*NOTE: MOTION DRAFTED IN NINTH CIRCUIT AND RELIES ON NINTH CIRCUIT CASES AND PRECEDENT.

I. The warrantless searches of CLIENT's cell phone violate the Fourth Amendment, and the resulting evidence must be suppressed.

A. The warrant requirement and exceptions.

The Fourth Amendment protects an individual's "person[], houses, papers, and effects" against "unreasonable searches and seizures." U.S. CONST. AMEND. IV. The "ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). And "reasonableness generally requires the obtaining of a judicial warrant" by law enforcement agents seeking to conduct a search to discover evidence of criminal wrongdoing. *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (quoting *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)).

Absent a warrant, a search is "*per se*" unreasonable unless it fits within "a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967). One such exception is for border searches, which "are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). This is because in a routine border search, the government's interest in "national self-protection" is strong, whereas the privacy interest that a "[t]raveler" may have in "identify[ing] himself as entitled to come in, and [in] his belongings as effects which may lawfully be brought in," is relatively weak. *Carroll v. United States*, 267 U.S. 132, 143 (1925). Still, reasonableness remains the touchstone. *See Ramsey*, 431 U.S. at 621. Therefore, the balance of interests may change when a border search is potentially destructive, highly intrusive, or particularly offensive. *See United States v. Flores-Montano*, 541 U.S. 149, 154 n.2 (2004) (observing that particularly offensive searches, including destructive searches of property, may be unreasonable under the Fourth Amendment); *see also United States v. Seljan*, 547 F.3d 993, 1000 (9th Cir. 2008) (acknowledging that some searches "are so intrusive, destructive, or offensive that they would be deemed unreasonable under the Fourth Amendment").

Under such circumstances, the search may be deemed unreasonable. *See Ramsey*, 431 U.S. at 618 n.13.

Another exception to the warrant requirement exists when agents conduct a search incident to arrest. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009). The Supreme Court in *Riley* established a bright-line rule that law enforcement agents may not conduct even a minimally intrusive search of a smart phone incident to arrest. 134 S. Ct. at 2494-95. This is because smart phones are effectively "minicomputers" that "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Id.* In other words, the Court held that the privacy interests at issue in a search of digital data are "vast." *Id.* at 2485. At the same time, the government's interest in protecting officers and evidence are negligible. *See id.* at 2485. Accordingly, the Court offered a "simple . . . answer to the question of what police must do before searching a cell phone seized incident to an arrest[:] get a warrant." *Id.* at 2495.

Riley signals a new era in applying the Fourth Amendment to searches of electronic media. But the case law on whether border searches of electronic media are reasonable is still evolving. This Court has held that a forensic search of electronic media is not a routine border search and so requires reasonable suspicion. *See United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) (en banc). *Cotterman*, however, was decided before *Riley*. It therefore did not address whether the *Riley* rationale for barring smart-phone searches in the context of a search incident to arrest exception applies with equal force in the context of a border search. Although other courts have held that the *Riley* rule does apply to border searches, *see, e.g., United States v. Kim*, 103 F. Supp. 3d 32, 55-56 (D.D.C. 2015), that remains an open question in this Court. Likewise, this Court has not resolved whether a highly intrusive and destructive search and seizure of a smart phone at the border violates the Fourth Amendment reasonableness requirement.

B. This Court should suppress under *Riley* because the government's search for incriminating evidence on cell phone necessarily is *not* a border search.

The government will likely seek to justify its warrantless manual and forensic searches of CLIENT'S cell phone under the border-search doctrine. But the objective circumstances show that the searches had nothing to do with identifying contraband on CLIENT'S phone. Instead, the searches were aimed at uncovering evidence against CLIENT for his prosecution. Because the searches were not limited in scope to the purposes for which the border-search exception was created, they were not valid border searches.

1. The border search is a narrow exception to the warrant requirement.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend IV. "[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967).

One such exception is a search incident to arrest. *See Riley*, 134 S.Ct. at 2482. In light of the "vast quantities of personal information" contained on modern digital devices, however, that exception is inapplicable to cell phones. *Id.* at 2485. Therefore, "before searching a cell phone incident to an arrest[,]" "police must . . . get a warrant." *Id.* at 2495.

