IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES Appellee v. Staff Sergeant (E-6) **ALEX J. SECORD** United States Army Appellant	BRIEF ON BEHALF OF APPELLANT Crim. App. Dkt. No. 20210667 USCA Dkt. No. 24-0217/AR

Amir R. Hamdoun
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 695-9862
USCAAF Bar No. 37920

Daniel Conway
Civilian App. Defense Counsel
Daniel Conway and Associates
20079 Stone Oak Parkway,
Suite 1005-506
San Antonio, TX 78258
(210) 934-8265 (UCMJ)
conway@militaryattorney.com
www.militaryattorney.com
USCAAF Bar Number 34771

Table of Contents

Table of Authorities

SUPREME COURT OF THE UNITED STATES

COURT OF APPEALS FOR THE ARMED FORCES/COURT OF MILITARY APPEALS

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES Appellee v. Staff Sergeant (E-6) **ALEX J. SECORD** United States Army Appellant	BRIEF ON BEHALF OF APPELLANT Crim. App. Dkt. No. 20210667 USCA Dkt. No. 24-0217/AR

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES:

Granted Issues

I. WHERE THE GOVERNMENT SEIZED AND HELD APPELLANT'S PHONE PURSUANT TO A NARROW SEARCH AUTHORIZATION, BUT COULD NOT ACCESS THE DATA WITHOUT APPELLANT'S PASSCODE, WAS THE DATA WITHIN THE POSSESSION, CUSTODY, OR CONTROL OF MILITARY AUTHORITIES FOR PURPOSES OF R.C.M. 701?

II. DID THE MILITARY JUDGE ERR BY RULING APPELLANT COULD NOT ACCESS THE DATA WITHOUT SIMULTANEOUSLY PROVIDING THE GOVERNMENT WITH FULL ACCESS TO ALL HIS PERSONAL DATA?

III. IF THE MILITARY JUDGE ERRED, DID THE ERROR CONSTITUTE PREJUDICIAL ERROR?

Statement of Statutory Jurisdiction

The Army Court of Criminal Appeals [Army Court] had jurisdiction over this matter pursuant to Article 66, Uniform Code of Military Justice [hereinafter

UCMJ], 10 U.S.C. § 866. This Honorable Court has jurisdiction over this matter under Article 67(a)(3), UCMJ, 10 U.S.C. § 867 (a)(3).

Statement of the Case

On December 17, 2021, an enlisted panel, sitting as a general court-martial, convicted appellant, Staff Sergeant Alex J. Secord, contrary to his pleas, of five specifications of wrongful use of a controlled substance and one specification of violation of a lawful general regulation (undue familiarity between a noncommissioned officer and an enlisted servicemember), in violation of Articles 92 and 112a, Uniform Code of Military Justice [UCMJ], 10 U.S.C. §§ 892, 912a. (JA at 222).[1] On December 18, 2021, an enlisted panel sentenced appellant to reduction to E-2, eighty-five days confinement, and a bad-conduct discharge. (JA at 223).[2] On February 2, 2022, the convening authority took no action on the findings and sentence. (JA at 260). On February 8, 2022, the military judge entered Judgment. (JA at 261). On June 26, 2024, the Army Court affirmed the findings and sentence. (JA at 2-9).

[1] Appellant was acquitted of one specification of aggravated assault with a dangerous weapon, in violation of Article 128, UCMJ, 10 U.S.C. § 928, two specifications of wrongful possession of a controlled substance with intent to distribute, and two additional specifications of wrongful use of a controlled substance in violation of Article 112a, UCMJ.

[2] The Judgment of the Court modified the Statement of Trial Results (the Statement of Trial Results incorrectly indicated that a reprimand was adjudged).

