Hr'g Tr. 69:14–22, 70:22–25.

Croft testified that on March 5, 2022, he and his colleague, Special Agent Luanne Walter, were directed to JFK to investigate "a traveler who was coming into the country with child sexual abuse material on his phone." *Id.* at 71:18–72:4. Upon arrival, Agents Croft and Walter manually inspected Sultanov's phone for ten to fifteen minutes, *id.* at 114:4–7, and were able to unlock the phone using "the password that Officer Pichardo gave [them]," *id.* at 77:12–18. They looked in the "photo album app on the phone" and observed "several thumbnails that appeared to be videos of child sexual abuse," *id.* at 77:19–23, which they confirmed by watching the videos, *id.* at 78:10–79:4. These included one video that appeared to depict a four-year-old child engaged in sexual activity with an approximately fourteen-year-old female and an adult male, and two videos that depicted sexual activity by female subjects whose age Croft estimated to be approximately thirteen and fourteen years old. *Id.* at 78:10–79:4. In addition to these three videos, Croft also observed many pornographic videos exclusively depicting adults on Sultanov's phone. Sultanov's phone included "a pretty large pornography library which contained videos of adults," and Croft agreed that adult videos were "the majority" of those he observed on the phone. *Id.* at 116:1–9.

Sultanov was taken to an interview room, roughly eight feet by ten feet in size, located in the back of the secondary screening area. *Id.* at 79:8–16. Croft then proceeded to conduct an audio-recorded interview with Sultanov in English. *Id.* at 81:15–23; *see also* HSI Audio Recording dated Mar. 5, 2022, Gov't Ex. 4 (audio recording); HSI Tr. (transcript).

Sultanov informed Croft that he was comfortable speaking in English "as long as we spoke slowly." Suppression Hr'g Tr. 81:24–82:3, 106:16–20. For most of Croft's interview with Sultanov, the door to the interview room was closed and unlocked. *Id.* at 81:3–7. Croft testified that Sultanov "could have stopped the interview any time he wanted," but he was not free to leave the secondary inspection area and reenter the airport. *Id.* at 107:11–25.

At the commencement of the interview, Croft advised Sultanov of his *Miranda* rights. *Id.* at 83:19–84:25; *see also* Miranda Waiver, Gov't Ex. 3. Sultanov did not sign the *Miranda* waiver form that Croft handed him. Suppression Hr'g Tr. 88:25–89:7, 111:13–20. After Croft provided Sultanov with his verbal *Miranda* warnings and handed him the *Miranda* waiver form, the following exchange ensued:

CROFT:	So you understand all those, right?
SULTANOV:	50/50.
CROFT:	Well, let me explain anything. What . . .
SULTANOV:	So I do not understand, so I have a video. I'm not going to say like, oh use [unintelligible] or something else. I didn't know that it was illegal. So after that . . .
CROFT:	I'm going to close the door real quick, sorry.
SULTANOV:	So I tried to understand, what is happening right now? I'm trying to read this stuff. You say, I'm not gonna arrest, right?
CROFT:	Yeah.
SULTANOV:	So what is that, this one?

CROFT:	You don't have to sign that if you don't want to. That's just saying that you understand what I just read to you.
SULTANOV:	So right now, so whatever you guys find out, so what gonna happen to me. Do you understand what I'm saying?
CROFT:	Sure. So. Well, first of all tell us about this video and maybe nothing is wrong at all.
SULTANOV:	Okay, what kind of video, like do you —
CROFT:	Well, you just told me that there's a video that there was some concern over.
SULTANOV:	Yeah, but, I have a video. So if you turn on the phone, I can show you that. Another like, Roberto, like a supervisor told me this is illegal and I said, maybe, but I didn't know that. I do have one.

HSI Tr. 3:26–46.

At no point in the rest of this nearly hour-long interview did Croft return to the question of whether Sultanov understood his *Miranda* rights. Nor did he offer to provide further clarification of the *Miranda* warnings. Instead, Croft proceeded with further questioning regarding the videos that were on Sultanov's cell phone, during which time Sultanov gave Croft his passcode and allowed him to unlock and access his phone. *See id.* at 4:47–69.

Sultanov and Croft understood their exchange concerning whether Sultanov was under arrest differently. Croft explained that when Sultanov asked whether he was under arrest, even though Croft had probable cause to arrest Sultanov, Croft responded that "he was not under arrest," which, from his perspective, was true "at

the moment." Suppression Hr'g Tr. 82:20–25. It was Croft's practice not to arrest suspects in child pornography cases without first receiving permission from prosecutors, which he had not yet done in this case, because prosecutors previously instructed him not to arrest persons even after he found them to be in possession of child pornography. *Id.* at 82:22–83:2, 104:2–105:12, 115:19–25. Sultanov, however, understood Croft's response to his question about being under arrest to mean that he was not under arrest and would not be arrested, and he went on to make "statements . . . in reliance" on that representation. First Aff. in Supp. of Mot. ¶ 25.

At the suppression hearing, Croft was asked about the portion of his interview in which Sultanov asked, "so whatever you guys find out, so what gonna happen to me[?] Do you understand what I'm saying?", to which Croft responded, "[w]ell, first of all, tell us about this video and maybe nothing is wrong at all." HSI Tr. 3:38–41. Croft explained that he made that statement "[t]o get [Sultanov] to continue speaking to us[,] to elicit an answer from him." Suppression Hr'g Tr. 121:24–122:6. Croft further acknowledged that at the moment he told Sultanov that "maybe nothing is wrong," this was not true: Sultanov had just admitted to possessing child pornography on his phone, and Croft had personally viewed three such videos on Sultanov's device. *Id.* at 112:10–21. Thus, while Sultanov "[p]otentially" could have said something in the interview to convince Croft that he had not illegally possessed child pornography, *id.* at 113:1, such an outcome was "not very likely," *id.* at 112:4–9.

For the remainder of the interview, which lasted approximately fifty-five more minutes, Sultanov proceeded to answer, at times in considerable detail, all the questions posed by Agents Croft and Walter regarding his access to and knowledge of the videos on his phone. Sultanov told the agents that he had no interest in child pornography and was only interested in viewing videos of adult women, particularly "older" women. HSI Tr. 29:636–32:688.

Sultanov maintained that he had downloaded the videos containing children and adolescents unintentionally, stating that while he typically purchased pornographic videos from the internet one at a time, at one point he downloaded "80 or 100 videos" from a Russian application "for 50 bucks." *Id.* at 38:831–45, 37:802–10. He told Croft that the video depicting young children on his phone may have been part of that bulk purchase and noted that he thought the video was from Russia because "a Russian conversation" could be heard in the background. *Id.* at 38:831–45. He also told Croft that he "was going crazy" when he saw this video on his phone and that he had immediately attempted to delete it but apparently "forgot" that it was still on his phone. *Id.* at 38:844–45. Croft also asked Sultanov whether it is "okay to have a video" depicting a four-year-old child engaged in sexual activity, to which Sultanov responded, "What do you mean is it okay? Of course it's not okay." *Id.* at 45:982–1001. Regarding the video that appeared to contain pornographic images of adolescent girls, however, Sultanov acknowledged that he had not deleted it and had occasionally looked at it when he was "bored": "[S]ometimes I would watch it because when I was on my trip, when I, when I don't

have like job, when I sitting in the truck. I would watch it sometimes. I don't wanna lie you." *Id.* at 45:1003–46:1007.

When asked whether he was concerned that Sultanov did not understand his *Miranda* rights — including after Sultanov's "50/50" answer to the question of whether he understood the warnings he had just been given — Croft testified that Sultanov "kept talking, so I allowed him to keep talking." Suppression Hr'g Tr. 110:9–13. Croft explained that he "believe[d] that [Sultanov] understood" his right to remain silent "because he kept speaking to us." *Id.* at 117:7–10.

Croft testified that Sultanov comfortably communicated in English over the course of the hour-long interview, *id.* at 93:12–94:14, though he knew that Sultanov spoke with an accent, *id.* at 106:24–107:4.[4] At the end of the interview, Croft arrested Sultanov. *Id.* at 94:19–22. Croft explained that although "the majority" of persons in Sultanov's position are not arrested immediately, he concluded in consultation with the Assistant United States Attorney on duty that, because Sultanov has a daughter, it was "safer" to arrest him than to permit him to return home. *Id.* at 105:7–106:13.

After handcuffing Sultanov, Croft found a second cell phone in Sultanov's pocket that was powered down with a dead battery. *Id.* at 94:23–95:7. The HSI

[4] Through Croft, the government also introduced a record related to Sultanov's naturalization, which included statements from Sultanov about his proficiency in English at the time. Suppression Hr'g Tr. 96:20–97:14, 98:7–100:13. Sultanov objected to the introduction of this record on the grounds that it is hearsay. *Id.* at 96:11–13. However, because "[a]t a suppression hearing, the court may rely on hearsay and other evidence, even though that evidence would not be admissible at trial," *United States v. Raddatz*, 447 U.S. 667, 679 (1980), the Court overrules Sultanov's objection.

Agents confiscated both of Sultanov's phones, and Croft later signed an affidavit in support of a search warrant to conduct forensic searches of Sultanov's devices. *Id.* at 100:14–19; Appl. for Search Warrant.

D. The Warrant Application for Sultanov's Cell Phones

On March 17, 2022, Croft prepared a search warrant affidavit regarding both of the cell phones seized from Sultanov. *Id.*; Second Aff. in Supp. of Mot. ¶ 47, ECF No. 28. Croft's affidavit alleged that Sultanov "voluntarily gave CBP officers the password" for one of his cell phones and that CBP officers found child sexual abuse material on the phone. Appl. for Search Warrant ¶ 8. The affidavit further alleged that Sultanov agreed to waive his *Miranda* rights before admitting to HSI agents that he purchased the child sexual abuse materials that were discovered on his cell phone. *Id.* at ¶ 10. According to the search warrant affidavit, after Sultanov was arrested and the HSI agents found Sultanov's second cell phone, he told the agents that his second phone had the same password as his first phone. *Id.* at ¶ 11. The affidavit described CBP's search of Sultanov's cell phone at JFK but did not contain any reference to the TECS hit that prompted the initial search of Sultanov's phone. Suppression Hr'g Tr. 103:2–8. After Magistrate Judge Cho granted the search warrant application, Croft's colleague completed a forensic search of Sultanov's phone. *Id.* at 100:18–20.

III. Post-Hearing Arguments

At oral argument, defense counsel conceded that the TECS hit provided law enforcement with reasonable suspicion that Sultanov may have possessed child sexual abuse material on his phone; the defense argued, however, that the

government needed probable cause and a warrant before conducting a search of Sultanov's cell phone, even at the international border. Oral Arg. Tr. 44:9–23, 45:13–46:7. The defense further argued that Sultanov's statements to Pichardo, including the provision of his phone passcode, should be suppressed as the product of custodial interrogation conducted without *Miranda* warnings. *Id.* at 37:12–40:14. Additionally, the defense argued that Sultanov's statements to Croft should be suppressed even though Croft had administered *Miranda* warnings before questioning him, because Sultanov indicated that he only understood the *Miranda* warnings "50/50" and at no time did he make a valid, knowing waiver of his *Miranda* rights. *Id.* at 54:9–56:1.

The government argued (1) that Sultanov's statements to Pichardo should not be suppressed because he was not subjected to custodial interrogation in the secondary inspection area, and therefore Pichardo had no obligation to provide him with *Miranda* warnings before asking him for his passcode; (2) that the evidence from Sultanov's cell phone should not be suppressed because the search of Sultanov's phone was a routine border search "that did not require any amount of suspicion" and that in any case, the TECS hit provided reasonable suspicion to search Sultanov's phone, which, according to the government, exceeds what is required for such a search; and (3) that Sultanov's statements to the HSI agents should not be suppressed because he "never clearly and ambiguously invoked his rights" and impliedly "wa[i]ved his *Miranda* rights" when he continued speaking to

law enforcement after stating he understood the *Miranda* warnings "50/50." *Id.* at 4:7–21:6.

After hearing from the parties, the Court requested supplemental briefing concerning whether any courts have found the secondary inspection area to be a custodial setting, whether the search warrant would still be valid if the Court found that key information on which the search warrant relied to establish probable cause was itself illegally obtained, and whether the government would continue to argue that electronic devices can be searched at the border without any particularized suspicion. *See id.* at 65:13–66:15.