Border searches are another exception to the warrant requirement. *See United States v. Seljan*, 547 F.3d 993, 999 (9th Cir. 2008) (en banc). "[T]he phrase 'border search' does not appear in . . . the Constitution." *United States v. Weil*, 432 F.2d 1320, 1323 (9th Cir. 1970). Rather, it is "the courts' shorthand way of defining the limitation the Fourth Amendment imposes upon the right of customs agents to search without probable cause." *Id.*

The scope of the border-search exception is "narrow." *Cotterman*, 709 F.3d at 956. Its purpose is "to identify the illegal transportation of contraband or undeclared articles across the border." *Seljan*, 547 F.3d at 999; *see United States v. Alfonso*, 759 F.2d 728, (9th Cir. 1985) ("The primary purpose of a border search is to seize contraband property sought to be brought into the country.").

Given its narrow scope, the border-search doctrine, though "long-standing," "is not without qualification and limitation." *United States v. Soto-Soto*, 598 F.2d 545, 548 (9th Cir. 1979); *see also Cotterman*, 709 F.3d at 957 (rejecting "an 'anything goes' approach" when it comes to border searches). Courts have been careful to differentiate a border search from "the usual search conducted in criminal investigations[,]" stressing that "[t]his distinction must be made." *Klein v. United States*, 472 F.2d 847, 849 (9th Cir. 1973); *see also Alexander v. United States*, 362 F.2d 379, 381-82 (9th Cir. 1966) (border searches are different "from other official searches made in connection with general law enforcement."); *Soto-Soto*, 598 F.2d at 548 ("courts have carefully examined whether searches conducted without warrant or probable cause" actually "fall within" the border-search exception).

Despite the moniker "'border search[,]'" then, "[i]t does not follow" that presence at the border "is the sine qua non of a 'border search.'" *Weil*, 432 F.2d at 1322. Rather, like any exception to the warrant requirement, a border "search must be limited in scope to that which is justified by the particular purposes served by the exception." *Florida v. Royer*, 460 U.S. 491, 500 (1983); *see also Arizona v. Gant*, 556 U.S. 332, 339 (2009) (the "scope" of a search conducted under an exception to the warrant requirement must be "commensurate with its purposes[.]"); *United States v. McLaughlin*, 170 F.3d 889, 894 (9th Cir. 1999) ("[S]earches conducted pursuant to an exception to the warrant requirement must be limited in scope to the purposes for which the exception was created."). In other words, just because a search happens to occur at the border, that does not necessarily transform it into border search or automatically make it constitutional. Instead, the question is whether the government's searches of

CLIENT'S cell phone was "limited in scope to the purposes for which the [border-search] exception was created." *McLaughlin*, 170 F.3d at 894. Here, they were not.

2. The searches of CLIENT'S cell phone do not fall within the narrow scope of a border search.

In CLIENT'S case, despite likely invoking the border-search doctrine, the government did not carry out the cell-phone searches for "the particular purposes served by the exception," *Royer*, 460 U.S. at 500—namely, "to identify the illegal transportation of contraband or undeclared articles across the border." *Seljan*, 547 F.3d at 999. Rather, the agents searched CLIENT'S phone as part of their criminal investigation, in contravention of the warrant requirement.

If the government had truly conducted a border search of CLIENT'S phone, one would expect the CBP agents at primary or secondary inspection to have "turned on the device[] and opened and viewed [] files while [CLIENT] waited to enter the country." *Cotterman*, 709 F.3d at 961; *see also United States v. Arnold*, 533 F.3d 1003, 1005 (9th Cir. 2008) (true border search occurred when CBP officer "saw Arnold while he was waiting in line to go through the checkpoint," "inspected Arnold's luggage, which contained his laptop computer," and "instructed Arnold to turn on the computer so she could see if it was functioning."). But none of the inspecting agents searched CLIENT'S phone, and it was not his attempted border-crossing that triggered the searches. This is simply not a case where the government had any concerns about "contraband" on CLIENT'S phone being "'brought into the country.'" *United States v. Guzman-Padilla*, 573 F.3d 865, 877 (9th Cir. 2009) (quoting *Alfonso*, 759 F.2d at 733).