Statement of Facts

Prior to trial, the government seized appellant's phone pursuant to a search and seizure authorization. (JA at 232-35). The authorization was limited to messages and media pertaining to wrongful use, possession, and distribution of cocaine and was based off witness interviews that alleged appellant would use his phone to contact drug dealers and then pay for the drugs with his phone via CashApp or Apple Pay. (JA at 233). The government was unable to access appellant's phone or extract data because the phone was protected by a passcode and the government's extraction software was incompatible with the phone. See (JA at 246-47); *see also* (JA at 35). Appellant's phone was placed in airplane/offline mode. (JA at 235).

On August 13, 2021, defense counsel filed a motion to compel discovery, seeking the opportunity to access appellant's phone and for the defense's appointed digital forensic examiner [DFE] to conduct an extraction of appellant's phone. (JA at 224-29).

At the motions hearing, the government acknowledged there may be "a good faith basis for [believing the data] contain[ed] exculpatory evidence" but nonetheless insisted its refusal to grant defense access was reasonable. *See* (JA at 35-37, 48). The purpose for maintaining "sole custody and control" was for the

further prosecution of "other individuals both known and unknown to the government," and "to maintain the phone's evidentiary value." (JA at 36).

The military judge granted appellant's motion to inspect his phone in part, (JA at 51), but the military judge's ruling was contingent upon the defense granting the government equal access to all the phone's data. (JA at 51-52). On December 3, 2021, appellant declined to utilize the military judge's "[offer of] a voluntary joint inspection, joint extraction." (JA at 57).

The Army Court affirmed. (JA at 2-9). In its opinion, the Army Court determined:

> [R.C.M.] 701(a) and 701(b) appear to contemplate that the data in question is in the current *physical* "possession, custody, or control" (ie: capable of being immediately reviewed and in a format that it could be presented as an exhibit for identification at trial) of one of the parties at the time of the discovery request by the party not in possession.

(JA at 6) (emphasis added). The Army Court concluded appellant's phone data was "not in the government's physical possession," and the military judge's ruling restricting appellant's discovery rights was not an abuse of discretion under R.C.M. 701(g)(1). (JA at 2-9).

Summary of Argument

The data in question, which was held in the government's evidence locker, fell within the plain meaning of "possession, custody, or control" as used in

R.C.M. 701(a)(2)(A). Indeed, the government at trial conceded as much by repeatedly referring to the evidence as within government "custody" and "control." The text is paramount and this Court should not follow the Army Court's example of adding to the rule's text to justify a result contrary to its plain meaning. The conclusion that the data was in the government's "possession, custody, or control" is further supported by caselaw and the presumption of consistent usage (because the same term is used elsewhere in the UCMJ and does not, in that context, carry the extra-textual caveats added by the lower court).

If this Court agrees the data was within the possession, custody, or control of military authorities, appellant had the right to inspect because it fell within two categories of R.C.M. 701(a)(2)(A). As conceded by the government at trial, it was relevant to defense preparation under R.C.M. 701(a)(2)(A)(i), and it was obtained from or belonged to appellant under R.C.M. 701(a)(2)(A)(iv). There is no support in the text of the rules for the prerequisite imposed by the military judge that appellant give the government unfettered access to the data because "[t]here must be equal access to evidence" because neither Article 46 nor the R.C.M require the defense to provide the government with total access to its files.

The government will have a hard time meeting its prejudice burden. The government at trial conceded the data may be exculpatory. The government's burden will be particularly difficult with respect to Specifications 5-7 of Charge II

because those specifications were weak and supported by testimony from unreliable witnesses. The phone data could have demonstrated that appellant was in a different location than alleged on the charged dates, could have further impeached the government witnesses' credibility, or could have provided alternate explanations for the supposed payment records relating to the drugs. The government relied on this evidence originating from appellant's phone to prove these specifications, while appellant was denied access to the information needed to challenge this evidence, increasing prejudice.