In its supplemental briefs, the government maintained that routine manual searches of cell phones at the border do not require any degree of individualized suspicion, and that here, CBP had reasonable suspicion to search Sultanov's phone. Gov't May 4, 2023 Letter at 2–5, ECF No. 27. With respect to the warrant, the government argued that Sultanov was not entitled to suppress any evidence obtained pursuant to the search warrant because the warrant affidavit provided ample information supporting probable cause even without consideration of the allegedly illegally obtained evidence from Sultanov's interactions with law enforcement at the airport. It also argued that even assuming some violation of Sultanov's rights at JFK had occurred, the Court may not suppress physical evidence derived from a *Miranda* violation or where, as here, the government may invoke the "good faith exception" to the warrant requirement. *Id.* at 6–9. In the defense's post-hearing submission, the defense maintained that the record

established that Pichardo subjected Sultanov to custodial interrogation in the secondary inspection area without advising him of his *Miranda* rights and therefore Sultanov's provision of his passcode (and all evidence obtained therefrom) should be suppressed. Second Aff. in Supp. of Mot. ¶¶ 3–36. The defense further argued that Sultanov's statements to the HSI agents and the results of the forensic search of his phone should all be suppressed because the good faith exception does not apply on the facts presented here. *Id.* at ¶¶ 37–65.

After the suppression hearing, several other courts issued opinions relating to the Fourth Amendment's application to cell phone searches at the border, which the parties brought to the Court's attention and addressed in supplemental briefings. *See* Gov't July 3, 2023 Letter, ECF No. 30; Def. Resp. in Supp. of Mot. to Suppress, ECF No. 33; Gov't Reply to Resp. to Mot. to Suppress, ECF No. 36; Gov't Dec. 18, 2023 Letter, ECF No. 42; Gov Jan. 11, 2024 Letter, ECF No. 43.

The Court also granted leave for the Knight First Amendment Institute at Columbia University and the Reporters Committee for Freedom of the Press to file an amici curiae brief on behalf of Sultanov. Amici Br., ECF No. 40. Amici argue, *inter alia*, that warrantless searches of electronic devices at the border are a profound and unreasonable intrusion on privacy interests protected by the Fourth Amendment and imperil freedom of the press under the First Amendment by chilling communications between reporters and their sources. Amici urge this Court to hold that probable cause and a warrant are required before the

government may search the contents of an international traveler's cell phone. *Id.* at 11–20.

DISCUSSION

On a motion to suppress in a criminal case, the defendant bears the burden of demonstrating the basis for the motion. *See United States v. Masterson*, 383 F.2d 610, 614 (2d Cir. 1967). Once the defendant meets his burden, the burden shifts to the government. Where the defendant's motion is premised on a Fourth Amendment violation, "the Government bears the burden of justifying an exception to the warrant requirement by a preponderance of the evidence." *United States v. Alisigwe*, No. 22-cr-425, 2023 WL 8275923, at *4 (S.D.N.Y. Nov. 30, 2023) (citing *United States v. Arboleda*, 633 F.2d 985, 989 (2d Cir. 1980)). Where the defendant alleges that he was questioned in violation of *Miranda v. Arizona* and the Fifth Amendment, "[t]he prosecution has the burden of establishing by a preponderance of the evidence that a suspect waived his *Miranda* rights, and that his confession is truly the product of free choice." *United States v. Anderson*, 929 F.2d 96, 99 (2d Cir. 1991).

I. Fourth Amendment

The Fourth Amendment to the Constitution protects "the right of the people to be secure . . . against unreasonable searches and seizures." U.S. Const. amend. IV. The Fourth Amendment "expressly imposes two requirements. First, all searches and seizures must be reasonable. Second, a warrant may not be issued

unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011).

Before law enforcement officers conduct a search for evidence of a crime, "reasonableness generally requires the obtaining of a judicial warrant," subject to several narrowly delineated exceptions. *Riley*, 573 U.S. at 382. This case implicates the so-called "border exception" to the warrant requirement, which has historically been applied to exempt government officials from the warrant requirement and allow them to conduct brief searches of travelers' persons and effects to prevent contraband from entering the country. The issue here is whether, in light of that exception, a compelled search of the contents of a traveler's cell phone or other handheld electronic device conducted without a warrant and without probable cause is reasonable under the Fourth Amendment if that search takes place at an international border.[5] If the Court answers that question in the negative, then the warrantless search of Sultanov's cell phone violated the Fourth Amendment, and the fruits of that search could be subject to suppression.

A. The Warrant Exception for Routine Border Searches

When assessing the reasonableness of a search, courts are guided by "balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). At the border, searches that would violate the

[5] An international airport, like JFK, "is considered the functional equivalent of a border" for Fourth Amendment purposes. *Alisigwe*, 2023 WL 8275923, at *3 n.5 (citation omitted).

Fourth Amendment if they were conducted within the country may be reasonable because the balance between the government's interests and the individual's privacy interests tips decidedly in the government's favor. That is because the government's "interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). And a traveler in an international airport seeking entry into the United States has a diminished expectation of privacy due in part to the surveillance and security measures that are endemic in air travel. *See Montoya de Hernandez*, 473 U.S. at 539–40 (citing *Florida v. Royer*, 460 U.S. 491, 515 (1983) (Blackmun, J., dissenting)).

The border search exception is based not only on the "balance between the interest of the Government and the privacy right of the individual," which is "struck much more favorably to the Government at the border," but also on the history and tradition of the government's customs enforcement power. *Id.* at 537, 540. The same Congress that proposed the Bill of Rights enacted the first customs statute that empowered customs officials to search incoming "ship[s] [and] vessel[s]" suspected of transporting "any goods, wares or merchandise subject to duty." *United States v. Ramsey*, 431 U.S. 606, 616 (1977).

Although such searches, if conducted domestically, would have required a warrant and probable cause to be reasonable under the Fourth Amendment, those warrantless searches by customs officials were reasonable "simply by virtue of the fact that they occur[red] at the border." *Id.*; *see also United States v. Thirty-Seven*

Photographs, 402 U.S. 363, 376 (1971) ("Customs officers characteristically inspect luggage and their power to do so is not questioned in this case; it is an old practice and is intimately associated with excluding illegal articles from the country."). The historic power of customs officials to conduct "routine inspections and searches" of goods at the border also extends to searches of people at the border based on the government's power "to exclude aliens from the country." *Almeida-Sanchez v. United States*, 413 U.S. 266, 272 (1973). Thus, for at least two centuries, the government's "inherent authority to protect" and "paramount interest in protecting[] its territorial integrity," *Flores-Montano*, 541 U.S. at 153, has led courts to uphold searches of people and property at the border that would under ordinary circumstances violate the Fourth Amendment. *See Montoya de Hernandez*, 472 U.S. at 554 (Brennan, J., dissenting) (emphasis in original) (distinguishing between searches at the border "*for purposes of immigration and customs control*" and searches "carried out *for purposes of investigating suspected criminal activity*").

B. Nonroutine Searches at the Border

"Nonetheless, the touchstone of the Fourth Amendment analysis remains reasonableness," and the border search exception "does not mean . . . that at the border 'anything goes.'" *Cotterman*, 709 F.3d at 960 (internal citation omitted). The Supreme Court has differentiated between routine border searches, like the search of a traveler's luggage, *see Thirty-Seven Photographs*, 402 U.S. at 376, and searches conducted at the border "for purposes other than a routine border search" that exceed the "scope of a routine customs search and inspection," *see Montoya de Hernandez*, 473 U.S. at 540. "[T]he level of intrusion into a person's privacy is what

determines whether a border search is routine" and thus whether the border search exception applies or not. *United States v. Irving*, 452 F.3d 110, 123 (2d Cir. 2006).

To determine whether a warrantless, nonroutine search is permissible under the Fourth Amendment, courts conduct the customary reasonableness balancing test, in which "the offensiveness of the intrusion must be weighed against the level of warranted suspicion." *Id.* For example, in *Montoya de Hernandez*, the Supreme Court held that a noncitizen traveler who presented herself for admission at the border and was suspected of "smuggling contraband in her alimentary canal" was lawfully detained by CBP for sixteen hours because CBP had reasonable suspicion that the traveler was attempting to smuggle drugs into the country, and because they detained her only "for the period of time necessary to either verify or dispel" the suspicion. 473 U.S. at 541–44. The Court considered the totality of the circumstances surrounding the traveler's detention and weighed the intrusiveness of the detention at issue against the government's "longstanding concern for the protection of the integrity of the border." *Id.* at 538. And the government's interest in taking reasonable measures to interdict the flow of illegal narcotics was, in the Court's view, entitled to great weight given what was, at that time, a "veritable national crisis in law enforcement caused by smuggling of illicit narcotics." *Id.*

Similarly, in *United States v. Asbury*, 586 F.2d 973 (2d Cir. 1978), the Second Circuit assessed the Fourth Amendment reasonableness of a strip search at the border of a traveler suspected of carrying contraband. The Court characterized the challenged strip search as a nonroutine search not governed by the border search

exception, reasoning that while "anyone entering or leaving the country may expect to have his luggage and personal effects examined, he does not expect that his entry or departure, standing alone, will cause him to be subjected to a strip search." *Id.* at 975. The Court then conducted the traditional Fourth Amendment reasonableness analysis in the specific (border-security) context presented. *Id.* at 976–77. It weighed the traveler's expectation of privacy against the government's heightened interest in preventing illegal narcotics from being smuggled across the border and ultimately upheld the search as supported by individualized suspicion and within the Fourth Amendment's bounds of reasonableness. *Id.*; *see also Irving*, 452 F.3d at 123 (citing *Asbury*, 586 F.2d at 975–76, for proposition that while "routine border searches of a person's belongings," including searches of "outer clothing, luggage, a purse, wallet, pockets, or shoes," "are made reasonable by that person's decision to enter this country, more invasive searches, like strip searches" that "substantially infringe on a traveler's privacy rights," "require reasonable suspicion").

To date, however, neither the Supreme Court nor the Second Circuit has yet addressed (1) whether a search of a traveler's cell phone or other handheld electronic device at the border is a routine search covered by the border search exception, or (2) if it is a nonroutine search, the level of suspicion required for the search to be reasonable under the Fourth Amendment (i.e., whether it may be conducted at the point of entry by border officials based on a mere showing of reasonable suspicion or whether it requires a warrant and probable cause).

C. *Riley v. California*

i. *Riley v. California* and the Search Incident to Arrest Exception to the Fourth Amendment Warrant Requirement

This Court turns principally for guidance to *Riley*, 573 U.S. at 385, in which the Supreme Court addressed how another historic exception to the Fourth Amendment's search warrant requirement — the search incident to arrest exception — applies to modern cell phones. In *Riley*, the Court discussed at great length the substantial intrusion on an individual's privacy that may result when the government is permitted to search the vast and often intimate contents of a person's cell phone. *Id.* at 393–97. The Court held that the intrusion was substantial enough to require a warrant and probable cause before conducting such a search — even where, as in *Riley*, law enforcement already had probable cause to arrest the phone's owner for one or more crimes. *Id.* at 403 (holding that a warrant is required to search a cell phone that is seized incident to arrest).

Like the border search exception, it has long been understood that the government has the right "to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime." *Weeks v. United States*, 232 U.S. 383, 392 (1914). Under this exception, courts generally construe a search of an arrestee's person and the area within the arrestee's immediate control ("the area from within which he might gain possession of a weapon or destructible evidence") to be reasonable under the Fourth Amendment, even though such searches are conducted without a warrant. *Riley*, 573 U.S. at 383 (quoting *Chimel v. California*, 395 U.S. 752, 762–63 (1969)). The intrusion on the arrestee's privacy is warranted

based on concerns for the arresting officer's safety and the preservation of evidence. *Id.* Thus, the Supreme Court has long categorically permitted searches incident to arrest: a "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." *Id.* at 384 (quoting *United States v. Robinson*, 414 U.S. 218, 235 (1973)). Indeed, the search of a person's pockets is merely a "minor additional intrusion[] compared to the substantial government authority exercised in taking [the suspect] into custody." *Id.* at 392.

Before the Court's decision in *Riley*, it was widely presumed that a police officer could similarly search an arrestee's phone incident to arrest. But in *Riley*, the Court found that while the Court's "categorical rule" that searches incident to arrest are lawful "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones." *Id.* at 386. Once an officer has gained control of an arrestee's cell phone, searching the content of the phone neither furthers officer safety nor prevents the destruction of evidence. *Id.* at 387–91. The Court's decision turned not only on the fact that searching an arrestee's cell phone does not promote the legitimate governmental interests that animate the search incident to arrest exception, but also on the Court's assessment of the unique privacy concerns implicated by searching cell phones. *Id.*

ii. *Riley v. California* and the Privacy Interests Implicated in Cell Phone Searches

The *Riley* Court concluded that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects" that might be searched by law enforcement. *Id.* at 393. In response to the government's claim that searching digital data on a smart phone is "materially indistinguishable" from searching physical items a person ordinarily has on their person, like a wallet, the Court stated: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Id.* The Court opined that cell phones are categorically different from other physical property because modern cell phones are essentially "minicomputers" with "immense storage capacity"[6] that "could just as easily be called "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Id.* Explaining the key differences between the privacy intrusion caused by searching an arrestee's cell phone as opposed to his person or physical property, the Court observed:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information — an address, a note, a prescription, a bank statement, a video — that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions;

[6] At the time *Riley* was decided, the "top-selling smart phone ha[d] a standard capacity of 16 gigabytes" and was "available with up to 64 gigabytes." *Riley*, 573 U.S. at 394.

