**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF KANSAS**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>**Plaintiff**,<br><br>**v.**<br><br>**FRANK CASTRO (01)**,<br><br>**Defendant**. | **Case No. 23-20032-01-DDC** |

**MEMORANDUM AND ORDER**

This matter comes before the court on defendant Frank Castro's Motion to Suppress (Doc. 18). Mr. Castro asks the court to suppress evidence found within two online accounts accessed through his phone. After the FBI approached his residence, Mr. Castro consented to a search of his phone. While searching the phone, the FBI reinstalled Telegram, a private messaging application, and logged into Mr. Castro's Telegram account. There, they found child pornography.[1] Later in the encounter, Mr. Castro consented to a search of a separate cloud storage account, MEGA. The FBI also found child pornography there.

Mr. Castro contends that the FBI's search of his Telegram account exceeded the scope of his consent. Specifically, Mr. Castro argues that he didn't authorize the FBI to install (or reinstall) an application on his phone and then log into it. Mr. Castro also asserts that this violation tainted his subsequent consent authorizing a search of his MEGA account. So, Mr.

[1] Consistent with the Indictment (Doc. 1), the court refers to the offending material as "child pornography." Mr. Castro's papers refer to the material found as child sexual abuse material (CSAM). *See* Doc. 18 at 2; Doc. 29 at 2. The government uses the term child pornography. *See* Doc. 26 at 2; Doc. 30 at 2.

Castro says, the court should suppress evidence found in his Telegram account and MEGA account.

The government disagrees. It argues that the FBI's search was within the scope of Mr. Castro's consent. The government also asserts that, in any event, the inevitable discovery exception to the exclusionary rule applies. Or, alternatively, the government contends the good faith exception applies. So, according to the government, even if a Fourth Amendment violation occurred, the court shouldn't suppress the evidence the FBI found.

This Order grants in part and denies in part Mr. Castro's Motion to Suppress (Doc. 18). The FBI's search of Mr. Castro's Telegram account exceeded the scope of his consent. And neither the inevitable discovery exception nor the good faith exception applies here. So, the court grants Mr. Castro's request to suppress evidence found in his Telegram account. But Mr. Castro separately and independently consented to a search of his MEGA account. That consent wasn't connected causally to the search of his Telegram account. The court thus denies Mr. Castro's request to suppress evidence found in his MEGA account.

This Order explains these decisions, *first*, by reciting the background facts. *Second*, the Order compares the scope of Mr. Castro's consent with the FBI's search of his phone and Telegram account. *Third*, the Order analyzes the inevitable discovery and good faith exceptions. And *finally*, the Order addresses the search of Mr. Castro's MEGA account and the question of tainted consent.

## I. Background

The court held an evidentiary hearing on the motion on June 5, 2024. Unless otherwise noted, the court derives the following factual findings from evidence presented at that hearing.

***2019 Encounter***

FBI Task Force Officer (TFO) David Albers was the FBI official who reinstalled Telegram on Mr. Castro's phone in 2021. But 2021 wasn't the first time that TFO Albers had encountered Mr. Castro. He first met Mr. Castro in 2019 when he was following up on an anonymous tip from a user on a social media site. The tip claimed that Mr. Castro had communicated a sexual interest in and desire to abuse minor boys. TFO Albers went to Mr. Castro's residence in Kansas City, Kansas, with another FBI agent. Mr. Castro voluntarily spoke with TFO Albers and admitted that he had received child pornography in the past but stated that he since had deleted it. Mr. Castro then consented to a search of his phone. TFO Albers searched Mr. Castro's phone and found no child pornography on it. The FBI took no more action following this 2019 interaction. It didn't seek a warrant or Mr. Castro's consent to search online accounts or to examine the phone forensically.

***Lead-Up to 2021 Encounter***

Some two years later, Mr. Castro resurfaced on the FBI's radar. In 2021, the Milwaukee Police Department began investigating Antonio Galicia for possession, distribution, and production of child pornography after receiving a tip from the National Center for Missing and Exploited Children. Doc. 26 at 2. MPD seized and searched Galicia's devices and discovered conversations between Galicia and Mr. Castro on Facebook and Telegram.[2] *Id.* Galicia and Mr. Castro discussed sexually abusing children and meeting up to do so. *Id.* at 2–3. Galicia also sent Mr. Castro a video involving sexual abuse of children. *Id.* FBI Milwaukee alerted FBI Kansas City of these interactions. *Id.* at 4.

[2] Telegram is a cloud-based application, meaning that all the data a user sees when logging into Telegram isn't necessarily stored on the device itself. Instead, the data is stored on the cloud which allows users to download content on any device they use to log on; they pick up where they left off at the end of the earlier session.

***2021 Encounter***

On July 7, 2021, FBI Special Agent (SA) Ashley Davis and TFO Albers approached Mr. Castro's residence in Kansas City, Kansas, to follow up on the lead from FBI Milwaukee. Doc. 18 at 2; Doc. 26 at 4. Agents didn't have an arrest warrant for Mr. Castro. Doc. 18 at 2. Nor did they have a warrant to search Mr. Castro's property. Doc. 18 at 2; Doc. 26 at 15–16. Mr. Castro answered the door. The agents audio recorded the ensuing interaction, which lasted for an hour and eight minutes.

After identifying themselves, SA Davis and TFO Albers explained that they were investigating online "suspicious activity" that traced back to Mr. Castro's residence. SA Davis asked Mr. Castro if he was familiar with Facebook and Telegram. Mr. Castro said that he was familiar with these applications but didn't use them. SA Davis explained the nature of Galicia's suspected crimes and told Mr. Castro that they believed he recently was in contact with Galicia through Facebook and Telegram. She showed Mr. Castro a Facebook account, and Mr. Castro confirmed that it was his "old" Facebook account. Mr. Castro added that he didn't get on Facebook much but later admitted that he had used it that same morning. When SA Davis asked if he recognized Galicia's Facebook account, Mr. Castro said no.

SA Davis then showed Mr. Castro a Telegram account with Mr. Castro's phone number and the same profile picture as his Facebook account. She asked him if it was his Telegram account. Mr. Castro responded that he doesn't use Telegram and that he doesn't remember using it at the time when conversations with Galicia allegedly had occurred. SA Davis replied that she wasn't familiar with Telegram but that it appeared Mr. Castro had created the account upon Galicia's request. Mr. Castro denied having Telegram on his phone. SA Davis then referenced a video of Galicia sexually abusing a child, which Galicia allegedly had sent to Mr. Castro through

Telegram. Mr. Castro contended that he didn't recognize the video and that he didn't have the video on his phone.