Rather, APPLY CASE FACTS – for example, it was the finding of drugs/etc. that triggered the seizure of the phone, the phone was searched by HSI agents whose primary responsibility was to investigate drug/etc. offenses, they went through the phone to gather information to prepare for their interrogation of the client, pull language from the search warrant about expecting to find evidence of drug trafficking/etc. offenses on phone.

The search of CLIENT'S cell phone is similar to the search that occurred in *Soto-Soto*, where the Ninth Circuit rejected the government's invocation of the border-search doctrine to justify an investigatory search. There, an FBI agent was conducting an investigation into stolen vehicles and inspected cars as they crossed the border. *Soto-Soto*, 598 F.2d at 546. The agent specifically "selected for inspection late-model pickups, especially Fords and Chevrolets, as likely to have been in stolen in the United States and transported to Mexico." *Id.* In the course of that investigation, the agent stopped the defendant, opened the hood of his truck to check serial numbers, and found packages inside containing marijuana. *Id.* On appeal, the Ninth Circuit rejected the government's efforts to characterize the agent's actions as a valid border search:

> Agent Summers testified that his sole purpose in conducting the search was not to enforce importation laws but rather to check whether the defendant's car was stolen. He acted for general law enforcement purposes, not for enforcement of customs laws . . . If Agent Summers had made this search in pursuit of general law enforcement away from the border, there would be no question that the search was illegal. Now the government seeks to justify the search on the mere basis that it occurred at the border. This asks too much. Congress and the courts have specifically narrowed the border searches to searches conducted by customs officials in enforcement of customs laws . . . The search of the defendant's truck was made at the border by an FBI agent as part of a general law enforcement effort . . . The search is therefore illegal, [and] the exclusionary rule applies[.]

Id. at 549-50. Here, too, the government "seeks to justify" its warrantless searches of CLIENT'S cell phone "on the mere basis that [they] occurred at the border." *Id.* at 549. Here, too, "[t]his asks too much." *Id.*

The fact remains that the agents were not concerned with contraband *on CLIENT'S phone*; they were only interested in the communications and messages on his phone. The border-search doctrine, however, is rooted in the "government's authority to protect the nation from contraband[,]" not communications relating to contraband (and future contraband at that). *Cotterman*, 709 F.3d at 966. In other words, a border search permits the government to look for contraband on the object or person being searched, thereby "control[ling] . . . who and what may enter the

country." *United States v. Ramsey*, 431 U.S. 606, 621 (1977). But this nexus between the source of contraband and the object of the search was lacking in CLIENT'S case. Permitting the government, under the guise of a border search, to examine an object in search of communications relating to speculative, future contraband "untether[s]" the border-search exception from its underlying rationale. *Gant*, 556 U.S. at 343. And it converts what is supposed to be a "narrow" exception to the warrant requirement into a broad one. *Cotterman*, 709 F.3d at 956.

The totality of the circumstances shows that the government searched CLIENT'S phone for investigative reasons. While that search happened to occur at the border, that did not make it a border search. "The search is therefore illegal, [and] the exclusionary rule applies." *Soto-Soto*, 598 F.2d at 550.

3. The government cannot establish that the good-faith exception applies.

Along with the inapplicability of the border-search exception, the good-faith exception to the warrant requirement has no place here. The good-faith exception arises when "the police act with an objectively reasonable good-faith belief that their conduct is lawful." *United States v. Lustig*, 830 F.3d 1075, 1080 (9th Cir. 2016) (internal quotations omitted). In such cases, "the deterrence rationale loses much of its force, and therefore the exclusionary rule does not apply." *Id.* (internal quotations omitted). The government bears the burden to demonstrate good faith. *See United States v. Camou*, 773 F.3d 932, 944 (9th Cir. 2014).

