**MILITARY LAW REVIEW**

**Volume 230** **Issue 1**

# COMPELLED DECRYPTION IN THE MILITARY JUSTICE SYSTEM: WHETHER THE ARTICLE 30A, UCMJ, INVESTIGATIVE SUBPOENA IS A LAWFUL AND PRACTICAL METHOD TO OBTAIN AN ACCUSED'S ELECTRONIC DEVICE IN AN UNENCRYPTED STATE

MAJOR JEFFREY C. SULLIVAN*

## I. Introduction

The use of investigative subpoenas under Article 30a, Uniform Code of Military Justice (UCMJ), to compel decryption of electronic devices under the control of the accused is a lawful and practical method to obtain access to otherwise lawfully seized electronic media. Specifically, the Government should seize the device through the normal search authorization process and then seek a judicially issued Article 30a, UCMJ, investigative subpoena compelling the accused to produce the device in an unencrypted condition with any security features that would frustrate forensic extraction disabled. If the accused declines to obey a military judge's order directing compliance with such a subpoena, the Government should both request that the military judge impose contempt punishment under Article 48, UCMJ, and consider prosecution for the refusal to comply under any of a number of articles of the UMCJ.

The applicability of the Fifth Amendment protection against self-incrimination will turn on applying the act of production doctrine and the foregone conclusion doctrine. Under the act of production doctrine, an act such as decrypting a device can qualify for Fifth Amendment protection if

* Judge Advocate, United States Air Force. LL.M., University of Nebraska College of Law (2021); J.D., University of Virginia School of Law (2009); B.A., Boston College (2006)). Major Sullivan has served as a Senior Trial Counsel and an Area Defense Counsel in the Air Force JAG Corps. He is a member of the bars of Maryland and the District of Columbia. The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

it is "testimonial, incriminating, and compelled."[1] The foregone conclusion doctrine, however, can render an act of production non-testimonial (and thus not protected by the Fifth Amendment) if any implied testimony is a "foregone conclusion."[2] Although military appellate courts thus far have declined to rule on the foregone conclusion doctrine and compelled decryption, an analysis of the UCMJ, the *Manual for Courts-Martial* (*MCM*), and military and civilian case law suggests that the foregone conclusion doctrine would apply to compelled decryption in the military justice system like in other Federal courts.

Employing the Article 30a, UCMJ, investigative subpoena to compel decryption would align military practice with the Federal civilian practice of using grand jury subpoenas to compel decryption. Although either a Government counsel-issued subpoena or a superior officer's extra-judicial order is lawful so long as the foregone conclusion doctrine applies, the judicially issued Article 30a, UCMJ, investigative subpoena is a more practical investigative tool that provides for more orderly litigation for a number of reasons. First, a pre-referral subpoena authorized by the general court-martial convening authority (GCMCA) and issued by Government counsel would be timely but would inevitably require judicial intervention to resolve a request for relief. Second, a superior officer's order would also be timely, but the Article 30a, UCMJ, process avoids placing defense counsel in the position of potentially advising a client to violate a superior officer's order and litigating its lawfulness at a later court-martial. Third, a subpoena issued either during a preliminary hearing or after referral comes too late in the military justice process to be a practical investigative tool. Therefore, in most cases, the Government should elect to pursue the Article 30a, UCMJ, judicially issued subpoena process over lawful alternatives. Where time is of the essence, however, the Government might elect more a more expeditious option, such as a superior officer's order.

---

[1] Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 189 (2004).

[2] Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 771 (2019).

## II. Background

### A. Decryption in Criminal Investigations

The accused's electronic devices, particularly mobile phones, "are potentially rich sources of evidence."[3] Evidence on the accused's mobile device may be contraband (e.g., child pornography) or it may be evidence of another offense (e.g., incriminating text messages, photographs, or videos). But efforts to search the accused's device may be frustrated if the device is encrypted.[4] Modern Apple and Android mobile phones, for example, are encrypted by default.[5] Thus, investigators with a proper search authorization will nonetheless need to overcome the decryption to obtain evidence. If the Government can overcome the encryption via technical means, there will be no legal impediment to using such evidence against the accused. It may not be possible, however, to decrypt a device by technical means, or the time required for technical decryption may be years or decades, making such decryption impracticable for prosecution.[6] In such cases, the Government's only option may be to compel the accused to decrypt the device and litigate likely Fifth Amendment based objections.[7]

---

[3] KRISTIN FINKLEA, CONG. RSCH. SERV., R444187, ENCRYPTION AND EVOLVING TECHNOLOGY: IMPLICATIONS FOR U.S. LAW ENFORCEMENT INVESTIGATIONS 4 (2016).

[4] The Third Circuit has explained encryption as follows:

> Encryption technology allows a person to transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process. Only those who possess a corresponding "key" can return the information into its original form, *i.e.* decrypt that information. Encrypted information remains on the device in which it is stored, but exists only in its transformed, unintelligible format.

United States v. Apple MacPro Comput., 851 F.3d 238, 242 n.1 (3d Cir. 2017).

[5] David Nield, *How to Get the Most Out of Your Smartphone's Encryption*, WIRED (Jan. 29, 2020, 8:00 AM), https://www.wired.com/story/smartphone-encryption-apps.

[6] FINKLEA, *supra* note 3, at 9 (discussing the Federal Bureau of Investigation's difficulty in unlocking an iPhone in the San Bernadino shooting case); KRISTIN FINKLEA, CONG. RSCH. SERV., RL 44481, ENCRYPTION AND THE "GOING DARK" DEBATE 1 (2017) (discussing the challenges of "warrant-proof" encryption).

[7] David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection Against Self-Incrimination*, 57 AM. CRIM. L. REV. 157, 157 (2020).

B. Military Subpoena Practice Prior to the Military Justice Act of 2016

Before addressing the ability to overcome an accused's Fifth Amendment objections to compelled decryption, it is necessary to review the mechanism by which the Government would seek to compel decryption. Prior to the enactment of Article 30a, UCMJ, the military justice system lacked a true pre-referral investigative subpoena process. The U.S. Army Criminal Investigation Division (CID), the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations could request Department of Defense (DoD) Inspector General (IG) subpoenas.[8] Despite access to this mechanism, jurisdiction over a respondent's refusal to obey such subpoenas rested with U.S. district courts rather than courts-martial.[9] Additionally, the subject matter of DoD IG subpoenas is limited to subpoenas "necessary in the performance of the functions assigned by this [IG] Act."[10] Thus, a respondent could also challenge a DoD IG subpoena as irrelevant to the DoD IG's mission of investigating fraud, waste, and abuse.[11]

Prior to implementation of the Military Justice Act of 2016 (MJA 2016), military prosecutors did not obtain subpoena power until after referral of charges to a court-martial. Military practice thus contrasted with Federal civilian practice, in which civilian Federal prosecutors could seek grand jury subpoenas during the investigative process. The Military Justice Review Group (MJRG) recommended that Congress bring military practice in this area in line with civilian practice. The MJRG's report and recommendations are discussed in detail in Section III.A. Congress adopted this recommendation by adding Article 30a to the UCMJ and amending Article 46, UCMJ, as part of MJA 2016.[12]

---

[8] U.S. DEP'T OF DEF., DIR. 5106.01, INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE (20 Apr. 2012) (C2, 29 May 2020); *see* United States v. Byard, 29 M.J. 803, 805 (C.M.R. 1989) (describing use of Department of Defense Inspector General subpoenas by Army, Navy, and Air Force investigators).

[9] 5 U.S.C. app. § 6.

[10] *Id.* § 6(a)(4).

[11] Major Joseph B. Topinka, *Expanding Subpoena Power in the Military*, ARMY LAW., Sept. 2003, at 15, 22; Major Stephen Nypaver III, *Department of Defense Inspector General Subpoena*, ARMY LAW., Mar. 1989, at 17, 17.

[12] The Military Justice Act of 2016 (MJA 2016) was part of the National Defense Authorization Act for the Fiscal Year 2017. *See* National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5001, 130 Stat. 2000, 2894 (2016) ("This division may be cited as the 'Military Justice Act of 2016.'").