SA Davis explained to Mr. Castro that she and TFO Albers were investigating him because of comments he made to Galicia about sexually abusing minors. Mr. Castro responded that he didn't remember making those comments because he was on methamphetamine. The agents continued to ask Mr. Castro about his interactions with Galicia, but Mr. Castro maintained that he couldn't remember anything because he was on methamphetamine. Mr. Castro asserted that he had deleted numbers off his phone in an attempt to better himself. The agents again asked Mr. Castro if he possessed child pornography or anything illegal on his phone. Mr. Castro said no.

After this back and forth, SA Davis asked for Mr. Castro's consent to search his phone. She asked, "Do you care if we take a look at it now? Would you consent to a search of the phone so we can take a look and make sure there's nothing on there that's concerning?" Mr. Castro agreed. He said his phone was in his bedroom. With Mr. Castro's permission, TFO Albers accompanied Mr. Castro into his home to retrieve the phone. Mr. Castro and TFO Albers returned to the porch. While TFO Albers searched Mr. Castro's phone, SA Davis and Mr. Castro conversed. According to TFO Albers, Mr. Castro and the FBI agents were standing in a "semi-triangle" with Mr. Castro and TFO Albers facing one another. At the evidentiary hearing, TFO Albers claimed that Mr. Castro could see what he was doing on the phone. But TFO Albers was equivocal about whether Mr. Castro actually was watching the phone.

TFO Albers testified that he couldn't remember the specifics of his search but that his manual review of the phone would have included searching areas of the phone commonly used to conceal child pornography. This includes reviewing the photo gallery, internet tabs and

history, SMS text messages, and all possible applications present or previously present on the phone. He also testified that he would have paid close attention to deleted files because it's common for subjects to hide illegal content from their family and law enforcement.

***Search of Telegram***

During this search, TFO Albers opened the App Store on Mr. Castro's iPhone and looked for the Telegram application. In the App Store, the Telegram icon had "an arrow pointing down," indicating that the phone's associated Apple ID once had downloaded the application. According to credible testimony by Mr. Castro's digital forensics expert, this icon also indicates that the application—and data associated with it—weren't located on the phone when TFO Albers examined it. TFO Albers typed Mr. Castro's phone number into Telegram, and Telegram sent a code to the phone via text message. TFO Albers input that code into the phone, effectively logging into Mr. Castro's account.[3]

Once logged in, TFO Albers observed that Mr. Castro's Telegram account had been active as recently as three days earlier—July 4. He also discovered that a Telegram user—who wasn't Galicia—had sent child pornography to Mr. Castro. TFO Albers streamed this conversation and content across the internet from Telegram's servers and displayed it in real-time on Mr. Castro's phone screen. In front of Mr. Castro, TFO Albers showed SA Davis something displayed on Mr. Castro's phone. Mr. Castro claimed that he was asleep at the time of these alleged communications. He also confirmed that nobody else uses his phone.

[3] In lieu of a password, Telegram requires users to input the phone number associated with the account which then sends a unique code via text message. After plugging this code into the application, users gain access to the account.

***Written Consent and Consent to Search MEGA***

SA Davis asked Mr. Castro for his phone passcode on two separate occasions; Mr. Castro provided it both times. TFO Albers asked if they could "take over" Mr. Castro's Telegram account and assume his identity. Again, Mr. Castro agreed. And he signed an FBI Consent to Assume Online Identity Authorization Form. Doc. 18-2 (Def. Ex. 2). SA Davis also asked Mr. Castro to sign, retroactively, an FBI Consent to Search Form covering the original search of the phone. Doc. 18-3 (Def. Ex. 3). He did. TFO Albers next asked Mr. Castro about his MEGA account.[4] After Mr. Castro initially denied having a MEGA account, TFO Albers read Mr. Castro's username and password aloud. Mr. Castro then—without solicitation—said, "You guys want to look it up or something?" The agents responded affirmatively. They then sought Mr. Castro's permission to add his MEGA account to the FBI Consent to Assume Online Identity Authorization Form that Mr. Castro already had signed for his Telegram account. Mr. Castro consented to this addition.

Toward the end of the interaction, SA Davis informed Mr. Castro that she needed to take his phone to the office to examine it forensically. She gave him two options: Mr. Castro could give consent—presumably a quicker turnaround—or she could seize the phone, get a warrant, and then search the phone, which could take "a couple days." Defendant expressed concern that if he gave consent, they could use what they found against him. But he also worried that he wouldn't get the phone back in time for work that day. In the end, he gave the agents consent to take the phone.

[4] MEGA is a cloud storage website that also has chat features. MEGA, mega.io (last visited Aug. 23, 2024).

***Forensic Extraction***

SA Davis and TFO Albers returned to the office to continue their examination of Mr. Castro's phone. They used the "Cellebrite UFED forensic tool" to extract data from Mr. Castro's phone. That extraction didn't yield any evidence of child pornography. The agents returned Mr. Castro's phone later in the day on July 7.

A grand jury indicted Mr. Castro on one count of Distribution of Child Pornography and one count of Possession of Child Pornography. Doc. 1. The Indictment is based solely on evidence found in Mr. Castro's Telegram and MEGA accounts. Doc. 18 at 4. Mr. Castro asks this court to suppress all that evidence. Doc. 18; Doc. 29.

## II. Analysis

Mr. Castro filed his Motion to Suppress (Doc. 18), and the government responded (Doc. 26). After the court held an evidentiary hearing, the parties filed supplemental briefs. Doc. 29; Doc. 30. Mr. Castro argues that the government exceeded the scope of his consent and that the court thus should suppress evidence found in his Telegram account and his MEGA account. Doc 18; Doc. 29. The government contends that its search was within the bounds of Mr. Castro's consent. Doc. 26 at 9–14; Doc. 30 at 6–13. It also asserts that the court shouldn't suppress any evidence because the inevitable discovery and good faith exceptions apply to both applications. Doc. 26 at 14–17; Doc. 30 at 15–19. In response, the government argues that Mr. Castro's consent to search his MEGA account wasn't tainted, even if the court concludes that the FBI unlawfully searched Mr. Castro's Telegram account. Doc. 30 at 13–15. The court addresses these arguments, below.