Here, the government cannot carry that burden. "The governing law at the time of the search made clear that," *id.*, (1) a warrantless search incident to arrest of a cell phone is unlawful, *Riley*, 134 S.Ct. at 2495, and (2) a search at the border as a tool of criminal investigation and for a purpose unrelated to border control is not a border search. *See Soto-Soto*, 598 F.2d at 549-50. The good-faith exception only applies to "search[es] conducted in objectively reasonable reliance on '*binding appellate precedent*[,]'" not on district court cases. *United States v. Lara*, 815 F.3d 605, 613 (9th Cir. 2016).

Moreover, that "binding appellate precedent'" must "'specifically authorize' the police's search;" the "appellate precedent" cannot be "unclear." *Id.* Here, the government cannot point to any binding appellate precedent specifically authorizing its agents to conduct warrantless cell-phone searches for evidence of criminal wrongdoing. Thus, the good-faith exception is inapposite.

C. Further, this Court should suppress under *Flores-Montano* and *Ramsey* because the agents' search and seizure was an intrusive, destructive, and thus unreasonable search.

1. The agents' search was highly intrusive and actually destructive.

Federal agents conducted a warrantless search of CLIENT'S phone. And the agents destroyed evidence on the phone in the course of their search and seizure.

Simply by virtue of the fact that the agents' search required a signal, it left the phone vulnerable to destruction of the phone's digital contents. Cell phone evidence may be destroyed "when a phone, connected to a wireless network, receives a signal that erases stored data"—either through "remote wiping" from a third party or through "preprogrammed deletion of data." *Riley*, 134 S. Ct. at 2486. This is why federal authorities recommend that when agents seize a smart phone, they remove the phone's battery or store it in a Faraday bag until such time as a warrant issues and a forensically trained agent can securely retrieve its data. *See* Dep't of Justice, National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders* 14, 32 (2d ed. Apr. 2008) (hereinafter "DOJ Guide") (recommending that agents use Faraday bags to properly preserve cell phone evidence); *see also Riley*, 134 S. Ct. at 2487 (stating that law enforcement agents are advised to "turn the phone off," "remove its battery," or "place it in . . . [a] 'Faraday bag[],' . . . an enclosure that isolates the phone from radio waves") (citing DOJ Guide at 32). Failure to employ any of these "simple" preservation methods during a phone seizure results in possible data corruption, including remote wiping and preprogrammed deletion. *Riley*, 134 S. Ct. at 2487.

But here, APPLY SPECIFIC CASE FACTS.

2. *Riley* does apply to border searches and the agents' intrusive, destructive search of CLIENT'S phone warrants suppression.

The *Riley* rationale *does* apply to border searches. The underpinning of *Riley*'s bright-line rule against searching smart phones incident to arrest is that even a cursory inspection is highly intrusive in view of the vast quantities of personal data stored on such devices. And *Flores-Montaro* and *Ramsey* together teach that a highly intrusive border search may violate the Fourth Amendment reasonableness requirement. *See Flores-Montano*, 541 U.S. at 154 n.2; *Ramsey*, 431 U.S. at 618 n.13.

By way of example of searches that would have offended the Fourth Amendment in the border-search context, the Court in *Ramsey* cited to *Kremen v. United States*, 353 U.S. 346 (1977), where officers, without a warrant, seized the entire contents of a cabin and took the items 200 miles away to be examined, and *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 356-58 (1931), where an officer falsely claimed to have a search warrant and then "made a general and apparently unlimited search, ransacking the desk, safe, filing cases, and other parts of the office." *See Ramsey*, 431 U.S. at 618 n.13. As *Riley* explains, smart-phone searches are at least as offensive of a person's privacy interests. They permit agents to effectively seize thousands of "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book," and other types of information that can reveal "the sum of an individual's private life." *Riley*, 134 S. Ct. at 2480. This is, by definition, implicates privacy interests so significant that it constitutes an offensively intrusive search. *See Flores-Montano*, 541 U.S. at 154 n.2; *Ramsey*, 431 U.S. at 618 n.13; *see also Kim*, 103 F. Supp. 3d at 56-57.