I. WHERE THE GOVERNMENT SEIZED AND HELD APPELLANT'S PHONE PURSUANT TO A NARROW SEARCH AUTHORIZATION, BUT COULD NOT ACCESS THE DATA WITHOUT APPELLANT'S PASSCODE, WAS THE DATA WITHIN THE POSSESSION, CUSTODY, OR CONTROL OF MILITARY AUTHORITIES FOR PURPOSES OF R.C.M. 701?

Standard of Review

Questions of statutory interpretation to include the interpretation of provisions of the R.C.M. are questions of law this Court reviews de novo. *H.V.Z. v. United States*, __ M.J. __, 2024 CAAF LEXIS 410 at *8, *11 (C.A.A.F. July 18, 2024) (citations omitted).

Law

Article 46, UCMJ, 10 U.S.C. § 846, provides equal opportunity for the accused to obtain evidence in accordance with the rules prescribed by the

President. R.C.M. 701(a)(2)(A)(i) and (iv) further define a trial counsel's obligations under Article 46, UCMJ:

> [U]pon request of the defense, the Government *shall* permit the defense to inspect . . . data . . . if the item is *within the possession, custody, or control of military authorities* and—
>
> (i) the item is relevant to defense preparation;
>
> . . .
>
> (iv) the item was obtained from or belongs to the accused.

(emphasis added).[3]

Argument

R.C.M. 701(a)(2)(A) applies to data that is disjunctively within the "possession, custody, *or* control of military authorities." (emphasis added). This Court should find the data in question fell within the plain meaning of this broad language. Appellant's phone, which was physically in the CID evidence locker, was within the *possession* of military authorities. *See* (JA at 22-23, 36) (statements by CID that they took possession of the phone). In plain language, as echoed by the testimony of the CID personnel, an item within the government's evidence locker is within its possession. Similarly, the item was within the *custody* of military authorities. Indeed, the evidence locker – where the phone was – is often referred to as a "custody locker." When an item is seized and placed therein, the

[3] References to the R.C.M. are from *Manual for Courts-Martial, United States* (2019 ed.).

military authorities fill out a "chain of custody" document. *See* (JA at 36-37) (trial counsel references to the chain of custody document for the phone); *see also* (JA at 234). During the litigation of this very issue, trial counsel conceded the government had "sole custody of the information on the phone." (JA at 37). Trial counsel also objected to the evidence being "signed out of custody" for defense. (JA at 36). Finally, the data was within the *control* of military authorities. Again, the government emphasized the importance of maintaining "sole custody and control" of the evidence. *See* (JA at 36); *see also* (*Id.*) (trial counsel objection to "pass[ing] the evidence outside the *control* of the government. . . .") (emphasis added).

The Army Court only avoided these obvious textual conclusions by adding to the text, declaring that: "Rules for Courts-Martial 701(a) and 701(b) appear to contemplate that the data in question is in the current physical 'possession, custody, or control' (ie: capable of being immediately reviewed and in a format that it could be presented as an exhibit for identification at trial) of one of the parties at the time of the discovery request by the party not in possession." (JA at 6). Neither military judges nor appellate courts are authorized to add language to

the R.C.M.[4] If the President wishes to add these caveats to the rule, along with appropriate definitions and other safeguards, he is free to do so.

The Army Court's holding that government's possession of data must be "physical" also conflicts with *Stellato*, where this Court observed that "the Government need not *physically* possess an object for it to be within the possession, custody, or control of military authorities." 74 M.J. 473, 485 (C.A.A.F. 2015) (emphasis added) (noting Article III courts have found evidence in possession of the government when, *inter alia*, "the prosecution has both knowledge of and access to the object" and "the prosecution has the legal right to obtain the evidence").

