

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

UNITED STATES OF AMERICA)

v.)

NATHANIEL CHASTAIN,)

Defendant.)

No. 22-cr-305 (JMF)

**REPLY MEMORANDUM OF LAW IN SUPPORT OF NATHANIEL CHASTAIN'S
MOTION TO SUPPRESS STATEMENTS AND EVIDENCE**

David I. Miller
Gregory W. Kehoe
Charles J. Berk
GREENBERG TRAURIG, LLP
One Vanderbilt Avenue
New York, NY 10017
(212) 801-9200

*Counsel for Defendant
Nathaniel Chastain*

TABLE OF CONTENTS

PRELIMINARY STATEMENT 1

ARGUMENT 2

 I. The Defendant Was Subjected to a Custodial Interrogation..... 2

 II. The Digital Contents of the Defendant’s Cell Phone Should Be
 Suppressed as the Unlawful Fruits of a Fifth Amendment Violation..... 5

 III. The Government Acted Outside the Scope of the Search Warrant 7

 IV. Discovery of the Contents of the
 Defendant’s Cell Phone Was Not Inevitable 9

 V. Should the Court Not Grant the Defendant’s Motion to
 Suppress Summarily, It Should Order an Evidentiary Hearing..... 10

CONCLUSION..... 10

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Orozco v. Texas</i> , 394 U.S. 324 (1969).....	2
<i>Rhode Island v. Innis</i> , 446 U.S. 291 (1980).....	4
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	5
<i>United States v. Anderson</i> , 929 F.2d 96 (2d Cir. 1991).....	6, 7
<i>United States v. Booker</i> , 561 F. Supp. 3d 924 (S.D. Cal. 2021).....	10
<i>United States v. Butt</i> , No. 18-CR-00087 (NSR), 2019 WL 479117 (S.D.N.Y. 2019)	3
<i>United States v. Craighead</i> , 539 F.3d 1073 (9th Cir. 2008)	2, 3
<i>United States v. Djibo</i> , 151 F. Supp. 3d 297 (E.D.N.Y. 2015)	3, 5, 6, 10
<i>United States v. Gladden</i> , 394 F. Supp. 3d 465 (S.D.N.Y. 2019).....	9
<i>United States v. Grant</i> , No. 07 Cr. 1119 (CM), 2008 WL 2971781 (S.D.N.Y. Aug. 1, 2008)	6
<i>United States v. Haygood</i> , 157 F. App'x 448 (2d Cir. 2005)	6
<i>United States v. McCoy</i> , 407 F. App'x 514 (2d Cir. 2010)	6
<i>United States v. Newton</i> , 369 F.3d 659 (2d Cir. 2004).....	2, 3
<i>United States v. Patane</i> , 542 U.S. 630 (2004).....	5
<i>United States v. Rodriguez-Garcia</i> , 983 F.2d 1563 (10th Cir. 1993)	5
<i>United States v. Sharma</i> , No. 18 Cr. 340 (LGS), 2019 WL 3802223 (S.D.N.Y. Aug. 13, 2019).....	6

United States v. Voustianiouk,
685 F.3d 206 (2d Cir. 2012).....7

United States v. Wilson,
914 F. Supp. 2d 550 (S.D.N.Y. 2012).....6

PRELIMINARY STATEMENT

In his Memorandum of Law in Support of his Motion to Suppress Statements and Evidence (ECF No. 28),¹ the defendant Nathaniel Chastain (the “Defendant”) demonstrated: (i) that all of his un-*Mirandized* statements, which were elicited by agents of the Federal Bureau of Investigation (“FBI”) during the course of a search warrant execution inside his small studio apartment, should be suppressed because they were illegally obtained during the course of a custodial interrogation; and (ii) that the digital contents of his cell phone, which were accessed through the use of an illegally-obtained statement regarding his cell phone password, should be suppressed as the unlawful fruits of a Fourth and/or Fifth Amendment violation.