At the same time, the government's national-security interests in searching electronic media that, as here, has already entered the country, are diminished. *See Kim*, 103 F. Supp. 3d at 55-56. When an electronic device is searched and seized at the border, it has already entered the country. *See id.*; *see also Ramsey* 431 U.S. at 620 (stating that border-search exception was grounded in right of sovereign to limit who and what

may enter the country); *United States v. Thirty-Seven (37) Photographs*, 402 U.S. 363, 376 (1971) (border-search exception "is intimately associated with excluding illegal articles from the country"). Moreover, as *Riley* recognized, a smart phone does not pose security concerns because "data on the phone can endanger no one." *Riley*, 134 S. Ct. at 2485. Accordingly, the government's interests in excluding illegal items do not apply in the context of smart phones that have entered the country.

On balance, just as in *Riley*, the privacy interests in a smart phone far outweigh the government's interests in a border search. Therefore, *Riley*'s *per se* rule should be extended to apply to border searches.

But even if this Court holds that *Riley* does not apply fully to border searches, the Court should still suppress the evidence because the agents' intrusive, destructive search was unreasonable. *See Ramsey*, 431 U.S. at 618 n.13 (offensive border search may violate Fourth Amendment); *Seljan*, 547 F.3d at 1000 (intrusive, destructive, or offensive border search may violate Fourth Amendment).

APPLY SPECIFIC CASE FACTS. (The agents here engaged in far more than a mere "look-see at the phone at the border." Unlike *Riley*, the agents here did more than "go through" the phone's call log, contacts, and videos. *Cf. Riley*, 134 S. Ct. at 2480-81. Instead, they repeatedly attempted to search the phone's Facebook app. ER31-32, 76; *see also Riley*, 134 S. Ct. 2490 (noting that using a smart phone to search the Internet or mobile apps implicate significant privacy concerns, as they can "reveal an individuals' private interests or concerns" and provide "detailed information about all aspects of a person's life."). Worse yet, the agents' improper preservation of the phone outside a Faraday bag constituted an unreasonable seizure because it left the phone vulnerable to wiping or deletion of information. *See Riley*, 132 S. Ct. at 2487.)

In *Flores-Montano,* the Court recognized that "*potentially* destructive" border searches may be unreasonable. 541 U.S. at 154 n.2 (emphasis added). Here, the agents' search and seizure were both potentially and actually destructive. Therefore, even if smart-phone searches at the border are not *per se* unreasonable in every case, the agents'

intrusive, destructive search and seizure in this case was and the evidence should be suppressed.

3. Because the search and seizure were unreasonable, the phone-related evidence should be excluded.

Because the agents' search and seizure were unreasonable, this Court should suppress the phone-related evidence. "Evidence obtained by . . . illegal action of the police is 'fruit of the poisonous tree,' warranting application of the exclusionary rule if, 'granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.'" *United States v. Crawford*, 372 F.3d 1048, 1054 (9th Cir. 2004) (quoting *Brown v. Illinois*, 422 U.S. 590, 599 (1975)).

It does not matter if the government may not intend to introduce at trial evidence of what the agents actually saw *during* their illegal search but instead only introduce evidence obtained from the subsequent warrant-based search of the phone. The agents' unreasonable search and seizure of CLIENT'S phone poisoned the proverbial tree that produced the evidence introduced at trial. The agents' active and potential passive deletion of evidence irretrievably corrupted any evidence that could later be produced by the phone. "Unlike analog technology, where a signal is recorded or transmitted in essentially its original form, digital recording equipment translates sounds and images into a string of 0s and 1s, which digital playback equipment can read and retranslate for display. This results in . . . [an image] that can be edited relatively easily by simply rearranging the sequence of 0s and 1s." Charles Alan Wright & Victor James Gold, *Federal Practice & Procedure* § 7114 n.23 (2000). Indeed, it is because digital data can be so easily rearranged that the federal government recommends that phones be stored in Faraday bags. *See Riley*, 134 S. Ct. at 2487 (citing DOJ Guide at 32). Here, the agents' destructive search and seizure necessarily rearranged the digital data on the phone, such that the evidentiary picture portrayed *after* the unlawful search and seizure was not, and could not be, the same as the one

portrayed *before* it.