Serving a subpoena on the subject of an investigation remains a rarity in the military justice system. Indeed, there are no military appellate opinions involving the Government serving a subpoena on the accused. As a result, the use of investigative subpoenas in cases where the accused has an encrypted device will be a new procedure for many military prosecutors and judges. The reasons for this lack of historic practice in courts-martial are both legal and practical. As a legal matter, the Article 30a, UCMJ, investigative subpoena authority and the corresponding jurisdiction of courts-martial to hear motions to quash did not become effective until 1 January 2019.[13] As a practical matter, the issue of encrypted electronic devices is relatively new, and there are far fewer courts-martial than civilian prosecutions, so there have been fewer opportunities to develop case law in the military.

### C. Federal Civilian Grand Jury Subpoena Practice and Decryption

In civilian Federal courts, prosecutors utilize grand jury investigative subpoenas to compel decryption. Federal Rule of Criminal Procedure 17 governs all subpoenas issued in Federal criminal proceedings, including grand jury subpoenas.[14] Rule 17(c)(1) permits a subpoena to "order the witness to produce any books, papers, documents, data, or other objects the subpoena designates."[15] The Rule further provides that "[t]he court may direct the witness to produce the designated items in court before trial or before they are to be offered into evidence."[16] The target of the investigation, like anyone else, may move to quash the subpoena under Rule 17(c)(2).[17]

Regarding subpoenas to the target of an investigation, the Department of Justice's *Justice Manual* provides that "[a] grand jury may properly subpoena a subject or a target of the investigation and question the target about his or her involvement in the crime under investigation."[18] The *Justice Manual* identifies several additional concerns when subpoenaing

---

[13] *Id.* § 5542; Exec. Order No. 13825, 3 C.F.R. 325 (2019).
[14] FED. R. CRIM. P. 17.
[15] *Id.* R. 17(c)(1).
[16] *Id.*
[17] *Id.* R. 17(c)(2).
[18] U.S. Dep't of Just., Just. Manual § 9-11.150 (2017) (citing United States v. Wong, 431 U.S. 174, 179 n.8 (1977); United States v. Washington, 431 U.S. 181, 190 n.6 (1977); United States v. Mandujano, 425 U.S. 564, 573–75, 584 n.9 (1976); United States v. Dionisio, 410 U.S. 1, 10 n.8 (1973)).

the target of an investigation, such as notification of target status and rights advisement. Nevertheless, these concerns are not legal bars to grand jury subpoenas to compel the production of evidence by the target.[19]

Under Federal Rule of Criminal Procedure 17(g), a "court (other than a magistrate judge) may hold in contempt a witness who, without adequate excuse, disobeys a subpoena issued by a federal court in that district."[20] Following noncompliance with a subpoena, a Federal civilian prosecutor will request that a Federal district judge hold the respondent in civil contempt to compel compliance. Federal prosecutors used this procedure to compel decryption in *United States v. Apple MacPro Computer*, discussed below in Section VII.B.1.[21]

### D. The Military Justice Review Group and the Military Justice Act of 2016

As part of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017, MJA 2016 added the Article 30a investigative subpoena power to the UCMJ.[22] With regard to investigative subpoenas, MJA 2016 largely enacted the recommendations of the MJRG, which proposed amendments to the UCMJ to bring military subpoena practice into line with Federal civilian practice.[23] It also extended the military judge's contempt powers to Article 30a, UCMJ, proceedings.[24] As a result, the investigative subpoena power in the UCMJ now mirrors the Federal grand jury subpoena power, although military subpoenas are issued by a judge rather than a grand jury.

Accordingly, like Federal civilian prosecutors' use of the grand jury subpoena power, military prosecutors should be able to use the UCMJ investigative subpoena power to compel a Service member to produce a device in an unencrypted state in cases where the foregone conclusion doctrine renders the act of production non-testimonial under the Fifth Amendment and similar protections in military criminal law. To ensure that such subpoena practice is effective, the Government should (1) lawfully

---

[19] *Id.*
[20] FED. R. CRIM. P. 17(g).
[21] United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017).
[22] National Defense Authorization Act for the Fiscal Year 2017, Pub. L. No. 114-328, § 5202, 130 Stat 2000, 2904 (2016).
[23] MIL. JUST. REV. GRP., REPORT OF THE MILITARY JUSTICE REVIEW GROUP—PART I: UCMJ RECOMMENDATIONS (2015) [hereinafter MJRG REPORT].
[24] UCMJ art. 48(a)(2)(B) (2017).

seize the device pursuant to a search authorization; (2) gather evidence to prove that the accused's ability to decrypt the device is a "foregone conclusion;" (3) draft a subpoena that directs the accused to provide the device in an unencrypted state with any security features disabled at a reasonable time after the service of the subpoena; and (4) if the accused has requested counsel, ensure counsel is present for both service and the accused's opportunity to comply to satisfy concerns under *Edwards v. Arizona*[25] and *United States v. Mitchell*.[26]

## III. The History of the Article 30a, UCMJ, Investigative Subpoena

Proposals to add a pre-referral investigative subpoena to the UCMJ predate the MJRG report and MJA 2016. The MJRG report identifies several prior published calls for an investigative subpoena power.[27] In particular, a 1999 report by the National Academy of Public Administrators recommended granting service general counsel (or other appropriate officials) authority to approve subpoenas.[28] A 2001 DoD IG report noted the need for additional subpoena authority.[29] In 2003, Major Joseph Topinka published an article in *The Army Lawyer* advocating for investigative subpoena power in the military justice system.[30] Additionally, "[i]n 2011, the Department of Defense proposed several amendments to Article 47 in order to address the lack of investigative subpoena power in military practice."[31]

In August 2013, the Joint Chiefs of Staff recommended a "comprehensive and holistic review" of the UCMJ.[32] Following that recommendation, Secretary of Defense Chuck Hagel issued a memorandum

---

[25] Edwards v. Arizona, 451 U.S. 477 (1981).
[26] United States v. Mitchell, 76 M.J. 413, 418 (C.A.A.F. 2017).
[27] MJRG REPORT, *supra* note 23, at 405.
[28] Topinka, *supra* note 11, at 15 (citing NAT'L ACAD. OF PUB. ADM'RS, ADAPTING MILITARY SEX CRIMES INVESTIGATIONS TO CHANGING TIMES 20 (1999)).
[29] *Id.* (citing OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF DEF., REP. NO. CIPO2001S004, EVALUATION OF SUFFICIENCY OF SUBPOENA AUTHORITY WITHIN THE DEPARTMENT OF DEFENSE IN SUPPORT OF GENERAL CRIMES INVESTIGATIONS 2–10 (2001)).
[30] *Id.*
[31] MJRG REPORT, *supra* note 23, at 404 (citing OFF. OF LEGIS. COUNS., U.S. DEP'T OF DEF., SIXTH PACKAGE OF LEGISLATIVE PROPOSALS SENT TO CONGRESS FOR INCLUSION IN THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2012 sec. 532 (2011)).
[32] Memorandum from Chairman of the Joint Chiefs of Staff, to Sec'y of Def. (Aug. 5, 2013), *in* MJRG REPORT, *supra* note 23, at 1263.

"direct[ing] the General Counsel to conduct a comprehensive review of the Uniform Code of Military Justice (UCMJ) and the military justice system with support from military justice experts provided by the Services."[33] Secretary Hagel directed that "a report including a recommendation for any appropriate amendments to the UCMJ be submitted within 12 months and that a second report recommending any appropriate amendments to the MCM be submitted within 18 months."[34]

Acting on Secretary Hagel's direction, the DoD General Counsel established the MJRG. The General Counsel's "Terms of Reference" directed the MJRG to, among other things, "consider the extent to which the principles of law and the rules of procedure and evidence used in the trial of criminal cases in the United States district courts should be incorporated into military justice practice."[35] The MJRG was composed of a full-time staff of judge advocates directed by Judge Andrew Effron, a retired Chief Judge of the Court of Appeals for the Armed Forces (CAAF).[36] The MJRG was further advised by a civilian judge on the U.S. Court of Appeals for the D.C. Circuit, a former DoD General Counsel, and an experienced civilian prosecutor from the Department of Justice.[37] Thus, the MJRG was not simply an effort by judge advocates but a collaborative effort drawing on the experience of judge advocates as well as civilian DoD counsel, judges, and prosecutors.