### A. Scope of Consent

Mr. Castro argues that the court should suppress the evidence of child pornography found in his Telegram account. Specifically, Mr. Castro contends that TFO Albers exceeded the scope

of his consent by reinstalling Telegram; generating a code in Telegram; sending that code to Mr. Castro's phone; and using that code to access information stored on a remote Telegram server. The court agrees.

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. Const. amend. IV. A party can establish that a search violates this Fourth Amendment protection when the search either "infringes on a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space[.]" *United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) (emphasis in original). Thus, "a warrant is generally required before an officer may search or seize persons or property." *United States v. Warwick*, 928 F.3d 939, 943 (10th Cir. 2019) (citing *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973)). The warrant requirement also applies to mobile phones. *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017) (citing *Riley v. California*, 573 U.S. 373, 401 (2014)) (noting that "a warrant is generally required to search digital information on a cell phone"). And it applies to password-protected accounts. *See United States v. Andrus*, 483 F.3d 711, 719 (10th Cir. 2007) (analogizing password protections on computers to locked containers); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (holding that party had reasonable expectation of privacy in password-protected computer files).

Consent functions as one of the "'few specifically established and well-delineated exceptions'" to the warrant requirement. *Warwick*, 928 F.3d at 943 (quoting *Bustamonte*, 412 U.S. at 219). "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?" *Florida v. Jimeno*, 500

U.S. 248, 251 (1991) (citation omitted); *see also United States v. Kimoana*, 383 F.3d 1215, 1223 (10th Cir. 2004) (quoting *Jimeno* and applying objective reasonableness test to determine consent's scope). The scope of consent "'is a question of fact to be determined from the totality of the circumstances[.]'" *United States v. Nelson*, 868 F.3d 885, 893 (10th Cir. 2017) (quoting *United States v. Pena*, 920 F.2d 1509, 1514 (10th Cir. 1990)).

On the circumstances presented here, a reasonable person, the court finds, wouldn't understand consent to search a mobile phone to permit law enforcement to (1) reinstall an application on the phone; (2) generate a login code and send that login code to the phone; (3) open a text message containing that login code; and (4) use that login code to access and search data on a remote server. The agent here exceeded the scope of Mr. Castro's consent in two ways. *First*, he searched content that wasn't *on* Mr. Castro's phone but instead lived on remote servers. And *second*, he impersonated Mr. Castro to gain access to those remote servers before Mr. Castro consented to that impersonation.

*First*, TFO Albers exceeded the scope of consent by accessing content that wasn't on Mr. Castro's phone. Mr. Castro consented to a search of the content on his phone. SA Davis asked Mr. Castro: "Do you care if we take a look at it now? Would you consent to a search of *the phone* so we can take a look and make sure there's nothing *on there* that's concerning?" Doc. 18-1 (emphasis added). There was no child pornography—or other incriminating evidence—*on* Mr. Castro's phone. TFO Albers redownloaded an application and used that application to stream data to Mr. Castro's phone from a remote server. That data wasn't located on Mr. Castro's phone until the agent pulled the data through the phone by accessing a remote server. This process exceeded the scope of Mr. Castro's authorization for the agent to look at what was *on* his phone.

Unsurprisingly, the court could find no authority addressing the unique facts presented here. *See In re Cellular Tels.*, No. 14-MJ-8017-DJW, 2014 WL 7793690, at *4 (D. Kan. Dec. 30, 2014) ("With technological developments moving at such a rapid pace, Supreme Court precedent is and will inevitably continue to be absent with regard to many issues district courts encounter. As a result, an observable gap has arisen between the well-established rules lower courts *have* and the ones they *need* in the realm of technology." (emphasis in original)). But some courts have held that remotely accessible data isn't *on* the device used to access it.

For example, in *Bowers v. County of Taylor*, a sheriff's deputy sued his employer for violating his Fourth Amendment rights. 598 F. Supp. 3d 719, 722 (W.D. Wis. 2022). There, the plaintiff shared case files with crew members from a television show. *Id.* His employer hadn't authorized him to do so. *Id.* The employer instructed the IT director to access the deputy's Dropbox account. *Id.* The IT director was "able to do so because the Dropbox account was linked to [the deputy's] work email." *Id.* The IT director changed the Dropbox password and accessed the employee's Dropbox account, where she found the case files. *Id.* The employer argued that it hadn't violated the deputy's Fourth Amendment rights because the deputy had signed an IT policy containing the following provision: "I have no expectation of privacy for any material on Taylor County equipment, even if that material was generated for my personal use." *Id.* at 727–28. The court disagreed with the government's argument. *Id.* at 728. It found the policy inapplicable because "it's undisputed that [the deputy's] Dropbox account was stored on the cloud, not on county servers." *Id.* The court also noted that "the policy doesn't say that the county may access private accounts stored outside the county's computer system." *Id.*

*Bowers*—while not directly on point—is helpful. Here, Mr. Castro expressly consented to a search of his phone. So, like the deputy in *Bowers*, Mr. Castro forfeited any right to

challenge the search of content contained on his device. But Mr. Castro—like the deputy in *Bowers*—retained a reasonable expectation of privacy in accounts that weren't located on his phone but merely accessible through his phone. TFO Albers thus exceeded his authority to search in the same way that the employer in *Bowers* did—by accessing a cloud-based account.

In other cases, the FBI expressly has sought consent to search online accounts before doing so. *United States v. Sharp*, No. 14-CR-229-TCB, 2015 WL 4641537, at *2 (N.D. Ga. Aug. 4, 2015) (explaining that the FBI asked for consent to search a defendant's "laptop, email accounts, and Dropbox folder"); *see also United States v. Voice*, No. 21-CR-30059-RAL, 2022 WL 2162842, at *2 (D.S.D. Apr. 7, 2022) (explaining that FBI had secured a separate warrant for defendant's Facebook and Snapchat accounts after executing warrant to search phone). These cases, like *Bowers*, imply that a mobile phone is distinct from the cloud-based accounts that the phone can access. And they bolster the court's conclusion that Mr. Castro's consent to search his phone didn't provide consent to search his Telegram account.