The Army Court's decision further conflicts with the recent decision in *United States v. Strong*, where this Court examined the question of when the seizure of a cellphone and its digital contents is complete, concluding the seizure of a phone's digital content is complete when law enforcement has possession of – and exclusive dominion over – the digital content. __ M.J. __, 2024 CAAF LEXIS 478 (C.A.A.F. Aug. 22, 2024). As this Court pointed out in *Strong*: According to

[4] Appellate courts, and particularly the CCAs, are not policy making bodies. *See United States v. Nerad*, 69 M.J. 138, 148–49 (C.A.A.F. 2010) (Baker, J., concurring) ("[I]t is clear that CCAs are not equitable courts, and they are not policy-making bodies."); *see also Bostock v. Clayton Cnty., Georgia*, 590 U.S. 644, 680 (2020) (noting that "policy appeals" are "the last line of defense for all failing statutory interpretation arguments.").

Black's Law Dictionary, "seize" is defined as "[t]o forcibly take *possession* (of a person or property)" and "[t]o be in possession (of property)." Seize, Black's Law Dictionary (10th ed. 2014) (emphasis added). Meanwhile, "possession" is defined as "[t]he fact of having or holding property in one's power; the exercise of dominion over property" and "[t]he right under which one may exercise control over something to the exclusion of all others; the continuing exercise of a claim to the exclusive use of a material object." Possession, Black's Law Dictionary (10th ed. 2014). Thus, explicitly defining possession as a subset of seizure, this Court held that seizure is complete after securing the data from outside manipulation. 2024 CAAF LEXIS 478 at *13 ("a seizure is complete for purposes of Article 131e, UCMJ, when a person authorized to seize certain property has possession of the property . . . ."). Government possession, custody, *or* control, as contemplated in R.C.M. 701(a)(2)(A), encompasses a wider range of government action than "seizure," and is thus an even lower hurdle. Here, seizure was clearly accomplished and, as such, the government had possession also.

The presumption of consistent usage also supports the conclusion that the term "possession, custody, or control" does not exclude encrypted data. For example, Art. 108a requires servicemembers report and turn all captured or abandoned property in their "possession, custody, or control." Surely the government would not contend the identical term applies only to unencrypted data. Absent action on the part of the drafters to define "possession, custody, or control" more narrowly in the context of R.C.M. 701 than elsewhere, appellate court should not read additional words into the exact same term.

II. DID THE MILITARY JUDGE ERR BY RULING APPELLANT COULD NOT ACCESS THE DATA WITHOUT SIMULTANEOUSLY PROVIDING THE GOVERNMENT WITH FULL ACCESS TO ALL HIS PERSONAL DATA?

Standard of Review

A military judge's ruling on a motion to compel discovery is reviewed for an abuse of discretion. *United States v. Roberts*, 59 M.J. 323, 326 (C.A.A.F. 2004) (citation omitted). "A military judge abuses his discretion when his findings of fact are clearly erroneous, when he is incorrect about the applicable law, or when he improperly applies the law." *Id.*

Law and Argument

If this Court agrees the data was within the possession, custody, or control of military authorities, appellant had the right to inspect if it fell within any of the categories of R.C.M. 701(a)(2)(A). It fell squarely within at least two. First, it was

relevant to defense preparation under R.C.M. 701(a)(2)(A)(i). The government conceded appellant's phone data was a covered item in this category. (JA at 48) ("the contents of the cell phone . . . may be the basis of a good faith basis for containing exculpatory evidence as the defense suggests"). Second, it was obtained from or belonged to appellant under R.C.M. 701(a)(2)(A)(iv). The law in plain terms afforded appellant with a non-discretionary right to discovery of phone data belonging to him and relevant to defense preparation.

There is no support in the text of the rules for the prerequisite imposed by the military judge that appellant give the government unfettered access to the data. While both the military judge and the Army Court relied on Article 46's "equal opportunity" language, nothing in Article 46 nor the R.C.M. requires the defense to provide the government with total access to its files. *See, e.g.*, (JA at 39) (Military Judge: "There must be equal access to evidence."). R.C.M. 701(a)(2) explicitly applies to government discovery. The defense equivalent, R.C.M. 701(b)(3) requires the defense to turnover only data it intends to use in its case-in-chief at trial. To the extent disclosure of the data in question triggered defense reciprocal discovery obligations, those obligations could have been fulfilled in the normal course of litigation.[5] But requiring the defense to allow unfettered access to all the

[5] Defense counsel acknowledged as much, stating the defense would "adhere to all reciprocal discovery obligations" and turn over anything from the phone that was required to be disclosed pursuant to R.C.M. 701(b). *See* (JA at 33).

data on appellant's phone – far beyond the scope of the authorization under which it was originally seized – imputed disclosure obligations to the defense outside those required by the rules.