> the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id. at 394–95.

Although the government in *Riley* argued that government agencies could "develop protocols" to limit the privacy intrusions attendant to cell phone searches by ensuring that such searches implicate only data "stored locally on the device" as opposed to data "pulled from the cloud," the Court rejected this argument. *Id.* at 397–98. As the Court bluntly stated: "the Founders did not fight a revolution to gain the right to government agency protocols." *Id.* at 398. Moreover, "[t]he possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests" in cell phones "dwarf those in" other physical property carried by arrestees. *Id.*

In holding that a "warrant is generally required before" "information on a cell phone" can be searched, "even when a cell phone is seized incident to arrest," the Court understood that its decision would limit law enforcement's ability to "combat crime." *Id.* at 401. But "[p]rivacy comes at a cost." *Id.* That cost can be mitigated by advances in technology that make it increasingly easy for law enforcement to quickly obtain a warrant. *Id.* Further, the Court noted that exigent circumstances may "still justify a warrantless search of a particular phone." *Id.* at 402.

The Second Circuit has similarly recognized the extraordinary privacy concerns implicated by searches of electronic devices. "The upshot is that the

search and seizure of personal electronic devices like a modern cell phone or tablet computer implicates different privacy and possessory concerns than the search and seizure of a person's ordinary personal effects." *United States v. Smith*, 967 F.3d 198, 208 (2d Cir. 2020). In *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016), the Court noted that searching a person's electronic device can give the government access to "a vast trove of personal information about the person to whom the [device] belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." The *Ganias* Court went on to explain what that "vast trove of personal information" constitutes in practical terms and how exponentially the storage capacities of such devices have grown in recent years:

> In 2005, Professor Orin Kerr noted that the typical personal computer hard drive had a storage capacity of about eighty gigabytes, which he estimated could hold text files equivalent to the information contained in the books on one floor of a typical academic library. By 2011, computers were being sold with one terabyte of capacity — about twelve times the size of Professor Kerr's library floor. The *New York Times* recently reported that commercially available storage devices can hold 16 petabytes of data, roughly equal to 16 billion thick books.

Id. at 217–18 (internal quotation marks and citations omitted).

And in its Fourth Amendment analysis, the Second Circuit has emphasized not only the sheer volume of information stored on modern electronic devices but the nature of that material:

> [Q]uantitative measures fail to capture the significance of the data kept by many individuals on their computers. Tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, banking and shopping information — all may be kept in the same device, interspersed among the evidentiary material that justifies the seizure or search . . . . While physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material, the

> reasonableness of seizure and subsequent retention by the government of such vast quantities of irrelevant private material was rarely if ever presented in cases prior to the age of digital storage, and has never before been considered justified, or even practicable, in such cases. Even as we recognize that search and seizure of digital media is, in some ways, distinct from what has come before, we must remain mindful of the privacy interests that necessarily inform our analysis.

Id. (citations omitted).

D. The Applicability of the Border Search Exception to Cell Phone Searches

Guided by the Supreme Court's decision in *Riley*, this Court concludes that the search of a cell phone at the border is a nonroutine search for Fourth Amendment purposes. As in *Riley*, this conclusion is based on the Court's examination of the history and purpose of the specific exception to the Fourth Amendment's warrant requirement cited by the government (here, the border search exception) weighed against the strength of a traveler's privacy interest in the "vast trove of personal information," *Ganias*, 824 F.3d at 217, stored in her cell phone.

i. The History and Purpose of the Border Search Exception Do Not Support its Application to Searches of Cell Phones

The *Riley* Court made clear that courts should not reflexively apply exceptions to the warrant requirement and should instead decide "whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Riley*, 573 U.S. at 374 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300

(1999)). As the Court concluded in the context of the search incident to arrest exception, while the border search exception "strikes the appropriate balance in the context of physical objects," none of "its rationales ha[ve] much force with respect to digital content on cell phones." *Id.* at 386.

The border search exception derives from the government's legitimate interest in protecting the integrity of the border by preventing "illegal articles" (including goods subject to duty) and inadmissible foreign citizens from entering the country. *Ramsey*, 431 U.S. at 616–19 (citation omitted); *see also Thirty-Seven Photographs*, 402 U.S. at 376 (explaining that customs officials are empowered to inspect luggage to "exclud[e] illegal articles" from the country); *Almeida-Sanchez*, 413 U.S. at 272 (noting customs officials conduct routine inspections at the border to "exclude aliens from the country"). While those interests are undoubtedly served when the government searches the luggage or pockets of a person crossing the border carrying objects that can only be introduced to this country by being physically moved across its borders, the extent to which those interests are served when the government searches data stored on a person's cell phone is far less clear. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 544 (remarking that customs and immigration officials at the border are charged "with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives"). Searching and seizing the data on a person's phone does not prevent that data, which the cell phone holder all but

certainly obtained and/or stores outside the device, from entering and circulating within the country. That is because the data

> very likely does exist not just on the phone device itself, but also on faraway computer servers potentially located within the country. And, wherever the servers are located, the owner of a cell phone can generally access or share part or all of the data on it with anyone else in the world so long as both parties have an internet connection. Stopping the cell phone from entering the country would not, in other words, mean stopping the data contained on it from entering the country.

United States v. Smith, 673 F. Supp. 3d 381, 394 (S.D.N.Y. 2023) (holding that the search of a cell phone at the border requires a warrant). The very notion of geographic boundaries has little meaning in the context of electronic data.

Here, the TECS alert flagged Sultanov because he had "been identified as a possible purchaser/possessor of child sexual exploitation material." TECS R. at 1. Sultanov told Agents Croft and Walter that while residing in the United States, he had unwittingly downloaded that child exploitation material as part of a bulk purchase of pornographic videos from a Russian website or application. HSI Tr. 35:774–36:799. Clearly, then, interdicting Sultanov's phone did not prevent any child sexual abuse videos stored on his phone from entering the United States. Such videos exist and could be accessed by untold numbers of other purchasers inside (and outside) the United States, independent of the government's seizure of Sultanov's device. Consequently, "the Government's interest in interdicting such 'digital contraband' as it exists on a specific device — when the exact same digital contraband likely is already stored outside the device and available to its owner and

others within this country" — is not "comparable to the Government's interest in interdicting physical contraband." *Smith*, 673 F. Supp. 3d at 395.

The government also argues that the search of Sultanov's phone was reasonable under the Fourth Amendment because, when conducting the search, Pichardo "plac[ed] the device on airplane mode so that the phone [was] not able to access the internet or the cloud." Oral Arg. Tr. 14:15–16. This is essentially the same argument the government advanced without success in *Riley*: the intrusiveness of cell phone searches incident to arrest could be limited by agency protocols that would require law enforcement officers to search only data "stored locally on the device" as opposed to data "pulled from the cloud." 573 U.S. at 397. But "the Founders did not fight a revolution to gain the right to government agency protocols," and there is a substantial risk that such a search "might extend well beyond" the locally stored data on a traveler's cell phone once the government begins an unlimited search of its contents. *Id.* at 398. Indeed, even a well-intentioned government agent attempting only to review data stored locally on a phone by setting it to airplane mode will likely uncover data stored in the cloud that is temporarily cached on the device itself, an event that increasingly occurs automatically and unbeknownst to the phone's owner.[7]

[7] *See* Lee Bell, *What Is Caching and How Does it Work?*, Wired UK (May 7, 2017), https://www.wired.co.uk/article/caching-cached-data-explained-delete (noting that many web-based sites and applications automatically save data that exists to a local device temporarily to enable the device to access the website or application more efficiently in the future without the user's knowledge) [https://perma.cc/537L-EYHA].

ii. The Strength of a Traveler's Privacy Interest Weighs Against Applying the Border Search Exception to Cell Phone Searches

Whereas searching cell phone data does little to promote the specific governmental interests that the border search exception was designed to protect, such searches, whether conducted manually or forensically, represent an extraordinary invasion of a traveler's privacy. Until technology that can "translate people's brain activity — like the unspoken thoughts swirling through our minds — into actual speech" meaningfully advances,[8] reviewing the information in a person's cell phone is the best approximation government officials have for mindreading. A person's search history can reveal the questions that keep him up at night, including questions he might be too ashamed to ask his spouse or doctor. Data on a person's cell phone may reflect information about her that is so private, she would not disclose it to her therapist or closest friend. It is not just that cell phones often contain intimate information available in microscopic detail — the number of steps the phone's user took that day and where she took them, the results of recent blood work in the application where her doctor uploads all her medical records, or the calendar reminder for a meeting with her local Alcoholics Anonymous chapter or prayer group. It is that the details, taken together, can provide a kaleidoscopic view of the user's whole life.

---

[8] *See* Sigal Samuel, *Mind-Reading Technology Has Arrived; An AI-Powered "Brain Decoder" Can Now Read Your Thoughts with Surprising Accuracy*, Vox (May 4, 2023), https://www.vox.com/future-perfect/2023/5/4/23708162/neurotechnology-mind-reading-brain-neuralink-brain-computer-interface [https://perma.cc/ZF9X-ZTMN].

In *Carpenter v. United States*, 585 U.S. 296, 311–12 (2018), the Court concluded that cell-site location data, even though it is collected by (and thus not kept private from) third party cell phone companies, requires Fourth Amendment protection for precisely this reason. In earlier decisions, the Court had previously held — in the context of governmental searches of telephone numbers and bank records — that individuals have a reduced expectation of privacy in information they had already provided to third parties. *Id.* at 308–09. But in *Carpenter*, it refused to apply the third-party doctrine "to the qualitatively different category of cell-site records" because of the unique privacy concerns implicated by cell-site data. *Id.* at 310. It reasoned that cell-site location data "provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 311 (citation omitted). In other words, the Court noted, "these location records hold for many Americans the 'privacies of life.'" *Id.* (cleaned up).

The logic of *Carpenter* applies with even greater force to the information contained on cell phones, which includes not only the historic and specific location information captured by cell-site data, but droves of other sensitive information that is "detailed, encyclopedic, and effortlessly compiled." *Id.* at 297. If the cell-site location records at issue in *Carpenter* hold "the privacies of life," *id.* at 305 (citation omitted), then surely the heightened privacy interests associated with the far

greater trove of information in a traveler's cell phone data strike at the very heart of the Fourth Amendment.

The government takes the remarkable position here that cell phones should not be treated *any* differently for Fourth Amendment purposes than any other property a traveler carries across a border. Opp'n Br. It urges this Court to deem such searches "routine" and to hold that no individualized suspicion whatsoever is needed for border officials to search a traveler's cell phone upon entry into the United States. Gov't May 4, 2023 Letter 2. In essence, the government argues that no practical limits should be placed on cell phone searches at the border whatsoever, as long as they fall into what agents categorize as a "manual" search (i.e., one unaided by extrinsic technology but limited only by the border agents' time and interest in examining the phone's contents). *Id.* at 3–4. However, "the level of intrusion into a person's privacy is what determines whether a border search is routine." *Irving*, 452 F.3d at 123. And the government's position fails to account for both the substantial privacy intrusions at issue here, as well as the Supreme Court's Fourth Amendment jurisprudence concerning other advanced technologies that carry with them the potential to reveal vast amounts of the owner's personal data.