The government’s opposition to the Defendant’s Motion to Suppress (ECF No. 34)² falls woefully short in its attempt to support the constitutionality of the agents’ actions. First, in failing to consider the totality of the circumstances during the course of the relevant search, the government erroneously contends that the Defendant’s statements, including the statement regarding his cell phone password, should not be suppressed because he was never subjected to a custodial interrogation—when he clearly was. Next, the government inaccurately insists that the digital contents of the Defendant’s cell phone—which were ultimately accessed using the Defendant’s illegally-obtained password—are not suppressible because they are, at best, the fruits of a *Miranda* violation. And finally, ignoring the language of its search warrant application, and the technical restrictions on the phone itself, the government wrongly contends that it did not act outside the scope of the relevant search warrant in seizing the cell phone’s contents, but that even if it did, the contents should not be suppressed because they would have been inevitably discovered.

¹ Hereinafter referred to as “Motion to Suppress” and cited as “Mot. to Supp.”

² Hereinafter cited as “Gov. Opp.”

For all the reasons set forth in the Motion to Suppress and herein, the government is wrong, and the Defendant's motion should be granted.

ARGUMENT

I. The Defendant Was Subjected to a Custodial Interrogation

In his Motion to Suppress, the Defendant demonstrated the government's failure to advise the Defendant of his *Miranda* rights should result in the suppression of any unwarned and illegally-obtained statements. The government, of course, cannot dispute that the agents failed to inform the Defendant of his *Miranda* rights before questioning him, but attempts to justify its error by arguing that the Defendant's statements were not the product of custodial interrogation. The government's arguments fail to move the needle.

First, the Defendant established that he was in custody during the execution of the search warrant because a reasonable person standing in the Defendant's shoes: (i) would not have "thought he was free to leave the police encounter"; and (ii) "would have understood his freedom of action to have been curtailed to a degree associated with a formal arrest."³ Notably, instead of supporting its opposition with documentary evidence to the contrary, the government attempts to reframe the narrative of the search by supplementing its own characterizations and facts to the Defendant's Declaration.⁴ But when stripped of the excess, the government's opposition is devoid of sufficient information to justify its erroneous conclusion that the Defendant was not in custody when the warrant was executed.

Specifically, the government argues that the Defendant was not in custody because: (i) the search took place in the "familiar surroundings" of the Defendant's home;⁵ (ii) the nature of the

³ See *United States v. Newton*, 369 F.3d 659, 672 (2d Cir. 2004) (citations omitted).

⁴ See Gov. Opp. at 5-12.

⁵ The location of a search is not dispositive in a custody analysis. Indeed, an individual's home—and in this case, the Defendant's small studio apartment—is capable of becoming a "custodial setting" in a police-dominated environment. See, e.g., *Orozco v. Texas*, 394 U.S. 324, 325-27 (1969); *Newton*, 369 F.3d at 677; *United States v. Craighead*, 539

questions asked of the Defendant would have assured him that he was not under arrest;⁶ and (iii) the Defendant's Declaration failed to allege a laundry list of additional factors bearing on the custodial determination.⁷ The government's argument highlights its own failure to recognize that any custody analysis requires the Court to examine the totality of the circumstances—not just particular factors—underlying the associated police encounter.⁸

Here, the relevant circumstances⁹ weigh in favor of a finding that the Defendant was in custody when the FBI agents asked him for the passcode to his cell phone. Indeed, no reasonable person would have felt free to leave an analogous encounter in which several FBI agents demanded entry into their home in the early hours of the morning, wearing bullet proof vests, carrying holstered firearms, and presenting them with a warrant that authorized a search of their person.¹⁰ Moreover, it strains credulity to conclude that any reasonable person would believe that the instant set of circumstances was not akin to that of a formal arrest when several FBI agents, in addition to the factors set forth above, confined the Defendant to his bed for an extended period of time, in an exceedingly small apartment (approximately 500 square feet), without telling him that he was not under arrest, that he did not need to answer questions, and that he was free to leave.¹¹

Second, the Defendant established that he was interrogated during the course of the search, as the totality of the circumstances demonstrate that the words and actions of the agents were

F.3d 1073, 1082-89 (9th Cir. 2008); *United States v. Butt*, No. 18-CR-00087 (NSR), 2019 WL 479117, at *14-18 (S.D.N.Y. 2019).