Military courts have treated provisions of MJA 2016 as having been informed by the MJRG report. In *United States v. Cruspero*[38] and *United States v. Finco*,[39] the Air Force Court of Criminal Appeals (AFCCA) cited the MJRG report when describing the scope of the statutory remand authority in Article 66(f)(3), UCMJ.[40] Judge Ohlson of the CAAF has also described adopting MJA 2016 as Congress acting upon recommendations from the MJRG.[41] Judge Ohlson's remarks are consistent with the history of

---

[33] Memorandum from Sec'y of Def., to Chairman of the Joint Chiefs of Staff et al. (Oct. 18, 2013), *in* MJRG REPORT, *supra* note 23, at 1267.
[34] *Id.*
[35] MJRG REPORT, *supra* note 23, at 14.
[36] *Id.*
[37] *Id.* at 1279–80.
[38] United States v. Cruspero, No. ACM S32595, 2020 WL 6938016, at *6 (A.F. Ct. Crim. App. Nov. 24, 2020).
[39] United States v. Finco, No. ACM S32603, 2020 WL 4289983, at *7 (A.F. Ct. Crim. App. July 27, 2020).
[40] UCMJ art. 66(f)(3) (2021).
[41] United States v. Hale, 78 M.J. 268, 275 (C.A.A.F. 2019) (Ohlson, J., concurring) ("Therefore, upon the MJRG's recommendation, Congress amended Article 2(a)(3), . . . so

MJA 2016. As Professor David Schlueter observes, Congress did not hold hearings specifically addressing MJA 2016 because "Congress was content that the DoD had sufficiently vetted the proposals and believed that hearings would not provide any additional benefit, except for publicity purposes."[42]

### A. The Military Justice Review Group Report

The MJRG published its report on 22 December 2015.[43] Consistent with the General Counsel's directive to consider incorporating civilian practice into military practice, the MJRG recommended revising military subpoena practice to more closely mirror civilian practice by adding a broad subpoena power at the investigative stage.[44] Under the heading "Major Legislative Proposals," the MJRG recommended seven categories of reforms to the UCMJ.[45] Investigative subpoenas were addressed in the second of these seven categories, entitled "Enhance Fairness and Efficacy in Pretrial and Trial Procedures."[46] As part of the effort to enhance pretrial procedures, the MJRG recommended "[e]xpanding authority to obtain documents during investigations through subpoenas and other process."[47]

The MJRG consistently cited to Federal civilian subpoena practice as a model for its proposal to add to the UCMJ what would become the Article 30a subpoena process. In particular, the MJRG noted that "[w]ith respect to subpoena practice, despite the similarities between military subpoenas and subpoenas issued under Fed. R. Crim. P. 17, federal prosecutors and law enforcement agencies have much broader authority to utilize subpoenas during the investigative, pre-indictment (pre-referral) stages of a case."[48] The MJRG cited to Federal grand jury practice in particular as a model for the capabilities proposed to be added to the military justice system. As the MJRG wrote, "Under Fed. R. Crim. P. 6 and 17, federal prosecutors have access to grand jury investigative subpoenas as soon as a grand jury is

---

as to eliminate jurisdictional gaps that previously arose within the interstices of blocks of time dedicated to inactive duty training.") (citation omitted).

[42] David A. Schlueter, *Reforming Military Justice: An Analysis of the Military Justice Act of 2016*, 49 ST. MARY'S L.J. 1, 21 n.90 (2017).

[43] MJRG REPORT, *supra* note 23, at 3.

[44] *Id.* at 14.

[45] *Id.* at 6–8.

[46] *Id.* at 6.

[47] *Id.*

[48] *Id.* at 410 (citations omitted).

summoned, which often happens before the accused is even aware of the investigation or afforded the right to counsel."[49] The MJRG also cited to analogous state prosecutorial investigative subpoena power, noting that, "in many states, prosecutors are given investigative subpoena authority by statute, to be exercised in advance of filing charges with the court or obtaining an indictment."[50]

The MJRG similarly referenced Federal civilian practice when proposing amendments to Articles 46 and 47, UCMJ. As the MJRG explained, its "proposal would amend Articles 46 and 47 to clarify the authority to issue and enforce subpoenas for witnesses and other evidence, and to enhance the Government's ability to use investigative subpoenas prior to trial, consistent with federal and state practice."[51] Specifically, the MJRG report recommended amending Article 46, UMCJ, "to allow the issuance of investigative subpoenas for the production of evidence prior to referral and preferral of charges" because "[*t*]*his will align UCMJ subpoena authority with that in federal and state jurisdictions*, and improve the operation of the military justice system in this area."[52]

The MJRG's analogue to Federal grand jury investigative subpoena power is particularly relevant when dealing with Article 30a, UCMJ, subpoenas to the accused. The Federal civilian grand jury power is used to compel decryption by the subject of an investigation in Federal civilian courts. The MJRG's analysis thus suggests no limitation on the proposed military investigative subpoena power excluding the accused or decryption. Rather, the MJRG report recommended moving the military into harmony with the civilian subpoena power that is deployed to compel decryption by subjects in Federal criminal investigations.

The MJRG recommended amendments to the UCMJ in part to enable obtaining electronic communications under the Stored Communications Act. Indeed, judge advocates may be most familiar with Article 30a, UCMJ, in the context of obtaining orders for the production of stored electronic communications. But the MJRG's references to the Stored Communications Act were not meant to limit the scope of the proposed investigative subpoena power. Rather, the MJRG proposed a broad scope of investigative

---

[49] *Id.*

[50] *Id.* (citing FED. R. CRIM. P. 6, 17; WAYNE LAFAVE ET AL., CRIMINAL PROCEDURE §§ 8.1(c), 8.3(c) (3d ed. 2013); Oman v. State, 737 N.E.2d 1131, 1136 (Ind. 2000); United States v. Santucci, 674 F.2d 624, 627, 632 (7th Cir. 1982)).

[51] *Id.* at 403.

[52] *Id.* at 109 (emphasis added).

subpoena power mirroring the scope of the Federal civilian investigative power. Indeed, it was only after describing the broad subpoena powers available to civilian Federal prosecutors that the MJRG went on to note that "[*i*]*n addition*, federal prosecutors and law enforcement agencies have several available means for obtaining electronic communications and other stored data protected by the Stored Communications Act, including—depending on the classification level of the information sought—grand jury investigative subpoenas, trial subpoenas, and search warrants and court orders."[53] The MJRG report goes on to recommend in a separate point that Congress amend the UCMJ to provide "military judges with the ability to issue warrants and court orders for the production of certain electronic communications under the Stored Communications Act, 18 U.S.C. § 2701 *et seq*."[54]

The MJRG also made clear that an important aspect of the pre-referral subpoena and Article 30a, UCMJ, proceeding was to move the subpoena power to a more useful time in the military justice process. Here, too, the MJRG references the timing of Federal civilian investigative subpoenas as a guide for the proposed reforms to the military process. As the MJRG report notes, "whereas probable cause is not required for the issuance of grand jury subpoenas, the vast majority of military subpoenas are issued post-referral, after the probable cause threshold has already been met. This difference provides Federal prosecutors with a superior investigative tool during the preliminary, investigative stages of a case."[55] The MJRG report goes on to state:

> The optimal time for use of subpoena power often occurs during the conduct of an investigation, making it possible to develop and analyze information for use in the decision as to whether to prefer charges, whether a preliminary hearing should be ordered, and for consideration during a preliminary hearing. The Article 32 proceeding, as recently revised, serves primarily as a preliminary hearing rather than as an investigative tool and will operate most efficiently and effectively when based upon information compiled prior to the hearing.[56]

---

[53] *Id.* at 410 (emphasis added).
[54] *Id.* at 109.
[55] *Id.* at 410 (citing United States v. Williams, 504 U.S. 36, 48 (1992)).
[56] *Id.* at 28.