When the Supreme Court has been confronted with new technology that enhances the government's ability to effortlessly surveil its citizens, it has carefully considered how the Fourth Amendment, and any recognized exceptions to the warrant requirement, should apply to that technology. *See Kyllo v. United States*,

533 U.S. 27, 29, 40 (2001) (holding law enforcement's use of new thermal-imaging technology to "detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment"); *Carpenter*, 585 U.S. at 318 (citing *Riley*, 573 U.S. at 386) ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."). Indeed, the Court has gone to great lengths to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *United States v. Jones*, 565 U.S. 400, 406 (2012) (alteration in original) (quoting *Kyllo*, 533 U.S. at 34), with "particular concern for government trespass upon the areas" enumerated in the Fourth Amendment, *id.*, including one's "papers" and "effects," *id.* (quoting U.S. Const. amend. IV). Given the extraordinary intrusion into a person's privacy posed by a cell phone search, this Court has no difficulty concluding that a manual search of a cell phone at the border is a nonroutine search to which a categorical border search exception does not apply.

iii. "Manual" and "Forensic" Searches Merit the Same Treatment Under the Fourth Amendment

Many courts have found the distinction between manual and forensic searches of electronic devices to have constitutional significance. This Court concludes, however, that the privacy intrusion of a manual search is substantially the same, for Fourth Amendment purposes, as the privacy intrusion of a forensic search, at least as those searches are conducted by CBP at the border. Each

involves such a vast intrusion on a traveler's privacy that, under the Fourth Amendment, both must generally be supported by a warrant.[9]

According to CBP's directives, a forensic or advanced search involves "connect[ing] external equipment . . . to an electronic device not merely to gain access . . . but to review, copy, and/or analyze its contents." U.S. CUSTOMS & BORDER PROTECTION, CBP DIRECTIVE NO. 3340-049A (Jan. 4, 2018), https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf [https://perma.cc/2EA3-NEFR]. A manual or basic search is any search that is not a forensic search — that is, any search conducted without the aid of external equipment. *Id.* A quintessential manual search involves "using the [device]'s touch screen . . . to scroll through" the device, whereas a forensic search involves connecting a cell phone to a device like "a Cellebrite Physical Analyzer, which extracts data from electronic devices," *United States v. Kolsuz*, 890 F.3d 133, 139 (4th Cir. 2018), and may take longer and provide more detailed information. A forensic search may, in theory, provide the government with more information than can be obtained through a manual search, like deleted files, and may make it easier for the government to authenticate the information it obtains and present it as

[9] In the border search context, as in *Riley*, notwithstanding the presumptive application of the Fourth Amendment's warrant requirement, "other case-specific exceptions may still justify a warrantless search of a particular phone." *Riley*, 573 U.S. at 401–02. For example, the exigent circumstances exception — which recognizes situations in which the "exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment," *id.* at 502 (alteration in original) (quotation marks omitted) — would remain available to law enforcement officials at the border.

evidence at trial. However, the essentially boundless manual searches conducted by CBP are not meaningfully different from their forensic counterparts in terms of the intrusion they impose on a traveler's privacy.

The record in this case illustrates why the manual-vs.-forensic distinction is not a meaningful one for Fourth Amendment purposes. Although law enforcement only spent approximately twenty-five minutes manually searching Sultanov's phone and apparently confined themselves to applications on his phone likely to contain pictures and videos, Pichardo testified that CBP does not require searches to be so circumscribed. *See* Suppression Hr'g Tr. 19:22–20:22. Other than putting the device on airplane mode, there is, as far as Pichardo knows, no meaningful limit on a manual search that any CBP officer may conduct at JFK. *Id.* A manual search could be conducted by any number of officers, for any amount of time, and include a review of any type of content on the phone, including content that is password protected or encrypted. *Id.* In a manual search, CBP can review "anything that's stored on the phone" at the time of the search. *Id.* at 20:13.

Once a CBP officer begins a manual search of an electronic device, the scope of the search is untethered from and unlimited by the original purpose of the search. *Id.* at 52:21–53:19. A manual search can extend to logging into applications that are stored on the phone and reviewing the encrypted data saved in those applications, like, for example, financial transactions in a banking application. *Id.* at. 53:6–10. CBP can review not only the traveler's personal emails and text messages, but highly confidential documents that may be attached to those

communications. In contexts that are familiar to readers of judicial opinions like this one, such confidential documents might include, for example, a draft divorce agreement prepared by a matrimonial lawyer that details the finances and child custody arrangements of her client and his spouse; sealed psychiatric records for a complaining witness or defendant in a criminal case; or a near-final draft of the terms of a multi-million-dollar corporate merger that is not yet public.

The only practical limitation on a manual search is a CBP officer's interest and zeal, and its potential scope is, in a word, breathtaking. That such searches are triggered by CBP's own highly discretionary and amorphous criteria, like a citizen's travel history — which currently includes, among other categories, "anyone from Europe," someone who has been "traveling here often," or a U.S. resident who has "been away from the United States for a certain amount of time," *id.* at 18:21–19:9 — gives the Court even greater pause about exempting them from the Fourth Amendment's historic safeguards.

It is true that manual and forensic searches differ in that the latter entails the use of one or more additional devices to review, trace, and analyze the contents of a cell phone, whereas the former is conducted without the aid of additional technology. But *Riley* did not turn on the method used to search a cell phone's contents and, in fact, held that the exact same manual cell phone searches at issue here were not exempted from the warrant requirement. 573 U.S. at 386. There, the police officer seized the defendant's phone immediately after his arrest and conducted a manual review that included accessing text messages and/or a contacts

list, and pictures and videos on the phone, among other things. *Id.* at 378–79. In analyzing the Fourth Amendment implications of the search, the Supreme Court invoked Judge Learned Hand's observation in 1926 that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." *Id.* at 396 (quoting *United States v. Kirschenblatt*, 16 F.2d 202, 203 (2d Cir. 1926)). The *Riley* Court observed: "If [the man's] pockets contain a cell phone, however, that is no longer true." *Id.* And because a "cell phone search" — manual or otherwise — "would typically expose to the government far *more* than the most exhaustive search of a house," *id.* (emphasis in original), the Court held that it violates the Fourth Amendment when conducted without a warrant, *id.* at 401. Notably, the Supreme Court reached that conclusion in *Riley* even though law enforcement in that case already had probable cause to conclude that the cell phone's owner had committed a crime and to place him under arrest. *Id.* at 378.

This Court recognizes that to date, none of the Courts of Appeals to consider this rapidly evolving area of law has held that a manual search of a cell phone at the border is a nonroutine search. Some of these courts have held that all cell phone searches at the border — whether forensic or manual — are routine. *See United States v. Touset*, 890 F.3d 1227, 1233–35 (11th Cir. 2018) (treating forensic searches of electronic devices as indistinguishable from searches of any other form of property at the border and characterizing all such searches as routine). Others have distinguished between forensic and manual searches. For example, the Ninth

Circuit concluded that, while manual searches of cell phones at the border are routine and can be conducted "without individualized suspicion, . . . the forensic examination of a cell phone requires a showing of reasonable suspicion of digital contraband" and is thus nonroutine. *United States v. Cano*, 934 F.3d 1002, 1016 (9th Cir. 2019) (internal citation omitted). The Fourth Circuit similarly characterized forensic searches as nonroutine but has not decided whether manual searches should be treated the same way. *See Kolsuz*, 890 F.3d at 144 (noting "in light of . . . *Riley*, a forensic border search of a phone must be treated as nonroutine" but not addressing whether a manual search of a phone is nonroutine); *see also Alasaad v. Mayorkas*, 988 F.3d 8, 19 (1st Cir. 2021) (holding that "basic border searches [of electronic devices] are routine searches" but not reaching the question of whether forensic searches require reasonable suspicion).

This Court respectfully concludes otherwise. Particularly in light of the record before this Court regarding the vast potential scope of a so-called "manual" search, the distinction between manual and forensic searches is too flimsy a hook on which to hang a categorical exemption to the Fourth Amendment's warrant requirement. And it is one that may collapse altogether as technology evolves. *See Kyllo*, 533 U.S. at 36 (noting, in case considering constitutionality of a warrantless search of home using thermal imaging technology, "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

Furthermore, many of the district courts in this Circuit to address the issue post-*Riley* have concluded that both manual and forensic searches of cell phones are nonroutine. *See, e.g.*, *Smith*, 673 F. Supp. 3d. at 395–96 (holding that a search of a cell phone at the border requires probable cause and a warrant); *United States v. Gavino*, No. 22-cr-136, 2024 WL 85072, at *4 (E.D.N.Y. Jan. 7, 2024) ("*Riley*'s discussion of privacy interests establishes that [both manual and forensic] searches of cell phones should be treated as intrusive border searches, rather than standard ones."); *Alisigwe*, 2023 WL 8275923, at *5 (holding that "cellphone searches cannot be conducted without reasonable suspicion of criminal activity because they are not routine border searches").[10] This Court joins those courts in holding that a search of a cell phone at the border, even a manual search, is nonroutine and thus falls outside of the border search exception.

iv. Probable Cause and a Warrant Are Required for the Search of a Cell Phone at the Border Under the Fourth Amendment

Having determined that the search of a cell phone at the border is a nonroutine search that falls outside of the border search exception, the Court now turns to the requisite degree of suspicion necessary for such a search to be

[10] The Court notes two district court cases which might be read to depart from the approach taken by the others in this Circuit to date. In *United States v. Tineo*, No. 23-cr-223, 2024 WL 2862289, at *6 (E.D.N.Y. June 6, 2024), the court declined to extend *Riley* to the border search context. But the court left open the question of whether reasonable suspicion was required for a cell phone search (and, while the court did not use this language, whether such a search was routine) because it found that the CBP agents acted with reasonable suspicion. *Id.* at *7. Additionally, in *Abidor v. Johnson*, No. 10-cv-4059, 2016 WL 3102017, at *6 n.* (E.D.N.Y. June 2, 2016), which concerned a motion to keep documents under seal, the court expressed in a footnote its view that *Riley* would not likely apply in the context of a border search.

reasonable under the Fourth Amendment. As the Court underscored in *Riley*, in the absence of an applicable exception to the warrant requirement, "a warrant is generally required before" the government may search the contents of an individual's cell phone, even when seized from a person whom the police had probable cause to arrest for a crime. 573 U.S. at 401.

The government argues that the Supreme Court's strict application of the warrant requirement in *Riley* does not apply to border searches because *Riley* concerned the search incident to arrest exception to the Fourth Amendment and not the border search exception. Gov't May 4, 2023 Letter 2–3. While technically correct, that argument fails to account for *Riley*'s substantial overlap with the issue presented here. *Riley* set forth how courts should approach the question of whether an exception to the warrant requirement applies to a category of property that raises extraordinary privacy interests: the vast trove of electronic data on modern cell phones. 573 U.S. at 386. Both the search incident to arrest exception and the border search exception are "longstanding, historically recognized exception[s] to the Fourth Amendment's general principle that a warrant be obtained." *Ramsey*, 431 U.S. at 621. This Court sees no reason that the Supreme Court's reasoning in *Riley* should apply with any less force to the border search exception than it does to the search incident to arrest exception, even after accounting for the government's distinct and legitimate interest in preventing the flow of contraband across its borders. *See Smith*, 673 F. Supp. 3d at 396 ("In holding that warrants are required for cell phone searches at the border, the Court believes it is applying in

straightforward fashion the logic and analysis of *Riley* to the border context."). Given the extraordinary privacy intrusion imposed by phone searches, whether at the border or incident to arrest, and the limited extent to which they actually further the government's interest in border security, a search of a cell phone at the border generally requires probable cause and a warrant to be reasonable under the Fourth Amendment.

It is true that even the two Circuit Courts to date (the Fourth and the Ninth) that have required some degree of individualized suspicion to authorize a search of a cell phone at the border did not go this far. The Fourth Circuit requires a warrant for border searches of cell phones only "where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests." *Kolsuz*, 890 F.3d at 143 (upholding a warrantless search of a phone at the border where there was a sufficient "link between the search of [the defendant's] phone and the interest that justifies border searches"). The Ninth Circuit limits forensic searches of phones at the border by requiring that officials "reasonably suspect that the cell phone contains digital contraband," as opposed to general evidence of a crime. *Cano*, 934 F.3d at 1007. And thus far, several district courts within the Second Circuit have found, post-*Riley*, that no warrant is required for cell phone searches at the border, provided that the agents who conduct the search have reasonable suspicion of criminal activity. *See Alisigwe*, 2023 WL 8275923, at *5; *Gavino*, 2024 WL 85072, at *5; *United States v. Bongiovanni*, No. 19-cr-227,

2022 WL 17481884, at *9 (W.D.N.Y. Aug. 5, 2022). *But see Smith*, 673 F. Supp. 3d at 398–99.

However, this Court is not bound by those decisions and respectfully disagrees with their conclusion that even after *Riley*, the border search exception permits the warrantless search of travelers' electronic devices, whether for "digital contraband" or evidence of a crime. *See United States v. Vergara*, 884 F.3d 1309, 1317 (11th Cir. 2018) (Pryor, J., dissenting) ("[C]ell phones do not contain the physical contraband that border searches traditionally have prevented from crossing the border . . . . And cell phone searches are ill suited to prevent the type of contraband that may be present on a cell phone from entering into the United States. Unlike physical contraband, electronic contraband is borderless and can be accessed and viewed in the United States without ever having crossed a physical border."). In this Court's view, categorically exempting border officials from the Fourth Amendment's warrant requirement fails to adequately protect individuals' reasonable expectation of privacy in the breathtakingly large trove of personal data stored on their cell phones.

Permitting the government to search any entering traveler's cell phone on a mere showing of reasonable suspicion, and without any showing of exigency, does not satisfy the ultimate test of reasonableness under the Fourth Amendment. The reasonable suspicion standard announced in *Terry v. Ohio* nearly six decades ago was designed to give law enforcement the tools needed to protect themselves and the public during brief, rapidly evolving street encounters — "necessarily swift

action predicated upon the on-the-spot observations of the officer on the beat — which historically has not been, and as a practical matter could not be, subjected to the warrant procedure." 392 U.S. 1, 20 (1968) (holding that the Fourth Amendment permits police to briefly detain and search an individual without a warrant during street encounters if they have reasonable suspicion that the person may be armed and dangerous). However, the reasonable suspicion standard is "applicable only to those brief detentions which fall short of being full-scale searches and seizures *and which are necessitated by law enforcement exigencies* such as the need to stop ongoing crimes, to prevent imminent crimes, and to protect law enforcement officers in highly charged situations." *United States v. Sokolow*, 490 U.S. 1, 12 (1989) (Brennan, J., dissenting) (emphasis supplied).