This Court should not endorse a rule which would allow the government to force an accused to choose between being wholesale deprived of discoverable material or allowing the government total access to the vast amounts of highly personal data stored on a modern smartphone. *See generally Riley v. California*, 573 U.S. 373, 393 (2014) (noting that modern cell phones "implicate privacy concerns far beyond those implicated by" other types of personal effects). Even if the phone was not locked to begin with, the government would never have had equal access to all its contents. *See generally United States v. Shields*, 83 M.J. 226, 232 (C.A.A.F. 2023), *cert. denied*, 144 S. Ct. 189, 217 L. Ed. 2d 76 (2023) (discussing how a search of cell phone data must be reasonably tailored to the data being searched for). Allowing the government to seize all of appellant's phone data pursuant to a search authorization for a limited subset thereof, but then making appellant's access to his own data contingent on granting the government full access to rummage through all the data, gives the government a backdoor path to a trove of highly personal information that would never otherwise be subject to government intrusion.

III. IF THE MILITARY JUDGE ERRED, DID THE ERROR CONSTITUTE PREJUDICIAL ERROR?

Standard of Review

"Where an Appellant demonstrates that the government failed to disclose discoverable evidence in response to a specific request the Appellant will be entitled to relief unless the government can show that nondisclosure was harmless beyond a reasonable doubt." *United States v. Cano*, 61 M.J. 74, 75 (C.A.A.F. 2005) (citing *Roberts*, 59 M.J. at 327) (additional citation omitted). "Failing to disclose requested material favorable to the defense is not harmless beyond a reasonable doubt if the undisclosed evidence might have affected the outcome of the trial." *United States v. Coleman*, 72 M.J. 184, 187 (C.A.A.F. 2013).

Law and Argument

As an initial matter, it is difficult to perform a detailed prejudice analysis without access to the underlying evidence which, of course, is not contained in the record nor available to the parties. The reason nobody has access to the evidence in question is because access was denied by the government, with the sanction of the military judge. If this Court reaches prejudice, this denial of access was erroneous, and it must be held against the government rather than appellant.

As the burden is with the government, this is really the government's problem.[6] The government not only has the burden of persuasion, but also the burden of proof beyond a reasonable doubt – the highest burden known to the law. One long-standing formulation of the beyond a reasonable doubt standard, though "often clothed in varying verbiage," is that it requires exclusion of every reasonable alternative hypothesis. *See generally United States v. O'Neal*, 2 C.M.R. 44, 49 (C.M.A. 1952). As it is the government's burden, appellant will wait to see how the government tries to meet it in its answer brief, but it will likely be difficult for the government to exclude every reasonable hypothesis that the evidence would have made a difference.

[6] Of note, in addressing prejudice in the alternative, the Army Court explicitly assigned the burden of establishing prejudice to appellant, even while acknowledging the potential application of the harmless beyond a reasonable doubt standard. (JA at 7-8). Under the harmless beyond a reasonable doubt standard, however, it is the *government's burden* to show harmlessness. *See, e.g.*, *Roberts*, 59 M.J. at 327 ("[T]he appellant will be entitled to relief unless *the Government can show* that nondisclosure was harmless beyond a reasonable doubt.) (emphasis added). Additionally, the Army Court's criticism of the defense for not putting on more evidence at trial regarding the specific helpful evidence that might be found on the phone is perplexing for a few reasons. (JA at 7-8). First, the defense was deprived access to the evidence, and therefore limited in its ability to analyze or present the data as evidence of prejudice. Second, at the trial level the defense's only obligation was to present sufficient evidence to meet the low threshold that the data was relevant to defense preparation, a threshold the defense cleared at trial with the apparent concurrence of the government.