Accordingly, the MJRG recommended a new investigative subpoena power decoupled from Article 32, UCMJ, proceedings. The sectional analysis for the MJRG's proposed revisions to Article 32, UCMJ, concludes that "the authority to issue pre-referral investigative subpoenas would be governed by a uniform policy that will apply throughout the process prior to referral, and would not be limited narrowly to Article 32 proceedings."[57]

The MJRG also proposes amendments to the contempt sanction using Federal practice as a model. The MJRG report recommends that Congress "extend the contempt power of military judges to pre-referral sessions and proceedings, consistent with the proposed amendments to Art. 26 and the authorities proposed in new Art. 30a."[58] The MJRG likewise proposes making appellate review of contempt punishments imposed in Article 30a proceedings.[59] The MJRG notes that this appellate procedure "will align the UCMJ more closely in this area with the review procedures applicable in federal district courts and federal appellate courts regarding the contempt power."[60]

In sum, while the MJRG report does not specifically address compelled decryption, the MJRG report recommends measures to bring military subpoena practice into line with civilian practice, where the target of an investigation is subject to subpoenas to compel decryption, and the MJRG report provides no indication that the accused in the military would be exempt.

### B. The Legislative History

Article 30a, UCMJ, became law as part of MJA 2016, which was a subset of the FY17 NDAA.[61] The legislative history of the FY17 NDAA does not specifically address the issues of investigative subpoenas to the accused or compelled decryption, nor does it indicate any legislative intent to exempt the accused from Article 30a, UCMJ, subpoena practice. As Professor Schlueter notes, in light of the comprehensive work of the MJRG, Congress did not hold hearings specifically on MJA 2016.[62] Thus, the

---

[57] *Id.* at 330.
[58] *Id.* at 109.
[59] *Id.*
[60] *Id.* at 109–10.
[61] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5202, 130 Stat 2000, 2904 (2016).
[62] Schlueter, *supra* note 42.

legislative history of MJA 2016 consists of the committee reports on the FY17 NDAA, the conference report, and a few statements of legislators.

*1. The Committee Reports*

The Senate Armed Services Committee report on the FY17 NDAA summarily recommended adding an investigative subpoena power to the UCMJ and authorizing its enforcement by contempt in pre-referral proceedings. Specifically, the committee's report simply recommended "add[ing] a new section 830a (Article 30a of the Uniform Code of Military Justice (UCMJ)) to provide statutory authority for military judges or magistrates to provide timely review, prior to referral of charges, of certain matters currently subject to judicial review only on a delayed basis at trial."[63] Regarding subpoenas and other processes, the report went on to recommend amending Article 46, UCMJ:

> to clarify authority to issue and enforce subpoenas for witnesses and other evidence, to allow subpoenas *duces tecum* to be issued for investigations of offenses under the UCMJ when authorized by a general court-martial convening authority, and to authorize military judges to issue warrants and orders for the production of stored electronic communications . . . .[64]

The committee report did not address judge-issued pre-referral investigative subpoenas. That provision would be added later in conference with the House of Representatives. Regarding enforcement, the committee report recommended amending Article 48, UCMJ, "to authorize the contempt power for military judges and military magistrates detailed to pre-referral proceedings under the proposed Article 30a."[65]

The House Armed Services Committee report does not address the issue of pre-referral investigative subpoenas.[66] The initial House version of the FY17 NDAA did not contain a provision similar to Article 30a, UCMJ.[67]

---

[63] S. REP. NO. 114-255, at 599 (2016).
[64] *Id.* at 602.
[65] *Id.*
[66] *See generally* H.R. REP. NO. 114-537 (2016).
[67] *See generally* H.R. 4909, 114th Cong. (2016).

*2. The Conference Report*

The final language of Article 30a, UCMJ, was settled in the conference committee. The provision empowering military judges to issue pre-referral investigative subpoenas in addition to warrants and orders for stored electronic communications was added in the conference committee. Like the Senate committee report, the conference report does not specifically address the issue of compelled decryption. Yet, here too, there is no indication of legislative intent to limit the scope of the newly-created investigative subpoena power to exclude the accused.

Section 5202 of the FY17 NDAA, entitled "Certain proceedings conducted before referral," would ultimately contain the newly-enacted Article 30a, UCMJ.[68] The conference report noted that the Senate's version of the FY17 NDAA contained the new Article 30a, UCMJ, providing "statutory authority for military judges or magistrates to provide timely review, prior to referral of charges, of certain matters currently subject to judicial review only on a delayed basis at trial"[69] while the House version lacked such a provision. To resolve this difference, "[t]he House recede[d] with an amendment that would limit the matters which may be reviewed prior to referral of charges to pre-referral investigative subpoenas, pre-referral warrants or orders for electronic communications, and pre-referral matters referred by an appellate court."[70] There is no indication that this resolution was controversial or that the House sought to limit the subject matter or recipients of pre-referral investigative subpoenas.

The conference report concerning section 5228 of the FY17 NDAA, entitled "Subpoena and other process" followed a similar pattern. The conference report noted that the Senate bill included a version of section 5228 "to clarify the authority to issue and enforce subpoenas for witnesses and other evidence, to allow subpoenas duces tecum to be issued for investigations of offenses under the UCMJ when authorized by a general court-martial convening authority, and to authorize military judges to issue

---

[68] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5202, 130 Stat 2000, 2904 (2016).

[69] S. REP. NO. 114-255, at 599.

[70] H.R. REP. NO. 114-840, at 1516 (Conf. Rep.). "The terms *recede, insist,* and *adhere* have technical meanings in the legislative process. When the House or Senate 'recedes,' it withdraws from a previous position or action. . . ." ELIZABETH RYBICKI, CONG. RSCH. SERV., RESOLVING LEGISLATIVE DIFFERENCES IN CONGRESS: CONFERENCE COMMITTEES AND AMENDMENTS BETWEEN THE HOUSES 6 n.11 (2019).

warrants and orders for [Stored Communications Act materials]."[71] In response, the House of Representatives "recede[d] with an amendment that would authorize a military judge to issue an investigative subpoena before referral of charges to a court-martial."[72] Here, too, there is no indication that either the House or Senate sought to limit the scope of the subpoena power to exclude the accused.

The MJA 2016 revisions to Article 48, UCMJ, followed a similar pattern. Regarding the contempt power of military judges, the Senate bill contained a version of section 5230 amending Article 48, UCMJ, "to authorize the contempt power for military judges and military magistrates detailed to pre-referral proceedings under the proposed Article 30a."[73] The Senate bill further provided for "appellate review of contempt punishments consistent with the review of other orders and judgments under the UCMJ."[74] The House bill contained a similar (but not identical) provision amending Article 48, UCMJ, and "[t]he House recede[d] with an amendment that would exclude commissioned officers detailed as a summary court-martial from the officials authorized to punish a person for contempt."[75] There is no indication that the contempt power of military judges was controversial.

*3. Legislators' Statements*

The statements of legislators concerning the FY17 NDAA do not specifically address the investigative subpoena provision of MJA 2016. Rather, when addressing MJA 2016, the legislators' comments are general compliments for the MJRG report and modernization of the military justice system.

Senator John McCain of Arizona provided the most substantive commentary on MJA 2016 in either chamber's debates on the bill. Senator McCain remarked:

> The NDAA also implements the recommendations of the Department of Defense Military Justice Review Group by incorporating the Military Justice Act of 2016. The legislation modernizes the military court-martial trial

[71] H.R. REP. NO. 114-840, at 1519 (Conf. Rep.).
[72] *Id.*
[73] *Id.*
[74] *Id.* at 1519–20.
[75] *Id.* at 1520.

> and appellate practice, incorporates best practices from Federal criminal practice and procedures, and increases transparency and independent review in the military justice system.
>
> Taken together, the provisions contained in the NDAA constitute the most significant reforms to the Uniform Code of Military Justice in a generation. . . .[76]

Senator McCain's reference to the MJRG report provides at least some evidence that the MJRG report should be considered when determining legislative intent in enacting the MJA 2016. Moreover, Senator McCain's favorable description of modernizing military justice by incorporating best practices from Federal civilian criminal practice and procedure may be read to support interpreting MJA 2016 in a manner that harmonizes military practice with Federal civilian practice. Nevertheless, these were a sole senator's brief remarks that did not specifically address subpoenas issued to an accused.