Although the "limited exception" created in *Terry* permitting searches and seizures based on reasonable suspicion rather than probable cause has been extended beyond so-called stop-and-frisk encounters, it remains the exception, not the rule. *See Royer*, 460 U.S. at 498. It has been extended to other "brief investigative stops," like traffic stops, where a minimal intrusion on a person's freedom and privacy is balanced against a law enforcement officer's "particularized and objective basis for suspecting the particular person stopped of criminal activity." *Navarette v. California*, 572 U.S. 393, 396 (2014) (citation omitted). But applying the reasonable suspicion standard to permit government officials to conduct essentially boundless examinations of devices containing a traveler's most private records, communications, and personal histories would broaden its

application far beyond its intended or appropriate scope. For even though the government has characterized non-forensic cell phone examinations as "manual searches," in practical terms, there is simply no equivalent of a street officer's "pat-down frisk" of a suspect's person when it comes to the contents of a traveler's cell phone.

The wide range of circumstances in which the reasonable suspicion standard has applied to law enforcement's detention of air travelers also disfavors its extension to the cell phone data context. In *Sokolow*, Justice Brennan famously detailed the innocuous and inconsistent factors that various courts had relied upon to uphold law enforcement's claims that they had reasonable suspicion to detain suspected drug couriers at airports: the suspect was first to deplane, last to deplane, or deplaned from the middle; the suspect purchased one-way tickets or round-trip tickets; the suspect flew on a nonstop flight or changed planes; the suspect flew with no luggage, light luggage, or new luggage; the suspect traveled alone or traveled with a companion; and the suspect acted nervously or acted too calmly. 490 U.S. at 13–14 (Brennan, J., dissenting). The list is all too reminiscent of CBP Officer Pichardo's testimony in this case regarding some of what he characterized as the "derogatory" factors that permit him and his fellow agents at JFK to search travelers' cell phones and other electronic devices: for example, whether the traveler has traveled to or from anywhere "in Europe," any country that has "political difficulties," or any country the United States government is "looking at for intelligence." Suppression Hr'g Tr. 19:6–19.

It is one thing for courts to give border officials the authority to briefly detain and question air travelers and search their physical belongings based on something more than a "hunch" but "'obviously less' than is necessary for probable cause." *Navarette*, 572 U.S. at 397 (citations omitted). But it is an entirely different matter for courts to exempt those agents from the Fourth Amendment's probable cause and warrant requirements in the vastly more intrusive context of a cell phone search, which can reveal "[t]he sum of an individual's private life." *Riley*, 573 U.S. at 394. Doing so would, in this Court's view, strain the Fourth Amendment's "reasonableness" requirement far beyond the bounds of *Terry* and its progeny.

Another factor weighing in favor of requiring border officials to obtain a judicial warrant before they may inspect the contents of a traveler's cell phone is the practicability of doing so in modern times, for "[r]ecent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient." *Id.* at 401 (citation omitted). With the advent of telephonic and emailed warrants, officers in some jurisdictions can obtain a warrant electronically "in less than 15 minutes," *Missouri v. McNeely*, 569 U.S. 141, 173 (2013) (Roberts, C.J., concurring in part), and in most jurisdictions, within a few hours, *see, e.g.*, *United States v. McKenzie*, 13 F.4th 223, 228–29 (2d Cir. 2021) (noting officers obtained warrant to search car several hours after stopping it on the street); *United States v. Caraballo*, 831 F.3d 95, 105 (2d Cir. 2016) (noting officers could have obtained search warrant in six hours). And at the border, officials are even more well-positioned to obtain a warrant while the traveler is temporarily detained in the secondary inspection area.

That was certainly the case here. Sultanov was detained for several hours while he waited, first for Pichardo to inspect his phone and then for off-duty HSI agents to arrive and question him (a delay that was due in part to the fact that HSI initially "denied interest" in sending an agent to examine Sultanov's phone when Pichardo contacted them). Suppression Hr'g Tr. 32:23. And even assuming that in a particular case, a warrant for a cell phone search cannot be obtained in the time that CBP is legally allowed to detain a traveler who has not been accused of a crime or found to be in possession of other contraband, an immediate warrantless search is not the government's only option. As Pichardo testified, CBP may seize a traveler's cell phone *without* inspecting its contents and permit him to leave the airport, giving them ample time to obtain a warrant for the search itself.[11] *Id.* at 45:22–47:7.

v. First Amendment Considerations

The Court's conclusion that electronic device searches at the border generally require probable cause and a warrant is based principally on the heightened privacy interest a person has in her phone and the limited legitimate governmental interest

[11] Here, Sultanov has challenged only the warrantless search of his cell phone at JFK and the subsequent forensic search of the device based, in part, on information obtained from him (and his devices) at the airport. As such, this Court does not consider or decide whether the warrantless *seizure* of a traveler's cell phone for some longer period of time (e.g., for hours or days) based on a showing of reasonable suspicion and/or probable cause, in order to give law enforcement time to seek a warrant for a search of its contents, would violate the Fourth Amendment. Courts might strike an entirely different balance when officials are not actually inspecting the private contents of these devices without a warrant and are merely refusing to let travelers enter the country without their devices in hand while law enforcement seeks judicial approval for a search of the phone's data. But as that issue is not presented here, the Court does not decide it.

promoted by such searches. Another important consideration is the substantial risk that allowing warrantless searches of incoming travelers' electronic devices will unduly burden, chill, or otherwise infringe upon their First Amendment activities.

It is well established that where governmental conduct implicates First Amendment conduct, the Fourth Amendment's warrant requirement must be applied with "scrupulous exactitude." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)). And "[w]here presumptively protected materials are sought to be seized, the warrant requirement should be administered to leave as little as possible to the discretion or whim of the officer in the field." *Id.*; *accord People v. Seymour*, 536 P.3d 1260, 1274–75 (Colo. 2023) (holding that a suspect's internet search history implicates core "expressive activity" protected by the First Amendment and that police must obtain a warrant that complies with the Fourth Amendment's rigorous requirements before accessing it).

After *Riley*, it is undeniable that the contents of a traveler's cell phone implicate core First Amendment activities. Whether from the phone owner's contact lists, private messages, calendar entries, diaries, internet search histories, photographs, videos, or location data, *see Riley*, 573 U.S. at 393–96, a governmental search of a traveler's phone will typically reveal a plethora of private information about that person's speech, association(s), beliefs, and religious practices, *see* U.S. Const. amend. I. Of course, the First Amendment does not shield electronic data from searches and seizures simply because it implicates expressive material. But it

does obligate courts to "scrupulous[ly]" apply the Fourth Amendment's safeguards against unreasonable searches of that material by government officials, which, this Court concludes, can only be achieved by application of the warrant requirement in most cases. *Zurcher*, 436 U.S. at 564 (citation omitted).

The amici brief filed by the Knight First Amendment Institute at Columbia University and the Reporters Committee for Freedom of the Press makes a persuasive case that warrantless searches of cell phones not only constitute an unjustified governmental intrusion into travelers' private expressions of religion, personal associations, and journalistic endeavors — they also risk chilling the exercise of those rights. Specifically, amici assert that border searches of electronic devices burden freedom of the press by chilling reporter-source communications. Amici Br. 12. They argue that "[j]ournalists are particularly vulnerable to the chilling effects of electronic device searches, both because confidential or vulnerable sources may refuse to speak with reporters for fear that anything they say may end up in the government's hands, and because such searches can be used to retaliate against or deter reporting critical of the government." *Id.* at 10.

Amici's concerns are not hypothetical but instead are based on the recent experience of numerous journalists who were flagged for secondary inspection and were required to surrender their electronic devices for warrantless searches and, in some cases, downloading of the devices' contact lists and contents based on these journalists' ongoing coverage of politically sensitive issues, like migration through

the U.S.-Mexico border.[12] After formal complaints were filed regarding a series of such incidents in 2019, it was revealed that they may not have been the isolated acts of individual border agents who suspected that a particular traveler's device contained contraband but instead part of a targeted effort to surveil journalists in particular: a non-public CBP database that contained the names of journalists covering migration issues and which pushed "alerts" to flag those journalists for secondary screening when they returned from international travel.[13] And even without the specter of a larger, insidious effort targeting journalists at the border, there remains a considerable and undue risk that — without the safeguards of a judicial warrant — journalists' sources in and outside the United States will be fearful of relaying information about matters of public concern to them. *Id.* at 10.

---

[12] Amici Br. 14–17 (citing Joseph Cox, *WSJ Reporter: Homeland Security Tried to Take My Phones at the Border*, Motherboard (July 21, 2016), https://www.vice.com/en/article/78ke9q/wsj-reporter-homeland-security-tried-to-take-my-phones-at-the-border [https://perma.cc/BMN9-96LW]; *Several Journalists Say US Border Agents Questioned Them About Migrant Coverage*, Comm. to Protect Journalists (Feb. 11, 2019), https://cpj.org/2019/02/several-journalists-say-us-border-agents-questione/ [https://perma.cc/QYK3-BKSF]; Ryan Devereaux, *Journalists, Lawyers, and Activists Working on the Border Face Coordinated Harassment from U.S. and Mexican Authorities*, The Intercept (Feb. 8, 2019), https://theintercept.com/2019/02/08/us-mexico-border-journalists-harassment/ [https://perma.cc/SR2Y-Y8KR]).

[13] Amici Br. 15; *Guan v. Mayorkas*, 530 F. Supp. 3d 237, 244–45 (E.D.N.Y. 2021) ("[A]ccording to NBC 7 San Diego, DHS maintained a secret database 'list[ing] people who[m] officials think should be targeted for screening at the border,' including journalists who documented the October 2018 caravan, and lawyers and activists who had communicated with migrants in the caravan." (some alterations in original) (citation omitted)); Bill Chappell, *U.S. Reportedly Compiled Database Of Journalists Working Along Southwest Border*, NPR (Mar. 7, 2019), https://www.npr.org/2019/03/07/701134722/u-s-reportedly-compiled-database-of-journalists-working-along-southwest-border [https://perma.cc/5MED-5KEH].

If journalists cannot reasonably assure their sources that border officials will not have broad discretion to access and download their contacts, notes, electronic messages, and recordings, the risk of chilling fundamental press activities is unduly high.

The Court also shares amici's concerns about the effect of warrantless searches of electronic devices at the border on other freedoms protected by the First Amendment — the freedoms of speech, religion, and association. *Id.* at 17. Even anecdotal accounts from travelers who complained that border officials improperly inquired into their religious practices, affiliations, and political views after conducting warrantless searches of their phones' contacts and social media applications[14] is enough to make clear the risks of taking judicial magistrates out of the equation. *Id.* at 9–10. In these divided and troubled times, travelers may harbor reasonable fears about the consequences of their affiliations with groups or expressions of views that are disfavored by those who hold the reins of power at any particular time. If this Court were to adopt the government's position that electronic device searches at the border require no suspicion whatsoever, the targets of political opposition (or their colleagues, friends, or families) would only need to travel once through an international airport for the government to gain unfettered

[14] For example, amici recount the story of a traveler who was detained by CBP officers in the Abu Dhabi airport and had her devices searched. Officers asked her intrusive questions about her political beliefs, including "[w]hat [she] think[s] when Americans say that Muslims are terrorists." Amici Br. 17–18 (alterations in original). Another traveler had his text messages, contacts, and photos searched, and officers asked "extensive questions about certain text messages" and "interrogated him about his political views." *Id.* at 18.

access to the most "intimate window into a person's life." *Carpenter*, 585 U.S. at 311. Even if the Court were to exempt border officials from the Fourth Amendment's warrant requirement and permit device searches based on reasonable suspicion, that flexible, all-too-easily satisfied standard is an insufficient bulwark against the potential abuse (or appearance of the same) of the government's power.

The right to dissent is the "fixed star in our constitutional constellation." *W. Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943). Courts must be vigilant in protecting that right, whether in the context of barring compelled speech, *see id.*, or — as here — guarding against government intrusion into the private, expressive activities of those who may hold disfavored viewpoints. Where the government seeks access to private devices that hold such a vast array of expressive content, only the standard conceived by the Founders and codified in the Fourth Amendment — probable cause and the approval of a neutral magistrate — can bear the weight of that obligation.