Indeed, the government conceded at trial there was reason to believe the data at issue would yield exculpatory evidence. (JA at 48) ("the contents of the cell phone . . . may be the basis of a good faith basis for containing exculpatory evidence as the defense suggests"). It is hard to reconcile this concession with the government meeting its burden to prove harmlessness beyond a reasonable doubt.

This is particularly the case with regard to Specifications 5-7 of Charge II, in that those specifications were by far the weakest. Both the dates and substance of these specifications were established through the testimony self-confessed drug-users who openly admitted they were trying to avoid criminal prosecution (and/or deportation to Iran) in exchange for providing evidence against appellant. *See* (JA at 13-15) (Statement of Trial Results). Indeed, the acquittals on multiple other charges relying on these witnesses' testimony shows just how questionable their veracity was in the eyes of the panel.

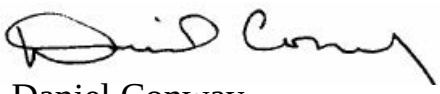
The phone data could have demonstrated that appellant was in a different location than alleged by the government's cast of characters on the charged dates, could have further impeached their credibility in other regards, or could have provided alternate explanations for the supposed payment records relating to the drugs. The government cannot disprove these reasonable alternative hypothesis and cannot carry its burden.

Additionally, the government relied on this evidence originating from appellant's phone to prove these specifications, arguing the evidence would show "how the accused would receive money via Cash App *on his phone* then go to meet his drug dealer and [return] with the cocaine." *See* (JA at 61) (emphasis added); *see also* (JA at 79-80, 83-89) (reliance of MB on information allegedly originating from appellant's phone to establish dates and details of charged offenses). Deprived of access to the data from appellant's phone, the defense at trial was hampered in its ability to counter incriminating evidence introduced by the government that purported to show appellant's activity on his phone. The key government witness, MB, "admittedly did not remember exact dates [the offenses] occurred." (*Government closing argument for findings*, JA at 198). In fact, "the only way [MB] was able to testify about using drugs with [appellant] was by looking at her [Cash App] records [with appellant]." (*Defense closing argument for findings*, JA at 215); *see also* (JA at 79-80, 83-89).

Conclusion

WHEREFORE, appellant respectfully requests this Honorable Court set aside the findings and the sentence.

Amir R. Hamdoun
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 695-9862
USCAAF Bar No. 37920



Daniel Conway
Civilian App. Defense Counsel
Daniel Conway and Associates
20079 Stone Oak Parkway,
Suite 1005-506
San Antonio, TX 78258
(210) 934-8265 (UCMJ)
conway@militaryattorney.com
www.militaryattorney.com
USCAAF Bar Number 34771

Certificate of Compliance with Rules 24(c) and 37

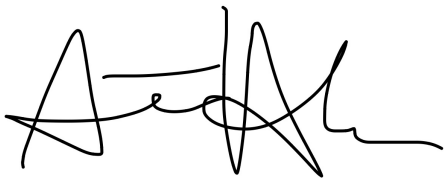
1. This Brief on Behalf of Appellant complies with the type-volume limitation of Rule 24(c) because it contains 4,134 words.

2. This Brief on Behalf of Appellant complies with the typeface and type style requirements of Rule 37 because it has been prepared in Times New Roman font, using 14-point type with one-inch margins.

Amir R. Hamdoun
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 695-9862
USCAAF Bar No. 37920

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing in the case of United States v. Secord, USCA Dkt. 24-0217/AR was electronically with the Court and Government Appellate Division on November 6, 2024.



Amir R. Hamdoun
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
(703) 695-9862
USCAAF Bar No. 37920