The illegal, warrantless search and seizure thus tainted the evidence that was produced by the subsequent search with a warrant. And the search warrant therefore could not purge the taint. In other words, the fact that a judge later found probable cause to issue a warrant does not somehow return the phone to its pre-search and -seizure condition. Accordingly, the exclusionary rule applies, and the Court should suppress the phone evidence.

D. At a minimum, this Court should hold an evidentiary hearing.

An evidentiary hearing on a motion to suppress should be held when the movant alleges facts "with sufficient definiteness, clarity, and specificity to enable the trial court to conclude that contested issues of fact exist." *United States v. Cook*, 808 F.3d 1195, 1201 (9th Cir. 2015); *see also United States v. Irwin*, 612 F.2d 1182, 1187 (9th Cir. 1980) ("If, in fact, a material issue of fact were raised which if resolved in accordance with appellant's contentions would entitle him to relief, an evidentiary hearing would be required") (internal quotation marks, brackets, and citation removed). In conducting this analysis, a district court must "assume[] that the specific factual allegations are true." *United States v. Schaflander*, 743 F.3d 714, 722 (9th Cir. 1984) (internal quotation marks and citation omitted).

Here, CLIENT moves to suppress the phone evidence that the government sought to introduce at trial based in part on the government's improper preservation of the phone. He alleges definite, clear, and specific facts to show that there is a genuine issue as to whether the phone's improper preservation corrupted the phone evidence, such that suppression is required. Because CLIENT meets the low legal hurdles necessary for holding an evidentiary hearing, the Court should grant his request and hold an evidentiary hearing.

II. The searches of CLIENT's cell phone violate the Fifth Amendment, and this Court should dismiss or, at a minimum, suppress the resulting evidence.

A. The government's bad-faith destruction of the phone evidence violates CLIENT'S due process.

In addition to violating CLIENT'S Fourth Amendment rights by illegally searching and seizing his phone, the government violated his due-process rights by failing to properly preserve the phone. The government violates a defendant's right to due process when it "acted in bad faith in failing to preserve . . . potentially useful evidence" and when the missing evidence "'is of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *Zaragoza-Moreira*, 780 F.3d at 977 (quoting *California v. Trombetta*, 467 U.S. 479, 489 (1984)) (brackets omitted). Here, APPLY CASE FACTS (the government failed to preserve phone-related evidence that was potentially useful to CLIENT'S no-knowledge defense, it acted in bad faith in doing so, and there is no comparable evidence that could replace the cell-phone data as it existed at the time of the offense.) Accordingly, the government violated CLIENT'S due-process rights, and the Court should dismiss the case against him, or at least suppress the phone-related evidence.

1. CLIENT'S request to preserve the phone evidence and the government's failure to comply.

APPLY CASE SPECIFIC FACTS detailing discovery requests and what was produced.

2. The phone evidence was potentially useful.

The phone evidence that the government failed to preserve was potentially useful to CLIENT'S defense. Potentially useful evidence is "'evidentiary material of which no more can be said than that it could have been subjected to tests, the results of which might have exonerated the defendant.'" *Zaragoza-Moreira*, 780 F.3d at 978 (quoting *Arizona v. Youngblood*, 488 U.S. 51, 57 (1988)).

Here, APPLY CASE FACTS. (the unpreserved evidence could have been subjected to tests that would have exonerated CLIENT. For example, the evidence

may have included text messages indicating CLIENT'S belief that he was transporting something other than drugs. In fact, CLIENT repeatedly insisted to the interrogating agents postarrest that the phone contained just such evidence in the form of text messages between him and his girlfriend—many of which had been deleted by the time the government forensically extracted the data pursuant to a warrant, months later.) Alternatively, the phone evidence could have shown what settings were active on the phone at the time of CLIENT'S arrest—for example, whether his Facebook page was private or public, or whether the phone was preprogrammed to delete messages after a certain point in time, as it was capable of doing.