* * *

The parties agree that the TECS hit to an ISP address associated with Sultanov gave the government reasonable suspicion that his device(s) contained illegal material when he returned to the United States. Oral Arg. Tr. 45:13–46:1. However, the government does not contend that the TECS hit alone — i.e., the only information it had when Sultanov entered JFK and was diverted to secondary screening — provided probable cause to believe that Sultanov's phone contained child pornography *before* CBP obtained his passcode and examined his phone in the secondary screening area. *See* Gov't May 4, 2023 Letter 5–6. Because the search

was conducted without probable cause and a warrant, the evidence obtained as a result of the search is potentially subject to suppression. The Court next considers whether, given the state of the law in the Second Circuit at the time of both the manual (in-airport) and subsequent forensic searches of Sultanov's phone, suppression is the appropriate remedy here.

E. Whether the Good Faith Exception Applies to the Forensic Search of Sultanov's Cell Phones Pursuant to the Search Warrant

The government argues that even if the manual search of Sultanov's phone at the airport violated the Fourth Amendment, the exclusionary rule should not apply to evidence collected from the later forensic search of Sultanov's devices because that search was conducted pursuant to a warrant. Opp'n Br. 32. In other words, because the officers who conducted the forensic search acted with objectively reasonable reliance on a warrant, there was no "conscious violation of the Fourth Amendment," and the good faith exception should apply. *See United States v. Raymonda*, 780 F.3d 105, 118 (2d Cir. 2015) (quoting *United States v. Leon*, 468 U.S. 897, 920–21 (1984)). The defense counters that the good faith exception should not apply because the search warrant was obtained based on the illegal, manual search of Sultanov's phone; when the illegally obtained information is excised from the search warrant affidavit, the warrant is not supported by probable cause; and because the search warrant affiant (HSI Agent Croft) intentionally misled the magistrate judge who signed the search warrant. Second Aff. in Supp. of Mot. ¶¶ 43–65.

The Supreme Court crafted the exclusionary rule, which excludes or suppresses from trial evidence that was obtained in violation of the Fourth Amendment, "to compel respect for the constitutional guaranty" against unreasonable searches. *Raymonda*, 780 F.3d at 117 (quoting *Davis v. United States*, 564 U.S. 229, 236 (2011)). Although application of the exclusionary rule can "exact[] a heavy toll on the justice system," resulting in the exclusion of inculpatory evidence and sometimes the dismissal of criminal charges, "the rule's corrective value justifies its cost when the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Id.* at 117–18 (internal quotation marks and citation omitted). However, when the police conduct a search pursuant to a search warrant and "execute[] that warrant in good faith, there is no conscious violation of the Fourth Amendment" and thus applying the exclusionary rule fails to serve its purpose — the deterrence of police misconduct. *Id.* at 118.

The search warrant affidavit here expressly includes information gleaned from the illegal search of Sultanov's phone at JFK. The affidavit states that "[u]pon manually reviewing [the phone], CBP officers identified that there was child sexual abuse material on [it]." Appl. for Search Warrant ¶ 8. The affidavit describes in graphic detail several videos containing child sexual abuse material that Agent Croft reviewed while at JFK. *Id.* at ¶ 9.

Where information obtained from an unlawful search was later used to obtain a search warrant, the Court must first determine whether there would have been probable cause for the warrant to issue had the affidavit not included the

illegally obtained information. *United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003) ("'[T]he mere inclusion of tainted evidence in an affidavit does not, by itself, taint [a] warrant or the evidence seized pursuant to the warrant,' [but instead] the court 'should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant.'" (citation omitted)). If the affidavit contained probable cause on other grounds, then the warrant remains valid. If, however, probable cause for the warrant depends on unlawfully obtained information, then the Court must determine whether the "agent who conducted the search acted in good faith reliance on the search warrant" and whether the agent's reliance was objectively reasonable. *United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985).

When a law enforcement officer acts in good faith, evidence that would otherwise be subject to the exclusionary rule need not be suppressed, except in four specific circumstances: "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (citation omitted).

Here, probable cause for the search warrant did not depend entirely on information obtained from the unlawful search of Sultanov's phone. The search warrant separately was supported by probable cause premised on Sultanov's

statements to the HSI agents. The affidavit alleges that after Sultanov "agree[d] to waive his *Miranda* rights," he told the officers that he "bought child sexual abuse materials online on a Russian social media platform and paid for them via Paypal," that he downloaded and purchased the materials in the United States, brought the materials to Uzbekistan, and then transported them back to the United States. Appl. for Search Warrant ¶ 10.

Sultanov argues that the search warrant cannot be based on statements he made to Agent Croft because those statements were unlawfully obtained (i.e., because Sultanov did not enter into a knowing, valid waiver of his *Miranda* rights). Even if that is the case, however, the "fruit of the poisonous tree" doctrine does not apply to tangible evidence discovered as the result of a *Miranda* violation, so long as the statement was "voluntarily" made. *See United States v. Patane*, 542 U.S. 630, 642 (2004). The remedy for a *Miranda* violation without a showing of involuntariness is limited to the exclusion of an unlawfully obtained statement and does not extend to the exclusion of derivative physical evidence. *Id.* at 643.

This record does not show that Sultanov's statements to Croft were involuntarily made, as that standard is applied in the custodial-interrogation context. "The central question in assessing whether a confession was given voluntarily is whether the defendant's 'will was overborne' at the time of the confession." *United States v. Carr*, 63 F. Supp. 3d 226, 239–40 (E.D.N.Y. 2014) (quoting *United States v. Corbett*, 750 F.3d 245, 253 (2d Cir. 2014)). "Whether a defendant's will was overborne is determined by examining 'the totality of all the

surrounding circumstances, including the accused's characteristics, the conditions of the interrogation, and the conduct of law enforcement officials.'" *Id.* at 240 (quoting *United States v. Taylor*, 745 F.3d 14, 23–24 (2d Cir. 2014)). Moreover, courts have found statements were made voluntarily when the individual "was not faced with actual violence, threats of violence or implied or express promises," did not show "that his mental capacity was diminished in any way, or that he was otherwise particularly susceptible to the pressures of the situation," and he "was not tricked or otherwise coerced into making the initial statements." *Id.*

Here, there is no evidence that the conditions of Sultanov's interrogation overbore his will. Sultanov was not handcuffed while he was questioned, Suppression Hr'g Tr. 59:3–7, and was asked if he wanted to take a break or if he needed a cushion to sit on during the interrogation, *id.* at 83:12–16. Nor is there evidence that Sultanov was faced with actual or threatened violence; that he suffered from any mental or cognitive impairment that impacted his ability to voluntarily participate in the interrogation; nor that he was any more susceptible to the pressures of the situation than any other suspect interrogated in that context would be. Thus, notwithstanding any potential *Miranda* violation, Sultanov's statements were not involuntary. In turn, the search warrant affidavit established probable cause without relying exclusively on information tainted by the unlawful manual search of Sultanov's phone.

Furthermore, even if the Court found, in the alternative, that the search warrant affidavit did not establish probable cause without the information from the

unlawful manual search of Sultanov's phone, the good faith exception would still apply. Sultanov has not disputed that CBP had reasonable suspicion that he had purchased or possessed child pornography at the time that Pichardo seized his phone and conducted a manual search. Although this Court concludes that a manual search of an electronic device at the border requires probable cause and a warrant, neither the Supreme Court nor the Second Circuit has yet addressed the quantum of suspicion necessary to support an electronic device search at the border since *Riley* was decided. Moreover, the first district court in this Circuit to hold that a warrant is required did not render that decision until fourteen months after Sultanov's phone was searched. *See Smith*, 673 F. Supp. 3d at 398–99 (issued on May 11, 2023). Accordingly, it was not "deliberate, reckless, or grossly negligent" for CBP to search Sultanov's phone without probable cause and a warrant given the state of the law at that time. *Raymonda*, 780 F.3d at 117–18. Law enforcement had no "significant reason to believe that their predicate act," the manual search of Sultanov's phone, "was indeed unconstitutional." *Ganias*, 824 F.3d at 223 (internal quotation marks and citation omitted) (applying good faith exception to evidence obtained pursuant to a warrant where probable cause for the warrant depended on information obtained through a Fourth Amendment violation). Because law enforcement's reliance on the search warrant was "objectively reasonable," the good faith exception applies here, and the Court denies Sultanov's motion to suppress the evidence obtained from his devices pursuant to the search warrant. *Id.*

II. Fifth Amendment

Sultanov next moves to suppress the statements he made to law enforcement at JFK, contending that the statements were obtained in violation of the Fifth Amendment.

The Fifth Amendment to the United States Constitution provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. "To protect the Fifth Amendment right against self-incrimination, the Supreme Court in *Miranda v. Arizona* ruled that police may not interrogate a suspect who has been taken into custody without first warning the person 'that he has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires.'" *United States v. Newton*, 369 F.3d 659, 668 (2d Cir. 2004) (quoting *Miranda v. Arizona*, 384 U.S. 436, 479 (1966)).

Law enforcement officers must provide a suspect with *Miranda* warnings before conducting a "custodial interrogation." *United States v. FNU LNU*, 653 F.3d 144, 148 (2d Cir. 2011). Custodial interrogation is a two-word phrase that imposes two separate requirements: "(a) there must be an interrogation of the defendant, and (b) it must be while she is in custody." *Id.* (internal quotation marks omitted).

The first element, interrogation, is more easily defined. "[I]nterrogation under *Miranda* refers not only to express questioning, but also to any words or actions on the part of the police (other than those normally attendant to arrest and custody) that the police should know are reasonably likely to elicit an incriminating

response from the suspect." *Rhode Island v. Innis*, 446 U.S. 291, 301 (1980); *FNU LNU*, 653 F.3d at 148 (interrogation is "express questioning or its functional equivalent"). While questioning performed "as part of the processing normally attendant to arrest and custody," like asking the suspect for his identification information, typically does not require *Miranda* warnings, "engagement short of a formal interview" may implicate a person's rights under the Fifth Amendment depending on the nature of the questions asked. *United States v. Familetti*, 878 F.3d 53, 57–58 (2d Cir. 2017). Volunteered statements, on the other hand, that are made by a suspect not in response to questions or actions by law enforcement are not the result of interrogation and do not require *Miranda* warnings. *Id.* at 57.

The second element, custody, is clearly met when a suspect is formally arrested but is harder to recognize in less formal encounters with law enforcement. Custody for *Miranda* purposes is not "coterminous with . . . the colloquial understanding of custody." *FNU LNU*, 653 F.3d at 152–53. Instead, in this context, the "test for determining custody is an objective inquiry that asks (1) whether a reasonable person would have thought he was free to leave the police encounter at issue and (2) whether a reasonable person would have understood his freedom of action to have been curtailed to a degree associated with formal arrest." *United States v. Faux*, 828 F.3d 130, 135 (2d Cir. 2016) (internal quotation marks omitted). Although a person must be seized to be in custody, a seizure alone is a "necessary, but not sufficient, condition" to establish custody. *Id.* Notably, neither the suspect nor the officer's subjective beliefs concerning whether the suspect is in

custody is dispositive of the analysis, though the officer's view, if communicated to the suspect, may affect "how a reasonable person" in the suspect's position "would gauge the breadth" of her "freedom of action." *Id.*; *see United States v. Ali*, 68 F.3d 1468, 1473 (2d Cir. 1995) ("In sum, an officer's views concerning the nature of an interrogation . . . may be one among many factors that bear upon the assessment whether that individual was in custody, but only if the officer's views or beliefs were somehow manifested to the individual under interrogation and would have affected how a reasonable person in that position would perceive his or her freedom to leave." (quoting *Stansbury v. California*, 511 U.S. 318, 325 (1994)).

Courts must consider the totality of the circumstances of a suspect's encounter with law enforcement when determining whether the suspect is in custody. *FNU LNU*, 653 F.3d at 153. In addition to a formal arrest, courts have identified the following factors as particularly salient to a custody determination: "the interrogation's duration; its location (e.g., at the suspect's home, in public, in a police station, or at the border); whether the suspect volunteered for the interview; whether the officers used restraints; whether weapons were present and especially whether they were drawn; whether officers told the suspect he was free to leave or under suspicion . . . and, now, a juvenile suspect's age, if known to the officer or readily apparent." *Id.*

Determining whether a person is in custody at the border, particularly in the case of an international traveler arriving at an American airport, presents additional difficulties. There, "compulsory questioning — with no freedom to enter

the United States and with nowhere else to go — inheres in the situation." *Id.* By participating in air travel and arriving at the border, "the traveler has voluntarily submitted to some degree of confinement and restraint," and "a reasonable traveler will expect some constraints as well as questions and follow-up about his or her citizenship, authorization to enter the country, destination, baggage, and so on." *Id.* at 153–54. Therefore, a court determining whether a traveler who is questioned by law enforcement at the border is in custody for *Miranda* purposes must consider whether a reasonable person in the traveler's position, who necessarily expects some degree of constraint and questioning, would consider herself to be under arrest. *Id.* At the border, "the content of the officer's questions substantially inform[s] whether a reasonable person would feel restrained in a way similar to a formal arrest. Indeed, in many such cases, the fact that the questions asked fall within the range of inquiries one expects will, by itself, be enough to assure a reasonable person that he or she is not under arrest." *Id.* at 154; *United States v. Djibo*, 151 F. Supp. 3d 297, 306 (E.D.N.Y. 2015) (the "*most* important factor in determining whether *Miranda* applies at our borders will often be the objective function of the questioning" (emphasis in original)).