Remarks on MJA 2016 in the House of Representatives were even more brief praise for modernization of the military justice system and steps to prosecute sexual assault, though these remarks did not specifically mention investigative subpoenas. Representative Mac Thornberry of Texas stated, "We have the first comprehensive rewrite of the Uniform Code of Military Justice in 30 years, and that is a big part of the reason that this bill is the size that it is."[77] Representative Denny Heck of Washington stated, "It modernizes the Uniform Code of Military Justice to improve the system's efficiency and transparency, while also enhancing victims' rights."[78] Representative Michael Turner of Ohio stated, "This bill calls for continued action to eradicate sexual assault in the military by providing greater transparency in the military criminal justice system."[79] Representative Bradley Byrne of Alabama stated, "It also updates the Uniform Code of Military Justice to promote accountability within our military."[80]

In sum, there is nothing in these legislators' statements to suggest that Articles 30a or 46, UCMJ, should be interpreted in a manner contrary to their plain text. To the extent that any intent can be gleaned from these

---

[76] 162 CONG. REC. S6871 (daily ed. Dec. 8, 2016) (statement of Sen. John McCain).
[77] 162 CONG. REC. H7123 (daily ed. Dec. 2, 2016) (statement of Rep. William Thornberry).
[78] *Id.* at H7130 (statement of Rep. Dennis Heck).
[79] *Id.* at H7126 (statement of Rep. Michael Turner).
[80] 162 CONG. REC. H7069-06, H7070 (daily ed. Dec. 1, 2016) (statement of Rep. Bradley Byrne).

statements, such intent would be to interpret MJA 2016 reforms in a manner consistent with the analogous civilian practice relied upon in the MJRG report.

## IV. A Textual Analysis of Articles 30a and 46, UCMJ, and Implementation in the Rules for Courts Martial Following the Military Justice Act of 2016

To determine the applicability of Article 30a, UCMJ, subpoenas to the accused, one must first analyze the text of the statute. Like civilian courts,[81] military courts of appeals have embraced textualism in statutory interpretation. Although an accused might argue that Congress did not intend for investigative subpoenas to apply to an accused, there is no such limitation in the statutory text. Writing for the CAAF in *United States v. Bergdahl*, Judge Ohlson stated, "Any suggestion that we should interpose additional language into a rule that is anything but ambiguous is the antithesis of textualism."[82] In support of this statement, Judge Ohlson's majority opinion cited statements by three sitting Supreme Court Justices: "We're all textualists now" (Justice Kagan);[83] "The text of the law is the law" (Justice Kavanaugh);[84] and "The text of the statute and only the text becomes law. Not a legislator's unexpressed intentions . . ." (Justice Gorsuch).[85]

The CAAF applied similar reasoning in *United States v. McPherson*.[86] In that case, Chief Judge Stucky wrote for the majority that there was no geographic limitation on the Article 12, UCMJ,[87] prohibition on confining Service members with foreign nationals based on the article's text, which was "plain on its face."[88] In support, the court cited to the majority opinion in *Barnhart v. Sigmon Coal Co.*, in which Justice Thomas wrote:

---

[81] Jesse D.H. Snyder, *How Textualism Has Changed the Conversation in the Supreme Court*, 48 U. BALT. L. REV. 413 (2019).
[82] United States v. Bergdahl, 80 M.J. 230, 235 (C.A.A.F. 2020), *reconsideration denied*, 80 M.J. 362 (C.A.A.F. 2020).
[83] *Id.* (citing Harvard Law School, *The 2015 Scalia Lecture | A Dialogue with Justice Elena Kagan on the Reading of Statutes*, YOUTUBE (Nov. 25, 2015), https://youtu.be/dpEtszFT0Tg).
[84] *Id.* (citing Brett Kavanaugh, *Fixing Statutory Interpretation*, 129 HARV. L. REV. 2118, 2118 (2016) (reviewing ROBERT A. KATZMANN, JUDGING STATUTES (2014))).
[85] *Id.* (citing NEIL GORSUCH, A REPUBLIC, IF YOU CAN KEEP IT 132 (2019)).
[86] United States v. McPherson, 73 M.J. 393, 395 (C.A.A.F. 2014).
[87] UCMJ art. 12 (2016).
[88] *McPherson*, 73 M.J. at 395.

> As in all statutory construction cases, we begin with the language of the statute. The first step "is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case." The inquiry ceases "if the statutory language is unambiguous and 'the statutory scheme is coherent and consistent.'"[89]

The Court likewise cited to Justice Thomas's majority opinion in *Connecticut National Bank v. Germain*[90] for the propositions that "courts must presume that a legislature says in a statute what it means and means in a statute what it says there" and "[w]hen the words of a statute are unambiguous, then, this first canon is also the last: judicial inquiry is complete."[91]

A. The Text of Article 30a, UCMJ

Article 30a(a), UCMJ, provides that the President shall make regulations related to pre-referral investigative subpoenas.[92] The text of Article 30a(a)(1)(A), UCMJ, places restrictions on neither the proper recipients of an investigative subpoena nor the subject matter of such a subpoena.[93] Only Article 30a(a)(1)(B), UCMJ, is modified by the purpose of issuing warrants or orders for electronic communications.[94] Article 30a(a)(1)(A), UCMJ, contains no such limitation (or any other). The contrast between the text of Articles 30a(a)(1)(A) and 30a(a)(1)(B), UCMJ, is significant. Congress demonstrated that it knew how to limit the scope or purpose of the powers it created, yet chose not to include any such limitation in the text of Article 30a(a)(1)(A), UCMJ.

Arguments for implied limitations on the Article 30a(a)(1)(A), UCMJ, subpoena power thus must fail in light of the CAAF's admonition in *Bergdahl* that "Any suggestion that we should interpose additional language

---

[89] Barnhart v. Sigmon Coal Co., Inc., 534 U.S. 438, 450 (2002) (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 340 (1997)).
[90] Conn. Nat'l Bank v. Germain, 503 U.S. 249, 253–54 (1992).
[91] *McPherson*, 73 M.J. at 395 (quoting *Germain*, 534 U.S. at 253–54).
[92] UCMJ art. 30a(a)(1)(A) (2019).
[93] *Id.*
[94] *Id.* art. 30a(a)(1)(B).

into a rule that is anything but ambiguous is the antithesis of textualism."[95] The CAAF's refusal in *McPherson* to read implied limitations into Article 12, UCMJ, based on policy considerations is likewise instructive.[96] Limiting Article 12, UCMJ, to make it inapplicable to civilian confinement in the United States might have made practical sense, but the text lacked any such limitation and the Court would not add it.[97] In the case of Article 30a, UCMJ, there is no similar policy argument for excluding the accused given that grand jury subpoenas are how civilian courts compel decryption.

Although the plain text of Article 30a(a)(1)(A), UCMJ, should end the inquiry from a textualist perspective, the context of the article further confirms the broad scope of the investigative subpoena power. Like Article 30a(a)(1), UCMJ, Article 30a(b), UCMJ, does not impose limits on the subject matter of the investigative subpoena or to whom such a subpoena may be directed. Indeed, the only restrictive language in Article 30a(b), UCMJ, requires Article 30a, UCMJ, proceedings to address only matters that a military judge could consider in a court-martial.[98] The President has the discretion to impose additional limitations under Article 30a(a)(2)(D), UCMJ, but the statutory language stating "may be ordered . . . as the President considers appropriate" in this subsection makes clear that any such additional limitations are not mandated by Congress but rather are at the President's discretion.[99]

In sum, by the plain text of Article 30a, UCMJ, any limitations on the subject matter or recipient of Article 30a, UCMJ, subpoenas must be found in the rules prescribed by the President because such limitations are not in the statute. As presented in Section IV.C below, the President has imposed no such limitations.