*Second*, TFO Albers exceeded the scope of Mr. Castro's consent by impersonating Mr. Castro to access his Telegram account. The Ninth Circuit's decision in *United States v. Lopez-Cruz* is illustrative. 730 F.3d 803 (9th Cir. 2013). There, the defendant consented to a search of two cell phones. *Id.* at 806. A border patrol agent then took the phones out of the defendant's presence and answered three phone calls, the content of which incriminated the defendant. *Id.* The Ninth Circuit affirmed the district court's holding that "consent to search the phones did not extend to answering incoming calls." *Id.* at 810. The Ninth Circuit found it important that the agent impersonated the defendant. *Id.* ("An individual who gives consent to the search of his phone does not, without more, give consent to his impersonation by a government agent[.]"). Here, like the agent in *Lopez-Cruz*, TFO Albers exceeded the scope of consent by impersonating

Mr. Castro to install and gain access to Telegram's remote servers. Consent to search and "take a look" at what is *on* a phone isn't consent to use the phone to generate a unique passcode and then use that passcode to gain access to a remote cloud account.

*Bowers* also corroborates this proposition. The court there noted that there is a "well-established rule that individuals generally have a reasonable expectation of privacy in locked or closed containers, which are comparable to a password-protected account." *Bowers*, 598 F. Supp. 3d at 729 (first citing *United States v. Basinski*, 226 F.3d 829, 835 (7th Cir. 2000); and then citing *United States v. Neff*, 61 F.3d 906 (7th Cir. 1995)); *see also Andrus*, 483 F.3d at 719 (analogizing password protections on computers to locked containers). And as Mr. Castro's digital forensics expert testified at the evidentiary hearing, the code that TFO Albers generated was essentially a password to access Mr. Castro's Telegram account. So, Mr. Castro maintained a reasonable expectation of privacy in his Telegram account even after he had consented to a search of his phone. TFO Albers intruded on that reasonable expectation of privacy by impersonating Mr. Castro to generate and receive a passcode.

As the government notes, courts have held that consent to search a phone generally permits law enforcement to extract the phone's data and search it for deleted content. Doc. 26 at 10–12; Doc. 30 at 11–12. For example, in *United States v. Thurman*, the Seventh Circuit opined that a "reasonable person may be expected to know that recently deleted information can be reconstructed on a cell phone." 889 F.3d 356, 368 (7th Cir. 2018). It held that a defendant who knows the purpose of a search and consents—in unlimited terms—to a search of his phone authorizes the government to search deleted data and extract it forensically. *Id.* at 368–69. Likewise, the Fifth Circuit has held that a defendant's broad consent—coupled with the failure to limit it—authorizes the government to search and extract data from his phone. *United States v.*

*Gallegos-Espinal*, 970 F.3d 586, 588 (5th Cir. 2020). The Fifth Circuit also opined that the "typical reasonable owner of a cell phone . . . would understand that a 'complete' cell phone search refers not just to a physical examination of the phone, but further contemplates an inspection of the phone's 'complete' contents." *Id.* at 592; *see also United States v. Carron*, No. 22-CR-475-AGF, 2023 WL 2837785, at *7 (E.D. Mo. Apr. 7, 2023) (relying on *Thurman* and *Gallegos* and holding that "general, unqualified consent to search a cell phone permits officers to conduct a forensic examination of the cell phone").

But these cases differ from this one. They establish that consent to search a cell phone permits law enforcement to find and reconstruct deleted data on the phone. Here, Mr. Castro's phone contained no data—deleted or otherwise—that inculpated him. To the contrary, incriminating evidence came from a Telegram server. So, "[a] reasonable person may be expected to know that recently deleted information can be reconstructed on a cell phone." *Thurman*, 889 F.3d at 368. But that doesn't mean that a reasonable person should expect law enforcement—after receiving consent to search, limited to a phone—to reinstall an application on that mobile phone, impersonate the user to gain access to that application, and then stream data from a remote server with that application.

The government next argues that Mr. Castro's failure to revoke consent authorized TFO Albers's search of his Telegram account. Doc. 26 at 10–14. To be sure, Tenth Circuit cases "consistently and repeatedly have held a defendant's failure to limit the scope of a general authorization to search, and failure to object when the search exceeds what he later claims was a more limited consent, is an indication the search was within the scope of consent." *United States v. Gordon*, 173 F.3d 761, 766 (10th Cir. 1999). But here, the court finds, the government hasn't proved that Mr. Castro was aware of what TFO Albers was doing on his phone. TFO Albers

explained that he, SA Davis, and Mr. Castro were standing in a "semi-triangle" and that Mr. Castro wasn't looking over his shoulder. TFO Albers also was equivocal about whether Mr. Castro was looking at his phone while TFO Albers was searching it. What's more, Mr. Castro was talking with SA Davis while TFO Albers was searching his phone. So, the court finds that Mr. Castro wasn't sufficiently aware of the scope of TFO Albers's search to limit it. In sum, Mr. Castro's failure to object didn't amount to consent to search his Telegram account.

Finally, the government argues that our Circuit has been forgiving about the particularity requirement for search warrants in child pornography cases. Doc. 30 at 8–9 (citing *United States v. Grimmett*, 439 F.3d 1263, 1269–70 (10th Cir. 2006); *United States v. Campos*, 221 F.3d 1143, 1146–47 (10th Cir. 2000); *United States v. Simpson*, 152 F.3d 1241, 1248–51 (10th Cir. 1998); *United States v. Wagner*, 951 F.3d 1232, 1247 (10th Cir. 2020); further citations to out-of-circuit cases omitted). This argument fails. The standard for assessing the breadth of a warrant search differs from that of a consent search. *Lopez-Cruz*, 730 F.3d at 810 ("A search pursuant to a warrant is limited by the extent of probable cause on which the warrant is based. In contrast, a search pursuant to consent is limited by the extent of the consent given for the search by the individual." (internal quotation marks and citations omitted)). And none of the government's cases suggest that a warrant authorizing the search of a device also authorizes the search of any cloud-based account accessible from that device. *Cf. United States v. Palms*, 423 F. Supp. 3d 1254, 1258 (N.D. Okla. 2019), *aff'd*, 21 F.4th 689 (10th Cir. 2021) (noting that search warrant for a phone in a sex trafficking case separately authorized collection of cloud data from the phone); *Voice*, 2022 WL 2162842, at *2 (explaining that FBI had secured separate warrant for the defendant's Facebook and Snapchat accounts in child sexual abuse case after executing warrant to search phone). And for good reason: If a warrant authorizing the search of a phone

allowed the government to search any cloud-based account accessible through that phone, the warrant would likely violate the Fourth Amendment's particularity requirement. *See In re Cellular Tels.*, 2014 WL 7793690, at *11 (explaining purpose of that requirement "is to prevent general searches" and that an "unrestricted search [of a cell phone] is tantamount to requesting disclosure of a vast array of intimate details"). So, the court rejects the government's argument that it should construe the scope of Mr. Castro's consent liberally.