If the government wishes to introduce at trial statements made by the accused after she received *Miranda* warnings and while she was subjected to custodial interrogation, the government must establish by a preponderance of the evidence that the accused "in fact knowingly and voluntarily waived [her] [*Miranda*] rights" before making the statements. *See United States v. O'Brien*, 926

F.3d 57, 73 (2d Cir. 2019) (internal citation omitted). The accused's waiver must be twofold — it must be "voluntary in the sense that it was the product of a free and deliberate choice rather than intimidation, coercion, or deception, and must be knowing in the sense that it was made *with a full awareness of both the nature of the right being abandoned* and the consequences of the decision to abandon it." *Id.* (cleaned up). A defendant's waiver may be express or implied through his "actions or words." *Id.* Regardless of the manner in which a defendant waives, the "prosecution must make the additional showing that the accused understood these rights." *Berghuis v. Thompkins*, 560 U.S. 370, 384 (2010).

Sultanov makes two distinct arguments for suppression of his statements. First, he argues that his statements to CBP — including the fact that he provided Officer Pichardo with his phone's passcode — should be suppressed because he was subjected to custodial interrogation in the secondary screening area but was not given *Miranda* warnings. Mot. to Suppress ¶¶ 34–63. Second, he argues that his statements to HSI Agents Croft and Walter should be suppressed even though they first administered *Miranda* warnings, because he did not knowingly waive his *Miranda* rights before answering their questions and, in fact, made clear that he did not understand the warnings after Agent Croft read them to him. *Id.* at ¶¶ 64–67.

A. Questioning by CBP

With respect to Sultanov's statements to Officer Pichardo, the key question for the Court to resolve is whether Sultanov's interactions with Pichardo constituted a "custodial interrogation." It is undisputed that Pichardo did not *Mirandize*

Sultanov before directing him to provide his cell phone's passcode. But if the surrounding circumstances do not rise to the level of custodial interrogation, no such warnings were required. *See, e.g.*, *FNU LNU*, 653 F.3d at 154 ("[I]t is possible, though unlikely, for [a custodial] environment to exist even at the border, and if it does, so, too, must *Miranda*'s protections.").

The parties agree on many of the facts relevant to whether Sultanov was in "custody" at the time he spoke with Pichardo: "the interrogation's duration" (neither side proffered evidence concerning the duration but both suggested it was brief); "its location" (the lobby of the secondary inspection area); "whether the suspect volunteered for the interview" (he did not); "whether the officers used restraints" (they did not); and "whether weapons were present and especially whether they were drawn" (they were not). *Id.* at 153. Pichardo also testified that all of the travelers detained in the secondary inspection area were required to have an officer escort them to the restroom and watch them ("from a distance") while they relieved themselves. Suppression Hr'g Tr. 42:2. In addition, Pichardo testified that on occasion, some detained persons were placed into shackles while in the secondary inspection area, although he could not recall whether any individuals were in shackles on the day of Sultanov's arrival; nor did Sultanov allege that he viewed any other detained persons in shackles on that date. *Id.* at 62:3–18.

The parties disagree, however, "whether [Pichardo] told the suspect he was free to leave or under suspicion." *FNU LNU*, 653 F.3d at 153. And they offer somewhat different versions of "the content of the officer's questions," *id.* at 154,

which, in the context of an interrogation at the border, may be the single most important factor for determining whether a traveler is in custody, *see Djibo*, 151 F. Supp. 3d at 306.

In an affidavit, Sultanov alleges that he first refused to provide CBP officers with his passcode, that they gave him a document in English that he could not understand, that they told him the document stated that he had to give them his passcode and that he did not have a "choice or right to refuse to provide it," and that he provided his passcode only after he was told he had no choice but to do so. First Aff. in Supp. of Mot. ¶¶ 10–11; Mot. to Suppress ¶ 59 (same). He further claims that at the time he provided his passcode to Pichardo, the doors to the secondary inspection area were locked from the inside, CBP had Sultanov's U.S. passport and phone, and a CBP officer specifically told him he could not leave the secondary inspection area. First Aff. in Supp. of Mot. ¶ 13. Sultanov did not testify at the suppression hearing.

Pichardo testified that he initially asked questions concerning Sultanov's recent travel and then asked for Sultanov's cell phone. Suppression Hr'g Tr. 26:25–27:3. After Sultanov produced his cell phone, Pichardo could not recall whether Sultanov refused to provide his passcode, though he acknowledged he may have. He did recall that Sultanov "seemed a little confused of why I was asking for his cellular device." *Id.* at 27:13–14, 48:11–21. Pichardo recalled responding to Sultanov's questions about why Pichardo needed to examine his phone by saying, "I

just need your passcode and I need you to have a seat." *Id.* at 27:22–25, 50:13–19, 54:18–23, 66:6–15.

Pichardo testified that he provided Sultanov with a flyer concerning searches at the border but gave differing accounts as to whether he did so before or after Sultanov provided his passcode. *See id.* at 49:9–12 (testifying that after he gave Sultanov the tear sheet, Sultanov looked at it and then provided his passcode); *id.* at 67:11–17 (testifying that he provided Sultanov with the tear sheet only after Sultanov provided the passcode).

On this record, even if the Court credits Sultanov's version of events, it is a close question whether Sultanov was subjected to custodial interrogation when he provided Pichardo with his passcode. Many courts in this Circuit have found that a CBP officer's request for a traveler's cell phone and passcode in the secondary inspection area does not amount to custodial interrogation. *See, e.g.*, *Kamaldoss*, No. 19-cr-543, 2022 WL 1200776, at *8 (E.D.N.Y. Apr. 22, 2022) (finding that questioning in secondary inspection area of airport did not become custodial even where CBP officer asked for traveler's electronic devices and passcodes because "this single factor," though important, did not "transform[] an otherwise non-custodial environment into a custodial one"); *United States v. Shvartsman*, No. 23-cr-307, 2024 WL 1193703, at *30 (S.D.N.Y. Mar. 20, 2024) (finding that although CBP officer's request for traveler's phone and passcode "lend some support to the conclusion that [the traveler] was in custody, the greater context of the secondary inspection establishes that those two questions did not render [the traveler] in

custody for purposes of *Miranda*"); *Gavino*, 2024 WL 85072, at *9 (declining to find custodial interrogation where CBP officer (1) requested traveler's cell phone and passcode and (2) threatened to seize the phone for several months if the traveler did not unlock it, because "the questioning occurred in circumstances akin to a run-of-the-mill secondary inspection — around ten to fifteen minutes of questioning in a publicly accessible area").

This Court is not aware of any case in which a traveler, like Sultanov, has alleged that he refused to voluntarily provide his passcode, repeatedly asked why he needed to provide his cell phone and passcode, and was expressly told that refusing to provide his passcode was not an option. If Pichardo told Sultanov that an official-looking document (which was provided to Sultanov only in English — a language in which Sultanov is not fluent) specified that he did not "have a choice" but to provide his passcode to CBP upon request (when in fact it did not), First Aff. in Supp. of Mot. ¶ 11, Sultanov would have a credible argument that these circumstances "transformed an otherwise non-custodial environment into a custodial one," *Kamaldoss*, 2022 WL 1200776, at *8. Combined with the other undisputed facts on record — including, but not limited to, the fact that Sultanov and his fellow detainees could not use the restroom without being accompanied by a law enforcement officer who watched them do so, Suppression Hr'g Tr. 41:24–42:2, and the fact that other detainees in the secondary screening area may have been shackled, *id.* at 62:3–18 — Pichardo's conduct as described in Sultanov's affidavit might well create the sort of "coercive" environment that requires *Miranda*

warnings be given, i.e., by falsely inducing a U.S. citizen to believe that he could not be admitted to his own country (or worse) unless he provided the passcode to his cell phone. *Cf. Gavino*, 2024 WL 85072, at *9 (finding that CBP officer's threat to seize traveler's phone if traveler did not unlock it was not coercive conduct because the officer's statement was a truthful representation of CBP's legal options).

However, the Court credits and gives greater weight to Pichardo's in-person testimony, which was subject to cross-examination, than Sultanov's affidavit. *See United States v. Cherry*, 541 F. Supp. 3d 407, 422 (S.D.N.Y. 2021) ("Courts give greater weight to witness testimony, which was subject to cross examination. This principle applies even where an adversary has submitted an affidavit or declaration."); *United States v. Frank*, 8 F. Supp. 2d 284, 291 n.2 (S.D.N.Y. 1998) (noting "the Court was unable to form an opinion as to [the defendant's] credibility or the truthfulness of his allegations" where defendant submitted an affidavit in support of a motion to suppress but made allegations that conflicted with law enforcement witnesses "who testified at the hearing" and "appeared forthright and truthful," leading the Court to give greater weight to the live testimony). While Pichardo had difficulty remembering certain aspects of his interactions with Sultanov, he consistently maintained that he did not expressly state or imply that Sultanov was required to provide his passcode as a condition of reentering the United States and did not suggest to him that the tear sheet stated in English that a passenger must provide his passcode. Suppression Hr'g Tr. 48:2–49:12. On the other hand, by his own account, Pichardo did not merely request that Sultanov

disclose his phone's passcode: he repeatedly told Sultanov that he "need[ed]" to disclose it. *Id.* at 28:18–20, 49:16–18.

Asking a detained traveler for his cell phone and passcode "stray[s] from the routine questioning a reasonable traveler would expect at the border," *Shvartsman*, 2024 WL 1193703, at *30, and having a uniformed agent additionally (and repeatedly) state, "I need your passcode" would likely be understood by most travelers to be an official command rather than a question. Nevertheless, under current Second Circuit precedent, *see, e.g.*, *FNU LNU*, 653 F.3d at 153–55, the Court finds that the totality of these circumstances did not rise to the level of custodial interrogation.

Because Sultanov was not subjected to custodial interrogation during his interactions with Officer Pichardo, Sultanov's motion to suppress his statements to Pichardo, including the provision of his phone's passcode, is denied.

B. Questioning by HSI Agents

Sultanov's argument concerning his recorded statements to the HSI agents rests on surer legal and factual footing. The Court need not resolve any factual disputes because the HSI agents made an audio recording of their interrogation of Sultanov (which memorializes that they administered *Miranda* warnings at the outset), *see* HSI Audio Recording dated Mar. 5, 2022, and the government has not disputed that Sultanov was subjected to custodial interrogation. The only question for this Court to resolve is whether the government has established by a preponderance of the evidence that Sultanov knowingly waived his *Miranda* rights before he began answering the HSI agents' questions.

Sultanov argues that he did not make an implied, knowing waiver of his *Miranda* rights because he expressly informed the agents that he did not fully understand the warnings; he asked questions about the *Miranda* rights form and otherwise indicated that he did not understand it; and his responses in the interrogation demonstrate that his English proficiency was limited. Oral Arg. Tr. 54:9–58:14. The government argues that Sultanov's overall course of conduct and his communications in English demonstrate that he made an implied, knowing waiver. Opp'n Br. 38–39.

The Court concludes that Sultanov did not make a knowing waiver of his *Miranda* rights. Accordingly, with the exception of brief, spontaneous utterances at the beginning of the interrogation (as explained below), nearly all of his statements to the HSI agents must be suppressed.

Before an accused's confession to law enforcement obtained in a custodial interrogation can be introduced against him at trial, the government must prove by a preponderance of the evidence that the accused made a knowing and voluntary waiver of his rights after receiving *Miranda* warnings. *See United States v. Plugh*, 648 F.3d 118, 127 (2d Cir. 2011). A waiver may be express, as when a suspect signs a "waiver-of-rights" form, or implied by "the actions and words of the person interrogated." *Id.* In the case of an implied waiver, "the law can presume that an individual who, with a full understanding of his or her rights, acts in a manner inconsistent with their exercise has made a deliberate choice to relinquish the protection those rights afford." *Id.*

Whether express or implied, where the government claims that the defendant waived his *Miranda* rights, the government must demonstrate that he understood the rights he waived before he forfeited them. *See Berghuis*, 560 U.S. at 384; *United States v. Male Juv. (95-CR-1074)*, 121 F.3d 34, 40 (2d Cir. 1997) ("Only if the totality of the circumstances reveals both an uncoerced choice and the requisite level of comprehension may a court properly conclude that the *Miranda* rights have been waived." (citation omitted)). There is a presumption against waiver, and the government's burden to demonstrate a waiver is "great" because a court will "indulge every reasonable presumption against waiver of fundamental constitutional rights." *United States v. Garibay*, 143 F.3d 534, 536–37 (9th Cir. 1998). "The Government must do more than show simply that a *Miranda* warning was given and the accused thereafter made a statement. We may imply waiver only when the prosecution has made 'the additional showing that the accused *understood* these rights.'" *United States v. Murphy*, 703 F.3d 182, 194 (2d Cir. 2012) (emphasis in original) (quoting *Berghuis*, 560 U.S. at 384).