Without that evidence, the government was able to argue that the deletion of text messages was precisely timed, manual, intentional, and indicative of CLIENT'S knowledge that drugs were in the car. But had the phone been properly preserved, the results of forensic tests might have exonerated CLIENT. Accordingly, the unpreserved evidence was potentially useful.

3. The government acted in bad faith.

When potentially useful evidence has been destroyed by the government, a due process violation inheres if the government acted in bad faith. *See Zaragoza-Moreira*, 780 F.3d at 979. "[T]he bad-faith inquiry initially 'turns on the government's knowledge of the apparent exculpatory value of the evidence at the time it was lost or destroyed.'" *Id.* (quoting *United State v. Sivilla*, 714 F.3d 1168, 1172 (9th Cir. 2013)).

The government here acted in bad faith in failing to preserve the CLIENT'S smart phone intact. As *Riley* recognizes, a smart phone's capacity to store all manner and quantity of potentially exculpatory personal data makes its evidentiary value "apparent." *Riley*, 134 S. Ct. at 2485, 2494-95.

In addition, the failure of the Assistant U.S. Attorneys ("AUSAs") assigned to the case to comply with their discovery obligations under Federal Rule of Criminal Procedure 16 contributed to the agents' bad faith. "While non-compliance with Rule 16 does not amount to a due process violation absent bad faith, the government's

failure to take action in response to defense counsel's letter in the instant case is particularly disturbing." *Zaragoza-Moreira*, 780 F.3d at 981.

In short, "the apparent value of [smart-phone] evidence, which was known to [the government]," as well as "[the government's] actions following [CLIENT'S] interview" and arrest, "are sufficient to establish that [the government] made 'a conscious effort to suppress exculpatory evidence,' thereby acting in bad faith." *Zaragoza-Moreira*, 780 F.3d at 980 (quoting *Trombetta*, 467 U.S. at 488).

4. No comparable evidence was available.

Finally, the government's bad-faith failure to preserve the cell-phone evidence violates CLIENT'S due-process rights because he was "'unable to obtain comparable evidence by other reasonably available means.'" *Zaragoza-Moreira*, 780 F.3d at 981 (quoting *Sivilla*, 714 F.3d at 1172). Proper preservation of electronic data is important precisely because such data is both unique and easily corruptible. Digital data "can be edited relatively easily by simply rearranging the sequence of 0s and 1s." Wright & Gold, Federal Practice & Procedure § 7114 n.23. Here, once the digital data on CLIENT'S phone had been rearranged, it could not be put back together in its original format, and there was no substitute for it.

5. The Court should dismiss the information for violation of due process.

In sum, the phone-related evidence was potentially useful to CLIENT'S defense, the government destroyed it in bad faith, and there is no comparable evidence that could replace it. *See Zaragoza-Moreira*, 780 F.3d at 977. Accordingly, the government's failure to properly preserve the phone evidence violates CLIENT'S right to due process, and the Court should dismiss the information.

6. At minimum, the government's failure to preserve the phone evidence requires exclusion of the evidence at trial.

Even if the government's misconduct did not warrant dismissal, the Court should exclude the phone-related evidence under the balancing test set forth in *United States v. Loud Hawk*, 628 F.2d 1139, 1152 (9th Cir. 1979) (en banc) (Kennedy, J.,

concurring); *see also* FED. R. CRIM. P. 16(d)(2)(C) (providing that remedy for violation of Rule is to "prohibit th[e violating] party from introducing the undisclosed evidence."). In *Loud Hawk*, this Court held that when the government spoliates potentially exculpatory evidence, a district court should weigh whether "the quality of the government's conduct" is outweighed by "the degree of prejudice to the accused" in determining whether to give an adverse-inference jury instruction. *See id.* The same balancing test should apply here and impose an evidentiary sanction for the government's failure to properly preserve the phone evidence.