In sum, Mr. Castro consented to a search of his phone. And TFO Albers searched more than Mr. Castro's phone. He also used Mr. Castro's phone to reinstall an application, generate a login code for that application, and deploy that code to access and search a remote server. Those actions exceeded the scope given by Mr. Castro's consent. So, the search of Mr. Castro's Telegram account violated the Fourth Amendment.

**B. Inevitable Discovery**

The government argues that even if law enforcement officers illegally searched Mr. Castro's phone, the court shouldn't suppress the evidence because they inevitably would have discovered the same evidence lawfully. Doc. 26 at 14–17; Doc. 30 at 15–17. Ordinarily, "evidence obtained in violation of the Fourth Amendment will be suppressed under the exclusionary rule[.]" *United States v. Christy*, 739 F.3d 534, 540 (10th Cir. 2014). One exception to this rule is the inevitable discovery doctrine. *Id.* For this exception to apply, the government must prove "by a preponderance of the evidence that the evidence would have been discovered without the Fourth Amendment violation." *Id.* (citing *United States v. Cunningham*, 413 F.3d 1199, 1203 (10th Cir. 2005)). The issue, then, is whether the government would have lawfully discovered the evidence "'if no police error or misconduct had occurred.'" *United States v. O'Neil*, 62 F.4th 1281, 1291 (10th Cir. 2023) (quoting *Nix v. Williams*, 467 U.S. 431, 443 (1984)). This inquiry "'involves no speculative elements but focuses on demonstrated

historical facts capable of ready verification.'" *Id.* (quoting *Nix*, 467 U.S. at 444 n.5). Our Circuit is "very reluctant to apply the inevitable discovery exception in situations where the government fails to obtain a search warrant and no exception to the warrant requirement exists[.]" *United States v. Souza*, 223 F.3d 1197, 1206 (10th Cir. 2000).

The inevitable discovery doctrine applies only when the court finds that a warrant "would have—not could have—been issued" and law enforcement officers would have secured the evidence lawfully. *Christy*, 739 F.3d at 541–42, 543 n.5 (citing *Souza*, 223 F.3d at 1205). To aid this assessment, the court must consult the four *Souza* factors:

> "1) the extent to which the warrant process has been completed at the time those seeking the warrant learn of the search; 2) the strength of the showing of probable cause at the time the search occurred; 3) whether a warrant ultimately was obtained, albeit after the illegal entry; and 4) evidence that law enforcement agents 'jumped the gun' because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli."

*Id.* at 541 (quoting *Souza*, 223 F.3d at 1204). "Ultimately, the court must examine each contingency that would need to have been resolved in favor of the government and apply the inevitable discovery doctrine 'only when it has a high level of confidence' that the warrant would have been issued and the evidence obtained." *Id.* (citing *Souza*, 223 F.3d at 1205).[5] The court evaluates the government's inevitable discovery argument here by considering, first, *Souza* factors (1) and (3) together before addressing factor (2) and factor (4).

**1. Factors 1 and 3**

Factors (1) and (3) are especially important to the inevitable discovery analysis. *Christy*, 739 F.3d at 541. "Efforts to secure particular evidence through the warrant process provide direct evidence that, absent the unlawful conduct, 'a warrant would in fact have been issued' and

[5] Some of our Circuit's cases have described the test as requiring the court to have "no doubt that the police would have lawfully discovered the evidence later." *United States v. Romero*, 692 F.2d 699, 704 (10th Cir. 1982).

'the same evidence would have been discovered.'" *United States v. Harris*, 102 F. Supp. 3d 1187, 1198 (D. Kan. 2015) (quoting *Souza*, 223 F.3d at 1204).

Here, the government concedes, the FBI neither attempted to nor actually secured a warrant. Doc. 26 at 15. Mr. Castro argues that this void is dispositive. Doc. 29 at 15. It's not. Our Circuit has clarified that "an effort to [secure] a warrant is but one factor of the inevitable discovery doctrine[.]" *Christy*, 739 F.3d at 543. Again, the "ultimate question . . . is 'how likely it is that a warrant would have been issued' and the evidence found." *Id.* (quoting *Souza*, 223 F.3d at 1204). Still, the government here failed to engage in the warrant process altogether. So, the court is skeptical that a warrant would have delivered the evidence stored in Mr. Castro's Telegram account for two reasons it now explains.

*First*, TFO Albers was ambiguous about whether the FBI would have sought a warrant in *this* case. His testimony established that he "normally" seeks a warrant if he can't secure consent to search a phone. He didn't testify that he would have sought a warrant here. And regardless, accepting this after-the-fact testimony "contravenes the Supreme Court's command that 'inevitable discovery involves no speculative elements but focuses on demonstrated historical facts capable of ready verification or impeachment.'" *Harris*, 102 F. Supp. 3d 1187, 1198 (D. Kan. 2015) (quotation cleaned up) (quoting *Nix*, 467 U.S. at 444 n.5). The court thus concludes that TFO Albers's testimony is of no moment here.

*Second*, TFO Albers didn't testify that he would have sought a warrant to search Mr. Castro's Telegram account, even if he did seek a warrant to search Mr. Castro's phone. As noted above, it isn't clear that a warrant to search Mr. Castro's phone would have authorized the FBI to download and access Mr. Castro's Telegram account. *See In re Cellular Tels.*, 2014 WL 7793690, at *5 ("[D]oes a warrant authorizing the search of a cell phone also authorize the

search of data, *accessible via* the cell phone, but not actually *stored* there? If so, the potential for abuse becomes abundantly clear." (emphasis in original)). And as Mr. Castro notes, the forensic search of Mr. Castro's phone yielded no evidence of child pornography. Doc. 29 at 17. The FBI likely had probable cause to believe that the Telegram account contained evidence of a crime, as discussed below. So, the FBI could have sought a warrant separately to access Mr. Castro's Telegram account. But the government doesn't argue that it ever considered seeking such a warrant. Because the government can't prove that it ever initiated the process of seeking a warrant, these particularly important factors favor suppression.[6]