### B. The Text of Article 46, UCMJ

The accused or other Service members are subject to subpoenas to obtain evidence issued under Article 46, UCMJ, which governs subpoenas and other process.[100] Article 46(b), UCMJ, provides that any subpoena

---

[95] United States v. Bergdahl, 80 M.J. 230, 235 (C.A.A.F. 2020), *reconsideration denied*, 80 M.J. 362 (C.A.A.F. 2020).
[96] United States v. McPherson, 73 M.J. 393, 395 (C.A.A.F. 2014).
[97] *Id.*
[98] UCMJ art. 30a(b).
[99] *Id.* art. 30a(a)(2)(D).
[100] *Id.* art. 46 (2016).

issued under that article "shall be similar to that which courts of the United States having criminal jurisdiction may issue; shall be executed in accordance with regulations prescribed by the President; and shall run to any part of the United States . . . ."[101] There is no carve-out for an accused or anyone else subject to the UCMJ as a subpoena recipient.

Subpoenas for the production of evidence fall under Article 46(d), UCMJ.[102] Article 46(d)(1)(C), UCMJ, provides that a subpoena "[m]ay be issued to compel production of evidence for an investigation of an offense under this chapter."[103] There is no exemption for the accused. Article 46(d)(2), UCMJ, addresses the authority to issue subpoenas pre-referral, providing that

> [a]n investigative subpoena under paragraph (1)(C) may be issued before referral of charges to a court-martial only if a general court-martial convening authority has authorized counsel for the Government to issue such a subpoena or a military judge issues such a subpoena pursuant to section 830a of this title (article 30a).[104]

Here, too, there is no carve-out for the accused.

The plain text of Article 46, UCMJ, thus provides for pre-referral investigative subpoenas like those in civilian courts, and nothing in the text of the article exempts an accused. Therefore, applying the CAAF's reasoning from *Bergdahl*, there is no basis for a court to "interpose additional language into a rule that is anything but ambiguous."[105] Moreover, even if there are prudential or policy arguments for exempting an accused, judicial imposition of such non-textual restraints would run afoul of the CAAF's reasoning in *McPherson*,[106] in which the CAAF refused to allow prudential concerns to read a non-textual exception into Article 12, UCMJ.

---

[101] *Id.*
[102] *Id.* art. 46(d).
[103] *Id.* art. 46(d)(1)(C).
[104] *Id.* Prior to MJA 2016, the Article 46, UCMJ, provision concerning subpoenas simply read: "Process issued in court-martial cases to compel witnesses to appear and testify and to compel the production of other evidence shall be similar to that which courts of the United States having criminal jurisdiction may lawfully issue and shall run to any part of the United States . . . ." UCMJ art. 46 (1956).
[105] United States v. Bergdahl, 80 M.J. 230, 235 (C.A.A.F. 2020), *reconsideration denied*, 80 M.J. 362 (C.A.A.F. 2020).
[106] United States v. McPherson, 73 M.J. 393, 395 (C.A.A.F. 2014).

C. The Text of the Rules for Courts-Martial Implementing Articles 30a and 46, UCMJ

Under the authority Congress provided in Article 30a, UCMJ, the President set forth rules governing the Article 30a, UCMJ, subpoena power in Executive Order 13825.[107] These amendments to the Rules for Courts-Martial (RCMs) do not contain any limitation exempting the accused or decryption from the scope of Article 30a, UCMJ, investigative subpoenas. Rather, RCM 309, entitled "Pre-referral judicial proceedings," mirrors Article 30a(a)(1)(A), UCMJ, in that no restriction is placed in the recipient or subject matter of an Article 30a, UCMJ, subpoena in RCM 309(b)(1). Likewise, mirroring Article 30a(a)(1)(B), RCM 309(b)(2) only limits the purpose of pre-referral warrants or orders—not investigative subpoenas—to electronic communications.

Rule for Courts-Martial 309(b)(3) provides procedures for relief from a subpoena. The text of the rule provides that "[a] person in receipt of a pre-referral investigative subpoena . . . may request relief on grounds that compliance with the subpoena or order is unreasonable, oppressive or prohibited by law."[108] The rule goes on to state that "[t]he military judge shall review the request and shall either order the person or service provider to comply with the subpoena or order, or modify or quash the subpoena or order as appropriate."[109] Here, too, the recipient of an investigative subpoena and the subject of the judge's order are described only as a "person" with no limitation excluding the accused.

In RCM 703(g)(3)(C), the provision referenced in RCM 309(b), the President likewise imposes no limitation that would shield an accused from a pre-referral investigative subpoena. Rather, the language of RCM 703(g)(3)(C)(i) states:

> In the case of a subpoena issued before referral for the production of evidence for use in an investigation, the subpoena shall command each person to whom it is directed to produce the evidence requested for inspection by the Government counsel who issued the subpoena or

---

[107] Exec. Order No. 13825, 3 C.F.R. 325 (2019). The executive order amended the *Manual for Courts-Martial. Id.*

[108] MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 309(b)(3) (2019) [hereinafter MCM].

[109] *Id.*

> for inspection in accordance with an order issued by the military judge under R.C.M. 309(b).[110]

Regarding the matters subject to subpoena, RCM 703(g)(3)(A) states, "The presence of witnesses not on active duty and evidence not under control of the Government may be obtained by subpoena."[111] Rule for Courts-Martial 703(g) thus provides for obtaining evidence broadly without any limitation shielding the accused.

Procedural rules related to investigative subpoenas likewise provide no indication that the President sought to exclude the accused from subpoenas for evidence. Rule for Courts-Martial 703(g)(3)(E), which concerns service, simply says that a subpoena shall be served by delivering a copy "to the person named" with no exclusion for the accused. With respect to motions to quash, RCM 703(g)(3)(G) allows a court to either "order that the subpoena be modified or quashed, as appropriate" or "order the person to comply with the subpoena."[112] Here, like in the UCMJ, these procedural rules use the broad term "person" rather than a term that would exclude an accused.

The only provision of RCM 703 that excludes Service members from subpoenas is the procedure for obtaining witnesses in RCM 703(g)(1), which simply provides that military witnesses may be obtained by requesting that the Service member's commander order the witness to attend.[113] This rule provides an easier means for compelling the attendance of military witnesses at a court-martial based on a commander's authority to order attendance. Nothing in RCM 703(g)(1) indicates that the President sought to exempt Service members from subpoenas for evidence.

In sum, the plain text of Articles 30a and 46, UCMJ, leaves any limitation excepting the accused from the Article 30a, UCMJ, investigative subpoena power to regulations prescribed by the President. But, if the President had intended to exclude the accused from the scope of pre-referral investigative subpoenas, surely the President would have made that clear when revising the RCMs after the enactment of Article 30a, UCMJ, particularly given the well-established Federal civilian practice of the accused being subject to subpoena.

---

[110] *Id.* R.C.M. 703(g)(3)(C)(i).
[111] *Id.* R.C.M. 703(g)(3)(A).
[112] *Id.* R.C.M. 703(g)(3)(F)(i)–(ii).
[113] *Id.* R.C.M. 703(g)(1).

## V. The Subpoena and the Search Authorization

The Article 30a, UCMJ, subpoena is merely a tool for obtaining the unencrypted state of the device. The subpoena itself does not grant the Government authority to search or seize the device. The authority to search or seize the device must be based upon a valid search authorization. Thus, prior to issuing a subpoena to obtain a device in an unencrypted state, the Government must first obtain authorization to seize and search the device. The Government should also execute the seizure as soon as possible and store the device in a way that renders remote access impossible to preserve evidence pending service of the subpoena.

Any search of the accused's device in an unencrypted state must remain within the scope of the search authorization.[114] The Article 30a, UCMJ, subpoena, however, need not necessarily refer to the search authorization. Indeed, the Government need only describe the matters to be inspected in the subpoena if the Government is taking the conservative approach to subpoena drafting under the Eleventh Circuit's *In re Grand Jury Subpoena* opinion.[115] The scope of the authorization and the search will be valid or invalid on their own terms separate from the subpoena.

The language of the subpoena should specify the state of each particular device at issue that will allow for an effective search. The necessary state of the device will depend on the type of device and the type of search the Government wishes to conduct. For example, a subpoena regarding a mobile phone might require that the accused produce the phone in an unlocked state with all locking (and re-locking) features disabled. A subpoena for an encrypted hard drive might require the hard drive to be produced in a decrypted state. The necessary subpoena language might differ from device to device and could change over time as devices and encryption features evolve. Thus, it is incumbent on judge advocates to consult with law enforcement agents and the DoD Cyber Crime Center to ensure that subpoena language directs the device at issue be produced in a state that will allow for an effective search. The foregone conclusion doctrine would govern a court's inquiry in any case.