⁶ The nature of the questions is also not dispositive in a custody analysis. And indeed, the government here fails to consider that the *Djibo* defendant was found to be in custody when he was asked to provide his cell phone password. *See United States v. Djibo*, 151 F. Supp. 3d 297, 306 (E.D.N.Y. 2015).

⁷ By way of example, the government faults the Defendant for failing to declare that he was at the mercy of the police such that the situation was akin to a formal arrest. *See Gov. Opp.* at 8. The relevant inquiry, however, is whether the objective circumstances of the encounter would have led a reasonable person to believe that his freedom of action was “curtailed to a degree associated with a formal arrest.” *See Newton*, 369 F.3d at 671-72.

⁸ *See Butt*, 2019 WL 479117, at *12 (noting that “all factors must be weighed, and no one factor is dispositive”).

⁹ That is to say, the only circumstances placed before this Court in a declaration.

¹⁰ *See Mot. to Supp.* at 6-9.

¹¹ *See id.*

“reasonably likely to elicit an incriminating response.”¹² Indeed, the agents should have known, at the very least, that their request for the Defendant’s password was reasonably likely to elicit an incriminating response because the search warrant affidavit explicitly stated that the government was not seeking authority to compel the Defendant to provide his password, an implicit acknowledgment that it would be unconstitutional to do so in the first instance.¹³

The government, in opposition, fails to address the Defendant’s arguments. Instead, the government insists that the request for the Defendant’s password, under the circumstances of this case, was not an interrogation because the password itself was not incriminating in nature.¹⁴ In drawing out the government’s reasoning to its logical conclusion, however, the government necessarily suggests that all passwords are rarely, if ever, subject to Fifth Amendment protections. Not so. As discussed in the Defendant’s Motion to Suppress, several courts have addressed this issue and determined that a defendant cannot be compelled to provide his or her password to the government because such information is, in fact, constitutionally protected.¹⁵

Next, the government confusingly argues that the agents’ request for the Defendant’s cell phone password did not amount to an interrogation because a mere request for a consent to search does not constitute an interrogation within the meaning of *Miranda*.¹⁶ Indeed, according to the government, because a request for a consent to search is not an interrogation, and because a request for consent to search is often followed by a request for a password, the two requests are virtually indistinguishable. Again, not so. Here, putting aside the fact that the government’s analogy is

¹² *Rhode Island v. Innis*, 446 U.S. 291, 300-01 (1980); *see also* Mot. to Supp. at 9-12.

¹³ *See* Mot. to Supp. at 9-12. Of course, the agents also should have known that they impermissibly interrogated the Defendant after the Defendant spoke to his attorney and informed them that he was not required to provide his cell phone password. *See id.*

¹⁴ According to the government, the password “ha[d] no value” as “just a series of numbers.” Gov. Opp at 10-11.

¹⁵ *See* Mot. to Supp. at 11-12 n.6. It also bears noting that if cell phone passwords were not protected by the Fifth Amendment, then the government presumably would have included language in its warrant authorizing the FBI to compel the Defendant to enter a password into his phone. That the government did not do so here speaks volumes.

¹⁶ *See* Gov. Opp at 12.

irrelevant because the agents never asked the Defendant if he would consent to the search of his devices, the government fails to recognize that a consent to search does not fall within the ambit of the Fifth Amendment because it does not elicit evidence of a testimonial nature,¹⁷ whereas the request for a cell phone password does.¹⁸ Accordingly, and in sum, this Court should find that the Defendant was subjected to a custodial interrogation during the execution of the search warrant.