**2. Factor 2**

The second factor favors the government. This factor assesses the strength of probable cause at the time of the unlawful search. *Christy*, 739 F.3d at 541. The stronger the showing of probable cause, "the more probable that officers *could* have obtained a warrant." *Harris*, 102 F. Supp. 3d at 1199 (emphasis in original) (citing *Souza*, 223 F.3d at 1204). Here, the government had probable cause to believe that Mr. Castro's Telegram account contained incriminating evidence. FBI Milwaukee had learned that Galicia sent child pornography to Mr. Castro through Telegram. And FBI Milwaukee also learned that Mr. Castro had discussed plans to commit sexual assault against minor boys with Galicia through Telegram. This is more than enough to conclude that there was a "fair probability" that Mr. Castro's Telegram account contained evidence of a crime. *See United States v. Biglow*, 562 F.3d 1272, 1281 (10th Cir. 2009) (citing

[6] The government argues that this case is like *Christy*, where our Circuit found the inevitable discovery exception applied. Doc. 26 at 15 ("As in *Christy*, the government concedes that no warrant was applied for or obtained prior to the search of defendant's phone (*Souza* factors 1 and 3)."). But in *Christy*, the government secured a warrant after the illegal entry. 739 F.3d at 542. So, factor (3) favored the government there. The case for applying inevitable discovery thus was much stronger in *Christy* than here.

*Illinois v. Gates*, 462 U.S. 213, 238 (1983)) (explaining that probable cause exists when there is a "fair probability that contraband or other evidence will be found in a particular place").

So, the government possessed a strong basis for probable cause to believe that Mr. Castro's Telegram account contained evidence of a crime. But that isn't enough. *Christy*, 739 F.3d at 543 n.5 ("But we reiterate that probable cause on its own is not enough[.]"). *See also Harris*, 102 F. Supp. 3d at 1199 n.55 ("The strength of probable cause only indicates whether officers had sufficient ability to lawfully gain access to the evidence. It does not, like factors (1) and (3), support the conclusion that officers inevitably would have pursued that recourse."). So, while this factor favors applying inevitable discovery, it isn't dispositive of the issue. The court moves on, therefore, to evaluate the final *Souza* factor.

**3. Factor 4**

The fourth factor also favors the government. Recall that this factor assesses whether "'law enforcement agents "jumped the gun" because they lacked confidence in their showing of probable cause and wanted to force the issue by creating a fait accompli.'" *Christy*, 739 F.3d at 541 (quoting *Souza*, 223 F.3d at 1204). Here, the FBI didn't act because it feared insufficient probable cause. Instead, TRO Albers mistakenly believed that the scope of consent included the right to access Mr. Castro's Telegram account. When an officer mistakenly believes consent authorizes a search, district court cases in our Circuit have distinguished between the officer's mistake of law versus mistake of fact. When an officer's error is a mistake of law, this factor doesn't favor the government, even when the officer acted in good faith. *United States v. Troxel*, 564 F. Supp. 2d 1235, 1242 (D. Kan. 2008) ("This fourth factor cannot be said to be in favor of the Government when a mistake of law was the cause of the illegal search."); *see also Harris*, 102 F. Supp. 3d at 1201 (citing *Troxel*, 564 F. Supp. 2d at 1242) ("Because the search occurred as a result of an unreasonable mistake of law and not to create a fait accompli, the Court balances

this factor neither to favor nor to disfavor applying inevitable discovery.").[7] On the other hand, when an officer's error is a mistake of fact, this factor favors the government if the officer acted in good faith. *See United States v. Coleman*, 554 F. Supp. 3d 1124, 1154 (D.N.M. 2021) ("The reason federal agents did not get a warrant is that they believed they had valid consent to search the phones, not that they did not have probable cause. The fourth factor thus weighs in favor of the Government."). Here, the officer's erroneous belief that Mr. Castro consented to a search of his Telegram account was a mistake of fact. *See Nelson*, 868 F.3d at 893 (characterizing the scope of consent as a question of fact). TFO Albers acted in good faith when he searched Mr. Castro's Telegram account. This factor thus supports applying inevitable discovery.

**4. Totality**

Overall, the *Souza* factors yield a reasonably close call. Factors (1) and (3) favor suppression; factors (2) and (4) weigh against suppression. The court concludes that inevitable discovery doesn't apply here because the most important factors support suppression. And the court doesn't have a "high degree of confidence" that the FBI would have sought and secured a warrant that would authorize a search of Mr. Castro's Telegram account.

The government's position boils down to this: Probable cause was so clear here that the FBI inevitably would have pursued a warrant that would have uncovered child pornography on Mr. Castro's Telegram account. That's unavailing. Judge Melgren explained in *Harris*:

> To conclude, the Government argues as follows. Officers had probable cause. Although officers did not use this probable cause to apply for a warrant as required, they could have. And if they had applied, they probably would have received a warrant that led to discovering the seized evidence. So, in *this* case, the Court might as well retroactively validate their conduct and admit the evidence. The Court, however, cannot distinguish *this* case from *every* case where an officer can

[7] In both *Troxel* and *Harris*, the mistaken consent was based on an officer's erroneous belief that a third party had authority to consent to a search. *Harris*, 102 F. Supp. 3d at 1200–01; *Troxel*, 564 F. Supp. 2d at 1242.

> demonstrate probable cause. To accept probable cause alone is to probably cause the (inevitable discovery) exception to swallow the (warrant requirement) rule.

102 F. Supp. 3d at 1201 (emphasis and parentheses in original). The court agrees with Judge Melgren's reasoning. It thus concludes that inevitable discovery doesn't apply here. And the court addresses the government's other argued exception—the good faith exception—next.

**C. Good Faith**

The government contends that the court shouldn't suppress any fruits of the illegal search here because of the good faith exception. Doc. 30 at 17–19. Even if this exception applied, it wouldn't matter because the government raised it for the first time in its supplemental response brief. The government could have raised this argument in its initial response but didn't. What's more, it would prove "manifestly unfair" to Mr. Castro, who's had no occasion to respond to it. *United States v. Leffler*, 942 F.3d 1192, 1197 (10th Cir. 2019). *See also Kim v. Kettell*, 694 F. Supp. 3d 1379, 1395–96 (D. Colo. 2023) (refusing to evaluate an argument raised for the first time in a supplemental response when the party had four previous opportunities to raise it); *Bordertown, LLC v. AmGUARD Ins. Co.*, No. 22-cv-01683-REB-GPG, 2022 WL 17538186, at *2 (D. Colo. Oct. 5, 2022) (collecting cases to demonstrate courts in our Circuit routinely refuse to consider arguments presented only in a reply brief). Regardless, even had the government made the argument in a timely manner, the argument fails on the merits.