---

[114] *See* United States v. Osorio, 66 M.J. 632, 637 (A.F. Ct. Crim. App. 2008) ("[W]hen dealing with search warrants for computers, there must be specificity in the scope of the warrant which, in turn, mandates specificity in the process of conducting the search.").

[115] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012).

## VI. Enforcement of Subpoenas to Compel Decryption in Military Courts

The UCMJ provides two avenues for enforcement of a subpoena if a Service member refuses to provide a device in an unencrypted state. The first is the military judge's contempt power under Article 48, UMCJ, and RCM 809. The second is follow-up prosecution for the same conduct under the UCMJ. Disobeying a judge's order compelling an accused to obey a subpoena could be prosecuted under Articles 90, 92(2), 131b, or 131f(2), UCMJ.[116] Article 133, UCMJ, could also apply if the accused is an officer.[117]

Like issuing a subpoena to an accused, contempt of court itself is a rarity in the military justice process. The reasons for this rarity are both practical and legal. Practically, the contempt power is rarely used simply because contemptuous conduct is rare. In the limited case law that exists, the most common contemners are civilian defense counsel, yet even this is rare.[118] Legally, appellate opinions on contempt are rare because punishment for contempt under the military judge's contempt power was not appealable to the service courts of criminal appeals until the FY17 NDAA.[119] As such, a military judge's contempt findings would be subject to appellate opinions only by way of arguments that the contempt finding prejudiced an accused on the merits of the case.[120] A conviction for contempt of court in a follow-on prosecution under the UCMJ has never made its way into a military appellate court opinion. Therefore, military appellate opinions on contempt of court are few and far between.

The best overview of the contempt sanctions available against a Service member is in Judge Cox's dissent in *United States v. Burnett*.[121] That case involved a civilian defense counsel held in contempt for in-court conduct,

---

[116] Because enumerated articles exist to address conduct, Article 134, UCMJ, would likely be preempted.
[117] UCMJ art. 133 (1950).
[118] *See, e.g.*, United States v. Burnett, 27 M.J. 99, 108 (C.M.A. 1988) (Cox, J., dissenting) ("One of the most difficult jobs for any military judge is to deal with a sarcastic, 'catty,' insulting, disrespectful civilian attorney . . . .").
[119] National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5230, 130 Stat. 2000, 2913–14 (2016). Prior to the National Defense Authorization Act for Fiscal Year 2017, the convening authority reviewed contempt judgments under Rule for Courts-Martial 809. MANUAL FOR COURTS-MARTIAL, UNITED STATES, R.C.M. 809 (2016) [hereinafter 2016 MCM]; *Burnett*, 27 M.J. at 108 (noting that contempt judgments were not appealable at the time).
[120] *See, e.g.*, *Burnett*, 27 M.J. at 108 (Cox, J., dissenting).
[121] *Id.*

an obsolete contempt standard,[122] and a since-repealed contempt procedure, so the majority's holding and Judge Cox's specific disagreement with that holding have little relevance today.[123] Yet Judge Cox's explanation of options for dealing with a military contemner remains instructive. Judge Cox explained that "[i]f the contemner is a military person, Articles 89, 90, and 91, as well as Articles 133 and 134 . . . provide ample authority for dealing with the contemptuous conduct and handle it much more severely than does Article 48."[124] When prosecuting a Service member in a separate court-martial, these options remain as valid today as when Judge Cox described them in *Burnett*. Such follow-on prosecution under the UCMJ, of course, is not available against civilian contemners, where "[e]nforcement of a duly issued subpoena is initially a military judge function, followed if necessary by enforcement in a federal court."[125]

Unlike civilian Federal courts, there is no civil contempt in courts-martial. Rule for Courts-Martial 201 states that "[t]he jurisdiction of courts-martial is entirely penal or disciplinary."[126] Civilian Federal judges,

---

[122] At the time of *Burnett*, Article 48, UCMJ, read as follows:

> A court-martial, provost court, or military commission may punish for contempt any person who uses any menacing word, sign, or gesture in its presence, or who disturbs its proceedings by any riot or disorder. The punishment may not exceed confinement for 30 days or a fine of $100, or both.

*Id.* at 103–04 (citing UCMJ art. 48 (1956)).

[123] *Burnett* occurred at a time after the creation of the office of military judge in military courts but while the Article 48, UCMJ, power to punish contempt still rested with the "court-martial" (i.e., the members). Thus, the trial judge instructed the members on contempt procedures, and the members sentenced the civilian defense counsel to a fine of $100 and a reprimand. *Id.* at 103. The majority found error because the conduct at issue was not contemptuous under the narrow language of the then-current Article 48, UCMJ. *Id.* at 105–06. The majority also commented that the version of Article 48 under consideration was an "anachronism . . . made obsolete by the Military Justice Act of 1968" which created the office of military judge. *Id.* at 107. The Court of Military Appeals thus remanded to determine if the accused had been prejudiced by the wrongful contempt ruling against the civilian defense counsel. *Id.* at 108.

[124] *Id.* (Cox, J., Dissenting). Judge Cox also argued that Congress should amend Article 48, UCMJ, to provide military judges "limited summary contempt powers that are clearly applicable to military and civilian persons alike" because, at the time, that article had not been updated to reflect creation of the office of military judge. *Id.* Congress would later enact such an amendment to Article 48, UCMJ, in the Ike Skelton National Defense Authorization Act for Fiscal Year 2011. Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. 111-383, § 542, 124 Stat. 4173, 4218.

[125] United States v. Morrison, No. 9600461, 2005 CCA LEXIS 515, at *27 (A. Ct. Crim. App. July 5, 2005).

[126] MCM, *supra* note 108, R.C.M. 201(a).

by contrast, have the option of civil contempt where a person disobeys a subpoena or court order. The Department of Justice *Criminal Resource Manual* explains that civil contempt sanctions "are designed to compel future compliance with a court order."[127] This form of contempt is "coercive and avoidable through obedience" and "thus may be imposed in an ordinary civil proceeding upon notice and an opportunity to be heard. Neither a jury trial nor proof beyond a reasonable doubt is required."[128] For example, civilian trial judges imposing civil contempt to compel decryption was at issue in *United States v. Apple MacPro Computer*[129] and *In re Grand Jury Subpoena Duces Tecum*.[130]

Criminal contempt, by contrast, serves as post-hoc punishment for wrongdoing—"a crime in the ordinary sense."[131] Unlike civil contempt, which may be avoided through obedience, "criminal penalties may not be imposed on someone who has not been afforded the protections that the Constitution requires of such criminal proceedings."[132] As court-martial jurisdiction is "entirely penal or disciplinary," the only procedures for contempt in the military justice system are a punishment for wrongdoing, whether administered by a military judge under Article 48, UCMJ, or in follow-on prosecution under the UMCJ. Additionally, as a practical matter, the military lacks standing courts to provide ongoing supervision of civil contempt proceedings. Yet the UMCJ's criminal sanctions, and the ex-ante threat of their imposition, can serve much the same function for Service members in the military setting. Thus, although military courts lack civil contempt authority, a military judge can order a member to comply with a subpoena under RMC 309(b)(3) with the support of the contempt power in Article 48, UCMJ, and the threat of subsequent prosecution.