II. The Digital Contents of the Defendant’s Cell Phone Should Be Suppressed as the Unlawful Fruits of a Fifth Amendment Violation

As demonstrated in the Defendant’s Motion to Suppress, the discovery of the entire digital contents of his cell phone—through the use of the Defendant’s un-*Mirandized* and involuntary statement regarding his cell phone password—should be suppressed. Indeed, as previously discussed, the circumstances underlying this case are analogous to *United States v. Djibo*, 151 F. Supp. 3d 297 (E.D.N.Y. 2015), and suppression is warranted because: (i) the defendant’s statement regarding his cell phone password necessarily invoked the Fourth and Fifth Amendments;¹⁹ (ii) the search of the cell phone at issue implicated significant privacy concerns;²⁰ and (iii) there exists significant incentive to deter police misconduct.²¹ Moreover, unlike the Supreme Court’s decision in *United States v. Patane*, the Defendant here did not voluntarily consent to the search at issue.²²

In response, the government argues that: (i) “a *Miranda* violation cannot justify suppressing [the digital contents of the Defendant’s cell phone]”; and (ii) “the fact of a *Miranda*

¹⁷ See *United States v. Rodriguez-Garcia*, 983 F.2d 1563, 1568 (10th Cir. 1993) (finding that consent to search is not evidence of a testimonial or communicative nature) (internal quotation marks omitted).

¹⁸ See Mot. to Supp. at 11-12 n.6. Even assuming, *arguendo*, that the Defendant initially consented to the search of his cell phone when he provided his password to the agents, the Defendant revoked consent after he spoke to his attorney and informed the agents that he was not required to divulge that information.

¹⁹ See *infra* at Section III (discussing Fourth Amendment violation); Mot. to Supp. at 14-16 (same).

²⁰ See *Riley v. California*, 573 U.S. 373, 394 (2014) (“The sum of an individual’s private life can be reconstructed through [the digital contents of their cell phone]”).

²¹ See Mot. to Supp. at 13-14 (noting that the government should not be permitted to advance the idea that it is narrowing the scope of its warrant and then execute the warrant outside of that defined scope).

²² See *id.* at 13 n.8.

violation does not mean there was a violation of the Fifth Amendment because the Defendant was not compelled to divulge his Password.”²³ As to its first argument, the government fails to address that the cases it cites do not implicate the same litany of concerns articulated by the *Djibo* court.²⁴ Indeed, none of the cases involve parallel Fourth Amendment issues relating to the execution of a search warrant; the enhanced privacy interests involved in searching an individual’s cell phone; and any pressing concern to deter police misconduct.

Presumably aware of this disconnect, the government tries to distinguish *Djibo* by noting that the court there relied on the initial warrantless search of the defendant’s phone—*i.e.*, a purported Fourth Amendment violation—to conclude that the information obtained from the subsequently-obtained search warrant qualified as a fruit of the poisonous tree and was therefore subject to suppression.²⁵ But the *Djibo* court suppressed the cell phone data not only because of the intervening warrantless search, but also because the phone was accessed using an illegally-obtained password.²⁶ Consequently, the court’s reasoning in *Djibo* holds firm and applies in equal measure to this case.

As to the government’s second argument, the Defendant did not voluntarily provide his cell phone password to the agents.²⁷ As previously discussed, the Defendant’s statement regarding

²³ See Gov. Opp. at 13.

²⁴ See *United States v. McCoy*, 407 F. App’x 514, 515-16 (2d Cir. 2010) (defendant voluntarily consented to search of his home where gun was recovered); *United States v. Haygood*, 157 F. App’x 448, 449-50 (2d Cir. 2005) (finding search warrant lawfully obtained based, in part, on pedigree information—namely, an address—provided by defendant and finding gun recovered during execution admissible); *United States v. Sharma*, No. 18 Cr. 340 (LGS), 2019 WL 3802223, *7-9 (S.D.N.Y. Aug. 13, 2019) (defendant provided implied consent to search by voluntarily offering that he wanted to cooperate and that there was a gun in his bedroom); *United States v. Wilson*, 914 F. Supp. 2d 550, 565-67 (S.D.N.Y. 2012) (defendant gave implied consent to search by voluntarily indicating location of firearm in bedroom); *United States v. Grant*, No. 07 Cr. 1119 (CM), 2008 WL 2971781, at *5-8 (S.D.N.Y. Aug. 1, 2008) (finding defendant voluntarily consented to search for gun in his bedroom and finding drugs found in kitchen cabinet admissible).