The good faith exception to the exclusionary rule dictates that "'even if a warrant is not supported by probable cause, evidence seized in good-faith reliance on that warrant is not subject to suppression.'" *United States v. Xiang*, 12 F.4th 1176, 1182 (10th Cir. 2021) (quoting *United States v. Knox*, 883 F.3d 1262, 1270 (10th Cir. 2018)). The government argues that the Supreme Court has expanded the good faith exception beyond search warrants. Doc. 30 at 18. That's true. *See Herring v. United States*, 555 U.S. 135 (2009) (applying good faith exception when

officers relied on rescinded arrest warrant); *Davis v. United States*, 564 U.S. 229 (2011) (applying good faith exception when officers relied on then-binding circuit court precedent); *Illinois v. Krull*, 480 U.S. 340 (1987) (applying good faith exception when officers relied on statute authorizing the search).

But none of these expansions are analogous to the illegal search here because they all involve good faith reliance on a third party's mistake. Our Circuit has instructed that "application of *Leon's* good-faith exception to the exclusionary rule turns to a great extent on whose mistake produces the Fourth Amendment violation." *United States v. Herrera*, 444 F.3d 1238, 1250 (10th Cir. 2006). The Tenth Circuit has never "extended *Leon* to a case where the officer's mistake, rather than that of a neutral third party, . . . resulted in a Fourth Amendment violation." *Id.* at 1251; *United States v. Cruz-Zamora*, 318 F. Supp. 3d 1264, 1271 (D. Kan. 2018) (explaining our Circuit doesn't apply good faith exception in cases involving officer's factual mistake). So, given that TRO Albers's mistake of fact about the scope of Mr. Castro's consent led to the unlawful search, the good faith exception doesn't apply. Because the search of Mr. Castro's Telegram account violated the Fourth Amendment—and because no exception to the exclusionary rule applies—the court grants Mr. Castro's request to suppress the evidence found in his Telegram account.

**D. Taint**

Finally, the government argues that the court shouldn't suppress evidence found in Mr. Castro's MEGA account. Doc. 30 at 13–15. It contends that Mr. Castro's separate consent to search that account authorized the government's search. *Id.* Mr. Castro responds, arguing that evidence found in his MEGA account is tainted. Doc. 29 at 11–13. He asserts that the government exploited its illegal search of his Telegram account to induce his consent. *Id.*

"Evidence will not be suppressed as fruit of the poisonous tree unless an unlawful search is *at least* the but-for cause of its discovery." *United States v. Chavira*, 467 F.3d 1286, 1291 (10th Cir. 2006) (emphasis in original) (citing *Hudson v. Michigan*, 547 U.S. 586, 592 (2006)). The defendant bears the initial burden to demonstrate a causal relationship between an unlawful search and the challenged evidence. *United States v. Nava-Ramirez*, 210 F.3d 1128, 1131 (10th Cir. 2000) ("At a minimum, a defendant must adduce evidence at the suppression hearing showing the evidence sought to be suppressed would not have come to light but for the government's unconstitutional conduct."); *United States v. Jarvi*, 537 F.3d 1256, 1260–61 (10th Cir. 2008) (explaining that burden is on defendant to establish, first, a causal connection between "a violation of his own Fourth Amendment rights and the discovery of the challenged evidence"). If the defendant makes that showing, the burden shifts to the government to prove that the challenged evidence is attenuated from the unlawful search. *Nava-Ramirez*, 210 F.3d at 1131.[8]

[8] There's a little ambiguity about the burden of proof in cases involving taint. Some of our Circuit's cases suggest that the burden is on the government to prove a break in the causal chain between the initial Fourth Amendment violation and discovery of the challenged evidence. *E.g.*, *United States v. Carter*, 360 F.3d 1235, 1243 (10th Cir. 2004) ("'When a consensual search is preceded by a Fourth Amendment violation, . . . the government must prove not only [1] the voluntariness of the consent under the totality of the circumstances, but the government must also establish [2] a break in the causal connection between the illegality and the evidence thereby obtained.'" (brackets and ellipses in original) (quoting *United States v. Melendez-Garcia*, 28 F.3d 1046, 1053 (10th Cir. 1994))); *United States v. Fox*, 600 F.3d 1253, 1259 (10th Cir. 2010) ("To demonstrate that the taint of an illegal seizure has dissipated, 'the government must prove, from the totality of the circumstances, a sufficient attenuation or break in the causal connection between the illegal detention and consent.'" (quoting *United States v. Gregory*, 79 F.3d 973, 979 (10th Cir. 1996))).

But the court concludes that these cases are expressing the standard having assumed the defendant already has made a threshold showing of a causal relationship between the Fourth Amendment violation and discovery of the challenged evidence. In those cases suggesting the burden is on the government, the initial causal connection between the Fourth Amendment violation and the challenged evidence was relatively clear. *Carter*, 360 F.3d at 1238–39 (police sought consent to search garage after illegally searching and discovering methamphetamine and weapons in it); *Fox*, 600 F.3d at 1256 (10th Cir. 2010) (police sought consent after unlawfully seizing woman); *Melendez-Garcia*, 28 F.3d at 1053 (police sought consent after illegally arresting man); *Gregory*, 79 F.3d at 979 (police sought consent after

The court denies Mr. Castro's request to suppress evidence from his MEGA account. Mr. Castro hasn't shouldered his initial burden; there is no causal relationship between the unlawful search of his Telegram account and his consent of the MEGA account search. But-for the illegal search, the government still would have requested permission to search Mr. Castro's MEGA account. After all, the government already knew Mr. Castro's username and password. And when they broached the subject of Mr. Castro's MEGA account with him, the FBI agents made no reference to the child pornography that they already had located from the unlawful search. That's significant because "the ultimate 'fruit of the poisonous tree' inquiry asks whether the challenged evidence 'has been come at by exploitation of [the] illegality or instead by means sufficiently distinguishable to be purged of the primary taint.'" *Nava-Ramirez*, 210 F.3d at 1131 n.1 (alteration in original) (quoting *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)). No exploitation of the unlawful search led to Mr. Castro consenting to the search of his MEGA account.