After Agent Croft read Sultanov his *Miranda* rights, he asked whether Sultanov understood those rights. Sultanov responded, "50/50" — that is, Sultanov stated that he half-understood, and half-did-*not*-understand, the warnings he had just been given. *See* HSI Tr. 3:26–27. The government bears the burden of demonstrating by a preponderance of the evidence — that is, by a showing that is *more* than fifty-fifty — that Sultanov's waiver of his *Miranda* rights was knowing. For obvious reasons, Sultanov's straightforward answer to Agent Croft's query is

problematic for the government. Put simply, this is the rare case in which the government may fall short of its burden with near mathematical certainty.

The government nonetheless argues that notwithstanding Sultanov's plain and candid response above, the entirety of the transcript establishes that Sultanov understood his rights to (among other things) remain silent and consult with an attorney and that he knowingly waived those rights and chose to answer the agents' questions. Opp'n Br. 35–39. The Court finds otherwise.

To determine whether a suspect made a valid waiver, courts must consider the totality of the circumstances, including the particular facts of the case before it, like "the background, experience, and conduct of the accused." *Plugh*, 648 F.3d at 127. A suspect's age, English language proficiency, and intellectual limitations may be particularly relevant to a court's waiver assessment. *See United States v. Zeng*, 804 F. App'x 18, 20 (2d Cir. 2020); *United States v. Ibrahim*, 998 F. Supp. 2d 12, 17–18 (N.D.N.Y. 2014) (citing *Zeng* for proposition that a defendant's lack of fluency in English is relevant to, but does not "automatically preclude" a finding that a defendant made a knowing waiver of his rights); *United States v. Jaswal*, 47 F.3d 539, 542 (2d Cir. 1995) (considering accused's apparent command of English when evaluating claim that language barrier, among other things, prevented accused from making a knowing waiver).

Courts in other circuits confronted with a language-barrier based waiver challenge have identified additional relevant factors, including: "(1) whether the defendant signed a written waiver, (2) whether the defendant was advised of his

rights in his native tongue, (3) whether the defendant appeared to understand his rights, (4) whether a defendant had the assistance of a translator, (5) whether the defendant's rights were individually and repeatedly explained to him; and (6) whether the defendant had prior experience with the criminal justice system." *Garibay*, 143 F.3d at 538 (cleaned up); *see United States v. Monreal*, 602 F. Supp. 2d 719, 722 (E.D. Va. 2008) (listing as factors: "1) whether the defendant indicated in the affirmative when asked if he or she understood his or her rights; 2) whether the defendant indicated that he or she understood English; 3) the length of defendant's residency within the United States; and 4) defendant's previous encounters with the criminal justice system" (citation omitted)).

When a suspect contends that a language barrier prevented him from comprehending his rights sufficiently to knowingly waive them, courts pay particular attention to whether the defendant was "advised of his rights in a language that he understands" and to the "defendant's conduct at the time the warnings are given." *United States v. Rijo-Carrion*, No. 11-cr-784, 2012 WL 6617388, at *5 (E.D.N.Y. Dec. 19, 2012) (noting that waiver determination is more straightforward where a non-English speaking person is advised of his rights in his first language rather than in English). "A defendant's indication at the time the warnings are given that he understands them and wants to speak to police is strong evidence of a knowing waiver. Even if the translation is not perfect or defendant's conduct initially suggests some confusion regarding his rights or hesitancy to speak,

the waiver is still knowing as long as [the] defendant ultimately confirms that he understands his rights and wants to talk." *Id.*

Based on the totality of the circumstances, the Court concludes that the government has not met its burden of proving that Sultanov knowingly waived his *Miranda* rights. First, Sultanov plainly stated from the outset that he did not understand the *Miranda* warnings. *See* HSI Tr. 3:26–27 (responding "50/50" when asked if he understood them). Second, Sultanov did not sign the written *Miranda* waiver form and asked questions about the form that made clear he did not understand the form's content or purpose. *See id.* at 3:32–35. Third, Sultanov's course of conduct throughout the interrogation demonstrates that his original expressions of confusion in response to the *Miranda* warnings were genuine, and the HSI agents had an obligation to address them before they began interrogating him. Instead, they exploited the fact that Sultanov did not understand his Fifth Amendment rights and charged ahead with the admitted aim of eliciting incriminating information from him.

Far from establishing an implied waiver, Sultanov's interactions with the agents after his "50/50" answer only underscore his lack of understanding. When the agents presented him with the written *Miranda* warnings, he said: "So I tried to understand, what is happening right now? I'm trying to read this stuff. You say, I'm not gonna arrest, right?" He then asked, "So what is that, this one?", referring to the written *Miranda* warnings. *Id.* at 3:32–35. In addition to expressly conveying his confusion, the interrogation recording and transcript demonstrate

that the language barrier meaningfully limited Sultanov's comprehension of the questions put to him and his ability to coherently respond to them.

From the beginning of the interrogation, it was clear that Sultanov has limited English proficiency. Early in the interview, before advising Sultanov of his *Miranda* rights, Agent Croft asked: "And you're comfortable communicating in English, right?" *Id.* at 2:11. Sultanov responded, "[i]f you're talking slowly." *Id.* at 2:12. Sultanov was then provided with *Miranda* warnings in English orally and in writing, but he clearly expressed that he did not understand them. The agents did not offer to provide Sultanov with *Miranda* warnings in Sultanov's primary language, nor did they offer him access to an interpreter. When Sultanov made it clear he was struggling to read and understand the written *Miranda* warnings, after one brief attempt to offer to further explain, *id.* at 3:28, in the face of multiple questions and statements that made clear that Sultanov did not understand the *Miranda* warnings, the agents continued to question him without any further clarifications. For example, Sultanov said, "You say, I'm not gonna arrest, right?", suggesting an obvious misunderstanding of the *Miranda* warnings or the preamble Croft gave before them when he said, "So first of all you're not under arrest." *Id.* at 2:15, 3:32–33. Rather than clarifying the warnings and Sultanov's custodial status, Croft said only, "Yeah." *Id.* at 3:34. Still confused, Sultanov went on to ask, "So right now, so whatever you guys find out, so what gonna happen to me. Do you understand what I'm saying?" *Id.* at 3:38–39.

Instead of resolving Sultanov's confusion about the meaning of the *Miranda* warnings, whether he had already been or would be arrested and whether what he said to the agents — "whatever [they] [found] out" — could be used against him, the HSI agents took advantage of his confusion. *Id.* at 3:38. They asked him a question with a false premise that was calculated to elicit an incriminating answer: "Well, first of all tell us about this video" — a video showing child sexual abuse — "and maybe nothing is wrong at all." *Id.* at 3:40–41. As Croft admitted when he testified, he asked that question specifically to encourage Sultanov to "continue speaking," Suppression Hr'g Tr. 121:24–122:6, and having viewed the video in question, it was "not very likely," *id.* at 112:4–9, that Sultanov could have said anything about the video to persuade Croft there was "nothing wrong at all" with possessing it, *id.* at 112:1–18.[15]

[15] This is not to say that there is anything unlawful about Croft's use of deception *per se*. The Supreme Court has held that law enforcement agents have considerable leeway to use deceptive techniques to encourage suspects to incriminate themselves, including the sort of "minimization" technique that Croft employed here. *See, e.g.*, *Illinois v. Perkins*, 496 U.S. 292, 297 (1990) ("*Miranda* forbids coercion, not mere strategic deception . . . . Ploys to mislead a suspect or lull him into a false sense of security that do not rise to the level of compulsion or coercion to speak are not within *Miranda*'s concerns."). The problem in this case is that Croft deliberately utilized a deceptive technique designed to elicit incriminating statements about the videos on Sultanov's phone *after* Sultanov made it clear that he did not understand that he had a right to remain silent, to consult with an attorney, and to refrain from making any statements that could be used against him at trial. It would be an entirely different matter if Croft had returned to the *Miranda* warnings, explained them in clear terms that Sultanov indicated he understood, or otherwise established that Sultanov was aware of but was willing to waive his core Fifth Amendment privileges.

The transcript of the interrogation is replete with examples of Sultanov's miscomprehension due to the language barrier, even with respect to questions that are far simpler than those posed to him at the outset of the interview. For example, he was asked, "When did you naturalize?" and thought he was being asked for his nationality, so he said, "Nationality is Uzbek." HSI Tr. 5:86–89. When he was asked whether the woman who was traveling with him that day was his wife's mother, he said: "I wasn't sent out already. It was like 12, I think or 1pm or something. So I am still here," a response that suggests a total misunderstanding of the question. *Id.* at 7:129–31.

Based on this transcript, the Court concludes that Sultanov's command of English was often good enough to understand the general topic being discussed but not good enough to understand and give a clear response to the particular question being asked, even in the course of courteous small talk.[16] It is no wonder, then, that he struggled to understand and give responsive answers to more loaded questions, like, "So what is the youngest legal age [in Uzbekistan] that you're allowed to marry or have sex with somebody," to which he said, "You cannot have sex except like virgin. Okay." *Id.* at 44:969–71.

[16] This conclusion is not undermined by Sultanov's general assertions on his naturalization form that he can read and understand English and did not require an interpreter to complete the form. Suppression Hr'g Tr. 99:13–100:3. These statements do not outweigh the evidence of his repeated difficulty understanding the questions put to him during the interrogation and are insufficient to meet the government's burden of establishing an implied, knowing waiver of his *Miranda* rights.

On multiple occasions, Sultanov's responses were not "appropriate to questions asked." *Ibrahim*, 998 F. Supp. 2d at 17–18 (finding that defendant who alleged that a language barrier prevented him from knowingly waiving his *Miranda* rights had given responses to questions that demonstrated his comprehension and undermined his argument). He repeatedly expressly communicated "that he failed to understand." *Id.* at 18. "Where, as here, English comprehension is the sole issue, the quintessential question is whether the government has proved by a preponderance of the evidence from the totality of the circumstances that [Sultanov] had a command of English sufficient to find that he understood his *Miranda* rights and the consequences of his waiver." *Id.* at 17. Based on Sultanov's clear statement that he did not fully understand the *Miranda* warnings from the outset, and his continued course of conduct throughout the interrogation, the Court concludes that the government failed to meet its burden to prove that he made a knowing waiver of his Fifth Amendment rights and that the bulk of his statements to the HSI agents must be suppressed.

On the other hand, Sultanov made one statement to the HSI agents before they began to substantively question him that need not be suppressed because it was a "spontaneous statement[]." *Carr*, 63 F. Supp. 3d at 237. After the agents read Sultanov his *Miranda* rights and Sultanov indicated he understood them "50/50," Agent Croft began to offer to explain them further when Sultanov interrupted him and said: "So, I do not understand, so I have a video. I'm not going to say like, oh use [unintelligible] or something else. I didn't know that it was

illegal. So after that . . . ." HSI Tr. 3:29–30. Sultanov had not yet been asked any questions by the agents (apart from whether he understood the *Miranda* warnings) when he made the statement. Indeed, Agent Croft appropriately responded to Sultanov's "50/50" expression of confusion by saying, "Well, let me explain anything," *id.* at 3:28, before Sultanov interrupted him and spontaneously made this statement. Because "volunteered information or spontaneous statements, even if made when an individual is in custody, do not implicate *Miranda*," that Sultanov had not knowingly waived his *Miranda* rights is of no moment. *Carr*, 63 F. Supp. 3d at 237. This statement, therefore, is not subject to suppression.

Furthermore, although it is unclear whether the government seeks to offer the exchange that immediately followed this remark (from "So I tried to understand . . ." to "Do you understand what I'm saying?", HSI Tr. 3:29–39) at trial, because these statements precede the juncture at which Croft made the decision to proceed with interrogating Sultanov, *see id.* at 3:40–41, they are not subject to suppression. However, Sultanov's motion to suppress is granted with respect to all portions of the interrogation that follow (from "Sure. So. Well, first of all tell us about this video . . . ." onward, *id.*).

CONCLUSION

For the foregoing reasons, Sultanov's motion to suppress is GRANTED in part and DENIED in part. The searches of Sultanov's phone violated the Fourth Amendment, which requires cell phone searches at the border to be supported by a warrant and probable cause; however, the Court denies suppression of the evidence

obtained pursuant to the search warrants in this case based on the good faith exception to the exclusionary rule. The Court grants Sultanov's motion to suppress the statements he made to Agents Croft and Walter, with the exception of the spontaneous statements discussed above.

SO ORDERED.

/s/ NRM
NINA R. MORRISON
United States District Judge

Dated: July 24, 2024
Brooklyn, New York