²⁵ See Gov. Opp at 15-16.

²⁶ See *Djibo*, 151 F. Supp. 3d at 303-04, 310.

²⁷ See *United States v. Anderson*, 929 F.2d 96, 99 (2d Cir. 1991). A statement is not voluntary when it was obtained under circumstances that overbore the defendant’s will at the time it was given. *Id.* Such a determination requires a consideration of the totality of the circumstances, including “the accused’s characteristics, the conditions of the

his cell phone password cannot be deemed voluntary when he was, *inter alia*, isolated in his small studio apartment and never told that he was free to leave, while several armed agents overran his personal space and interrogated him about one of the devices that was a subject of the warrant.²⁸ Accordingly, the totality of the circumstances necessitates a finding that the Defendant's statements—including the statement about his cell phone password—were not voluntarily provided during the course of the search warrant execution.

III. The Government Acted Outside the Scope of the Search Warrant

As discussed in his Motion to Suppress, and as the government does not dispute, the Defendant has a reasonable expectation of privacy in the digital contents of his cell phone. Accordingly, the government was not only required to obtain a search warrant before attempting to retrieve the digital contents stored on the Defendant's cell phone, but was also required to abide by the terms and limitations of any warrant authorizing such a search: a search will be deemed to have violated the Fourth Amendment when agents executing the warrant "exceed[] the authority that they had been granted by the magistrate judge."²⁹ Such was the case here.

In his Motion to Suppress, the Defendant sufficiently demonstrated that the terms and limitations of the relevant search warrant were clear.³⁰ And indeed, the government cannot avoid the fact that the search warrant affidavit specifically stated that the government was not seeking authorization to compel the Defendant to provide the password to his cell phone.³¹ Consequently, the government argues predictably that: (i) the agents complied with the terms and limitations of the warrant; and (ii) wholesale suppression is inappropriate where the agents, acting in good faith,

interrogation, and the conduct of law enforcement officials." *Id.* Additional relevant factors may include whether the agent's statements were false, misleading, or intended to trick and cajole a defendant into confessing. *Id.*

²⁸ See *infra* at Section I.

²⁹ *United States v. Voustianiouk*, 685 F.3d 206, 212 (2d Cir. 2012) (citation omitted).

³⁰ See Mot. to Supp. at 14-16 (noting the search warrant affidavit provided that the government was not seeking authorization to compel the Defendant to provide the password to his phone).

³¹ See *id.* at 16.

did not effect a widespread seizure of items outside the warrant's scope.³² The government is wrong.

First, in asserting that the agents complied with the terms of the warrant, the government attempts to justify the agents' actions after the fact by noting that the language of the search warrant affidavit merely prevented the agents from *compelling* the Defendant to provide his password. And, according to the government, the agents never legally *compelled* the Defendant to provide anything.³³ This argument is baseless. The clear and practical import of the language contained within the search warrant affidavit is that the agents would not ask the Defendant for his password in the first instance. By doing so, they acted outside the scope of the warrant and the material seized should be suppressed.³⁴

Next, the Defendant does not dispute that wholesale suppression of all evidence seized pursuant to a search warrant is only appropriate under certain circumstances.³⁵ And while the Defendant believes that the Court could find those circumstances present here—where the government “flagrantly” disregarded the terms of the warrant—in lieu of wholesale suppression of *all* evidence seized pursuant to the warrant, the Court should suppress the evidence obtained outside of the warrant's scope.³⁶ Here, the agents were not authorized to compel the Defendant to provide the cell phone password. Accordingly, the limited evidence obtained in direct violation

³² See Gov. Opp. at 18-19.