What's more, Mr. Castro volunteered permission to the agents to search his MEGA account before the FBI solicited his consent. His offer strongly suggests that Mr. Castro's consent to search his MEGA account was uncoerced and voluntary. *See United States v. Mendoza-Salgado*, 964 F.2d 993, 1012 (10th Cir. 1992) ("While her unsolicited consent does not end the inquiry, it weighs heavily into our conclusion that agents did not coerce Mrs. Garcia into signing the consent form."). It's possible that Mr. Castro felt cornered or powerless after the FBI found blatant evidence of criminality on his Telegram account. And it's possible that Mr. Castro

---

illegally seizing man). The court thus concludes that *Nava-Ramirez* and *Jarvi* correctly express that the threshold burden of establishing a causal connection between the Fourth Amendment violation and the challenged evidence rests with the defendant. Regardless, the court concludes that the government has proven by a preponderance of the evidence that the FBI's unlawful search of Mr. Castro's Telegram account didn't taint his subsequent consent authorizing the search of his MEGA account.

thus felt compelled to offer his MEGA account as soon as the FBI broached the subject. But possibility isn't enough. Mr. Castro adduced no evidence at the suppression hearing or otherwise that would allow the court to find, by a preponderance of the evidence, that the government's unlawful search of his Telegram account *caused* him to consent to the search of his MEGA account.[9]

Mr. Castro urges the court to engage in the *Wong Sun* taint analysis. Doc. 29 at 12. But even if Mr. Castro established a causal connection between the unlawful Telegram search and his consent, the court's conclusion wouldn't change. That is, the challenged evidence is attenuated from the unlawful search—and untainted—because the government didn't exploit the Telegram search to get Mr. Castro's consent. "When a consensual search follows a Fourth Amendment violation, the government must prove both (1) that the consent was voluntary under the totality of the circumstances, and (2) that there was 'a break in the causal connection between the illegality and the evidence thereby obtained.'" *Fox*, 600 F.3d at 1257 (quoting *Melendez-Garcia*, 28 F.3d at 1053). As already discussed, the court easily finds that Mr. Castro's consent was voluntary under the totality of the circumstances. Mr. Castro volunteered consent. And the entirety of the conversation between Mr. Castro and the FBI agents was calm and cordial. Under the totality of the circumstances, Mr. Castro's consent to search his MEGA account thus was free and voluntary.

And even assuming a causal connection, that connection breaks. To assess a break in the causal chain, the Supreme Court has articulated three relevant factors: (1) the "'temporal proximity'" between the unlawful activity and discovery of the challenged evidence; (2) "'the presence of intervening circumstances'"; and (3) "'the purpose and flagrancy of the official

[9] The issue of Mr. Castro's consent to search his MEGA account was barely addressed at the suppression hearing.

misconduct.'" *Utah v. Strieff*, 579 U.S. 232, 239 (2016) (quoting *Brown v. Illinois*, 422 U.S. 590, 603–04 (1975)). Here, the unlawful search occurred close in time to Mr. Castro's consent. And there were no intervening circumstances.[10]

But the third factor—which is particularly important—favors finding attenuation. *See id*. The attenuation doctrine favors "exclusion only when the police misconduct is most in need of deterrence[.]" *Id.* at 241. TFO Albers acted in good faith; his illegal search was neither flagrant nor purposeful. Ultimately, the *Strieff* factors are relatively balanced. But what's most significant is that there is no "evidence of coercion or exploitation of the alleged entry." *United States v. Lowe*, 999 F.2d 448, 451 & n.6 (10th Cir. 1993) (declining to suppress evidence when the first two factors supported suppression because the record was "devoid of *any* evidence of coercion or exploitation" of the Fourth Amendment violation (emphasis in original)). So, the court concludes it shouldn't suppress the evidence from Mr. Castro's MEGA account because the government's illegal search of Mr. Castro's Telegram account didn't taint his consent.[11]

## III. Conclusion

The court thus grants Mr. Castro's Motion to Suppress, in part. The court will suppress evidence discovered in Mr. Castro's Telegram account. The FBI exceeded the scope of Mr.

---

[10] Mr. Castro's consent to have his MEGA account added to the "Consent to Assume Online Identity Authorization Form" wasn't an intervening circumstance contemplated by the second factor. In *Fox*, our Circuit clarified that consent alone can't be the intervening event that purges the taint of an illegal search. 600 F.3d at 1260 ("The district court clearly erred in suggesting that Ms. Chiles's voluntary consent itself was an intervening circumstance. Her consent is not in itself an intervening event which could remove the taint of the prior illegal seizure."). Providing and explaining a consent form can contribute to purging the taint of an illegal search. *Mendoza-Salgado*, 964 F.2d at 1012–13. But here, Mr. Castro already had signed the form before any discussion of MEGA began.

[11] The government doesn't argue that the signed consent form salvages the unlawful search of Mr. Castro's Telegram account. Nor could it. Our Circuit's precedent establishes that subsequent consent alone can't purge the taint of a prior illegal search. *Fox*, 600 F.3d at 1261 n.6 (citing *United States v. Santa*, 236 F.3d 662, 678 (11th Cir. 2000)); *United States v. Colbert*, No. CR 21-1221 JB, 2023 WL 5672694, at *82 (D.N.M. Sept. 1, 2023) (citing *Fox*, 600 F.3d at 1261 n.6) ("A consent form which a suspect signs only after officers have begun the search does not constitute an intervening circumstance.").

Castro's consent when it discovered that evidence. And neither inevitable discovery nor the good faith exception prevents the exclusionary rule from applying. But the court denies Mr. Castro's request to suppress evidence found in his MEGA account. Mr. Castro voluntarily consented to that search, and his consent wasn't caused by the unlawful search of his Telegram account.

**IT IS THEREFORE ORDERED BY THE COURT THAT** Mr. Castro's Motion to Suppress (Doc. 18) is granted in part and denied in part. The court grants Mr. Castro's request to suppress evidence found in his Telegram account. But the court denies Mr. Castro's request to suppress evidence found in his MEGA account.

**IT IS SO ORDERED.**

**Dated this 29th day of August, 2024, at Kansas City, Kansas.**

**s/ Daniel D. Crabtree**
**Daniel D. Crabtree**
**United States District Judge**