The first inquiry—the quality of the government's conduct—weighs in favor of excluding the phone evidence. In assessing the government's conduct, *Loud Hawk* held that courts should determine "whether the evidence was lost or destroyed while in custody, whether the Government acted in disregard for the interests of the accused, whether it was negligent in failing to adhere to established and reasonable standards of care for police and prosecutorial functions, and if the acts were deliberate, whether they were taken in good faith or with reasonable justification." 628 F.2d at 1151. But while the absence of good faith is relevant, bad faith is not required. *See Sivilla*, 714 F.3d at 1173. Here, APPLY CASE FACTS. (the phone evidence was destroyed while it was in the government's custody. The government acted in disregard for CLIENT'S interests in searching his phone and deleting information on it and in improperly seizing the phone in a manner that permitted it to make outgoing calls and receive incoming messages.) The government was at least negligent in failing to adhere to Department of Justice protocols for preserving cell phones. And for all the reasons stated *supra*, the government lacked reasonable justification for failing to properly preserve the phone. Accordingly, the government's conduct weighs in favor of excluding the phone-related evidence.

The second inquiry—the degree of prejudice—also weighs in favor of exclusion. *Loud Hawk* held that the following factors are relevant in determining prejudice:

> the centrality of the evidence to the case and its importance in establishing the elements of the crime or the motive or intent of the defendant; the probative value and reliability of the secondary or substitute evidence; the nature and probable weight of factual inferences or other demonstrations and kinds of proof allegedly lost to the accused; the probable effect on the jury from absence of the evidence, including dangers or unfounded speculation and bias that might result to the defendant if adequate presentation of the case requires explanation about the missing evidence.

628 F.2d at 1153. Here, APPLY CASE FACTS. (the phone-related evidence is central to the government's effort to prove knowledge, the sole element in dispute at trial. There is no substitute evidence available, because the improper preservation irreparably corrupted the phone's data. The data that was potentially lost may well have included text messages exonerating CLIENT, so the weight of that information is important in the credibility contest as to knowledge. And the absence of evidence will likely have significant effect on the jury given if the government uses the missing information as a sword against CLIENT in its case.) Accordingly, the prejudice to CLIENT caused by the improper preservation also weighs in favor of excluding the phone-related evidence.

III. The Court should exclude the phone-related evidence under the Federal Rules of Evidence.

A. The authentication rule precludes admission of the unauthenticated evidence.

Even if the Court does not suppress the phone-related evidence under either a Fourth Amendment or a Fifth Amendment theory, it should exclude the evidence because its admission violates the Federal Rules of Evidence.

Rule 901 provides that a piece of evidence is properly "authenticat[ed] or identif[ied]" when its proponent lays a foundation "sufficient to support a finding that the item is what the proponent claims it is." FED. R. EVID. 901(a); *see also United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (holding that under Rule 901, "a foundation must be established for the information through authentication"). In the case of evidence produced by a machine, the proponent can lay this foundation by

producing "[e]vidence describing a process or system and showing that it produces an accurate result." FED. R. EVID. 901(b)(9).

Here, CASE FACTS (the government seeks to introduce machine-produced evidence at trial. Specifically, the government seeks to admit screenshots of text messages, ETC.) The Court should preclude the admission of this evidence.

"[E]vidence derived from the operation of a machine or instrument normally depends for its validity on the premise that the device was in proper working order." *See United States v. Espinal-Almeida*, 699 F.3d 588, 610 (1st Cir. 2012) (cited in *United States v. Lizarraga- Tirado*, 789 F.3d 1107, 1110 (9th Cir. 2015)) (internal quotation marks and citation omitted). Thus, to satisfy the authentication requirement under Rule 901(b)(9), the proponent must show that the machine is reliable and correctly calibrated and that the data produced by the machine is accurate. *See Lizarraga-Tirado*, 789 F.3d at 1110 (citing *Washington*, 498 F.3d at 231). By the same token, concerns that "[a] machine might . . . have been tampered with" do not satisfy the Rule 901(b)(9) authentication requirement. *Id.* The government has not shown that here.

Thus, admission of this evidence would fundamentally misinterpret the authentication rule under Rule 901(b)(9). The government has failed to "establish[] . . . a foundation . . . for the information through authentication" by showing that the cell phone "produce[d] an accurate result" at the time the evidence was obtained. *Washington*, 498 F.3d at 231. Therefore, the evidence should not be admitted at trial.

B. The evidence is also inadmissible under FRE 401 and 403.