³³ See *id.*

³⁴ In a footnote, the government suggests, without any supporting legal citation, that it could have compelled the production of the Defendant's passcode through the use of a grand jury subpoena. For reasons already discussed *supra*, the Defendant submits that the government would not have had such authority because cell phone passcodes are protected by the Fifth Amendment.

³⁵ See Mot. to Supp. at 15 (noting that wholesale suppression is appropriate when the government “flagrantly” disregards the terms of the warrant and (i) effects a widespread seizure of items not within the scope of the warrant and (ii) does not execute the warrant in good faith) (citations omitted).

³⁶ See *id.* at 16.

of that authority (and the Fourth Amendment)—*i.e.*, the digital contents of the Defendant’s cell phone—should be suppressed.

IV. Discovery of the Contents of the Defendant’s Cell Phone Was Not Inevitable

The government finally argues that even if this Court were to conclude that the Defendant’s Fourth or Fifth Amendment rights were violated, suppression of the data seized from the Defendant’s cell phone is not warranted because the data inevitably would have been discovered without the Defendant’s password. To prevail under the inevitable discovery doctrine, the government must “prove that each event leading to the discovery of the evidence would have occurred with a sufficiently high degree of confidence for the district judge to conclude, by a preponderance of the evidence, that the evidence inevitably would have been discovered.”³⁷ The government’s conclusory assertions in opposition, of course, cannot give rise to such a finding.

First, the government insists that it would have inevitably accessed the digital contents on the Defendant’s cell phone because the cell phone itself “had the ‘FaceID’ features enabled.”³⁸ To the best of the Defendant’s recollection, however, and as set forth in his Declaration, the Defendant does not believe that his cell phone was accessible through the use of biometrics at the time the search warrant was executed.³⁹ Second, although the government insists that the inevitable discovery doctrine would also apply because the FBI agents recovered, and would have been able to deliver, the cell phone in a “warm” state,⁴⁰ the Defendant fails to see how the government could prove—over one year after the cell phone was initially seized and accessed by the government using an illegally-obtained password—that the phone was actually delivered in such a state at any

³⁷ *United States v. Gladden*, 394 F. Supp. 3d 465, 484 (S.D.N.Y. 2019) (internal quotation marks and citations omitted).

³⁸ See Gov. Opp. at 20.

³⁹ See Mot. to Supp. at 4-5.

⁴⁰ See Gov. Opp. at 20.

Court-ordered evidentiary hearing. Third, the government concludes, without any supporting affidavit from an FBI agent qualified to extract data from cell phones, that it also would have accessed the contents of the Defendant's cell phone using a software program to crack the password.⁴¹ Notably, courts have rejected similar arguments under circumstances in which the government was incapable of demonstrating that cracking a password was inevitable.⁴² Accordingly, the government's conclusory arguments regarding the inevitable discovery of the contents of the Defendant's cell phone should be rejected.

V. Should the Court Not Grant the Defendant's Motion to Suppress Summarily, It Should Order an Evidentiary Hearing

The Defendant respectfully submits that he has sufficiently demonstrated a violation of his constitutional rights. As discussed in the Motion to Suppress, should the Court determine that additional information is needed, it should order an evidentiary hearing.

CONCLUSION

For the aforementioned reasons and for the reasons described in the Motion to Suppress, the Court should grant the instant motion in its entirety.

Dated: New York, New York
October 21, 2022

Respectfully submitted,
GREENBERG TRAURIG, LLP
By: /s/ David I. Miller
David I. Miller
Gregory W. Kehoe
Charles J. Berk
One Vanderbilt Avenue
New York, NY 10017
(t) (212) 801-9200; (f) (212) 801-6400
Counsel for Defendant
Nathaniel Chastain

⁴¹ See *id.* at 21.

⁴² See, e.g., *Djibo*, 151 F. Supp. 3d at 303-04, 310-11; *United States v. Booker*, 561 F. Supp. 3d 924, 932-35 (S.D. Cal. 2021).