### A. The Military Judge's Contempt Power Under Article 48, UCMJ

Service members ordered to comply with a subpoena in an Article 30a, UCMJ, proceeding are subject first to the military judge's contempt power under Article 48, UCMJ. Article 48(a)(1)(C), UCMJ, allows a "judicial

---

[127] U.S. Dep't of Just., Crim. Res. Manual § 754 (2020).
[128] *Id.* (quoting International Union, UMWA v. Bagwell, 512 U.S. 821 (1994)).
[129] United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017).
[130] United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012).
[131] U.S. Dep't of Just., *supra* note 127 (quoting Bloom v. Illinois, 391 U.S. 194, 201 (1968)).
[132] *Id.* (quoting Hicks v. Feiock, 485 U.S. 624, 632 (1988)).

officer" to "punish for contempt any person" who "willfully disobeys a lawful writ, process, order, rule, decree, or command issued with respect to the proceeding."[133] Article 48(a)(2)(B), UCMJ, provides that a "judicial officer" includes "any military judge detailed to a court-martial, a provost court, a military commission, or any other proceeding under [the UCMJ]."[134] Such a judicial officer may impose as punishment confinement for thirty days, a fine of $1,000, or both.[135] Under Article 66(h), UCMJ, a person subject to contempt punishment may appeal such a punishment to the service court of criminal appeals pursuant to procedures established by the service Judge Advocate General.[136] In the case of disobedience of an order to comply with an Article 30a, UCMJ, subpoena, the disobedience would likely occur outside the presence of the military judge, so the military judge would exercise the contempt power through disposition upon notice and hearing under RCM 809(b)(2). If the military judge directly witnesses the disobedience, summary disposition under RCM 809(b)(1) would be appropriate.

Nothing in the UCMJ or the RCMs exempts an accused or disobedience of orders regarding decryption from the military judge's contempt power. Indeed, Article 48, which governs contempt, expressly applies to "any person," with no carve-out for the accused. The *MCM*'s discussion of RCM 809(a) further clarifies that "[t]he words 'any person,' as used in Article 48, include all persons, whether or not subject to military law, except the military judge, members, and foreign nationals outside the territorial limits of the United States who are not subject to the UCMJ."[137]

### B. Prosecution Under the UCMJ

Service members are subject to prosecution under the UCMJ in addition to the military judge's contempt power. Disobeying a military judge's order enforcing a subpoena could violate Articles 90, 92(2), 131b, 131f(2), and 133, UCMJ. Although the accused's conduct would be factually sufficient under any of these articles, the offenses of obstruction of justice under Article 131b, UCMJ, and noncompliance with procedural rules under

---

[133] UCMJ art. 48(a)(C) (2017).
[134] *Id.* art. 48(a)(1)(C).
[135] *Id.* art. 48(b).
[136] *Id.* art. 66(h).
[137] MCM, *supra* note 108, R.C.M. 809(a) discussion.

Article 131f(2), UCMJ, are most applicable, as these are specific to the military justice process and case law supports their application.

*1. Disobeying Orders Under Articles 90 or 92, UCMJ*

Refusal to comply with an Article 30a, UCMJ, subpoena and a judge's order to comply would first constitute disobeying the order of a superior commissioned officer under Article 90, UCMJ, or disobeying another lawful order under Article 92(2), UCMJ. Disobedience of the judge's order compelling obedience of a subpoena would satisfy the elements of Articles 90 or 92(2), UCMJ. Article 90, UCMJ, requires (1) a lawful order; (2) from a superior commissioned officer of the accused; (3) known by the accused to be the accused's superior commissioned officer; and (4) willful disobedience.[138] Article 92(2), UCMJ, requires (1) a lawful order; (2) the accused's knowledge of the order; (3) a duty to obey the order; and (4) a failure to obey.[139] In a case involving a military judge's order, these offenses are functionally identical, save the Article 90, UCMJ, requirement that the person issuing the order be the superior commissioned officer of the accused.

Judge Cox's dissent in *Burnett* suggests that a military judge's order would be enforced under Article 90, UCMJ.[140] Although judge advocates may not colloquially consider a military judge's order as enforceable under Articles 90 or 92(2), UCMJ, nothing in those articles excludes a military judge's order from their scope. There has not been a military appellate case involving prosecution under Articles 90 or 92, UCMJ, for disobeying a military judge's order. But, in most cases, such prosecution would be unnecessary to give a judge's order force because the UCMJ and the RCMs provide judges with other remedies in the course of a court-martial (e.g., suppression of evidence, unfavorable instructions, dismissal of charges).[141]

Despite a lack of historic examples, military judges, as commissioned officers of the Armed Forces, have the authority to issue orders enforceable under Articles 90 or 92(2), UCMJ. In the vast majority of cases, the military judge will be a superior officer relative to the accused, so the judge's order will be the order of a superior officer under Article 90, UCMJ. In the rare

---

[138] UCMJ art. 90 (2016); MCM, *supra* note 108, pt. IV, ¶ 16.
[139] UCMJ art. 92(2) (1950); MCM, *supra* note 108, pt. IV, ¶ 18.
[140] United States v. Burnett, 27 M.J. 99, 108 (C.M.R. 1988) (Cox, J., dissenting).
[141] *See, e.g.*, MCM, *supra* note 108, R.C.M. 905–907.

cases where the accused outranks the presiding military judge, Congress (in the UCMJ) and the President (in the RCMs) will have conferred on the judge the authority to give lawful orders to the accused relating to the proceeding, the disobedience of which could be punished under Article 92(2), UCMJ. An officer's authority under Article 90, UCMJ, "may be based on law, regulation, custom of the Service, or applicable order to direct, coordinate, or control the duties, activities, health, welfare, morale, or discipline of the accused."[142] Under RCM 801(a)(3), the military judge "is the presiding officer in a court-martial" and shall "exercise reasonable control over the proceedings to promote the purposes of these rules and this Manual."[143] Additionally, RCM 309(b)(3) provides that a military judge reviewing a request for relief from an Article 30a, UCMJ, subpoena "shall either order the person or service provider to comply with the subpoena or order, or modify or quash the subpoena or order as appropriate." Rules for Courts-Martial 801 and 309, part of the *MCM* issued by Executive Order, thus provide authority for the military judge's order.

The lawfulness of a judge's order would thus turn on the applicability of the foregone conclusion doctrine. As discussed in Parts III and IV, nothing in the UCMJ or the RCMs excludes subpoenas issued to the accused from this authority. Thus, the only question of lawfulness would be whether the accused may lawfully claim the Fifth Amendment privilege against self-incrimination. That question turns on the applicability of the foregone conclusion doctrine to the facts of the particular case. As explained in Part VII, if the foregone conclusion doctrine applies, the right against self-incrimination no longer shields the accused from the duty to provide the device in an unencrypted state. There being no other impediment to the lawfulness of the order, it would be lawful and the accused's refusal would violate Articles 90 or 92(2), UMCJ.

Additionally, although an officer who is not a judge is not acting under RCM 309(b)(3), an order from a non-judge officer would also be lawful. The test for the lawfulness of an order is found in the *MCM*'s explanation of Article 90, UCMJ:

> The order must relate to military duty, which includes all activities reasonably necessary to accomplish a military mission, or safeguard or promote the morale, discipline, and usefulness of members of a command and directly connected with the maintenance of good order in the

[142] MCM, *supra* note 108, pt. IV, ¶ 16(c)(2)(a)(iii).
[143] *Id.* R.C.M. 801(a)(3).

> Service. The order may not, without such a valid military purpose, interfere with private rights or personal affairs. However, the dictates of a person's conscience, religion, or personal philosophy cannot justify or excuse the disobedience of an otherwise lawful order.[144]

"Orders are clothed with an inference of lawfulness," and the burden is on the Service member disobeying the order to demonstrate that the order is unlawful.[145] Ordering a Service member to produce a device in an unencrypted state as part of a criminal investigation relates to an activity necessary to maintain good order and discipline. As the CAAF explained in *United States v. Ranney*, where the court upheld a conviction for violating an order to cease an unprofessional relationship, "with a sufficient nexus between the mandate and a stated military duty—good order and discipline—extant in the record, the presumption that the order was lawful remains intact."[146] The constitutional or statutory right against self-incrimination can, of course, render such an order unlawful despite its military purpose, but that is a matter to be resolved in litigation over the foregone conclusion doctrine.[147]

In the case of a military judge's order and a follow-up order by a superior officer in the accused's chain of command, the subsequent superior officer's order would not run afoul of the "ultimate offense doctrine" as set out in the *MCM*, *United States v. Landwehr*,[148] and *United States v. Phillips*.[149] The *MCM* provides that "[d]isobedience of an order which has for its sole object the attainment of some private end, or which is given for the sole purpose of increasing the penalty for an offense which it is expected the accused may commit, is not punishable under [Article 90, UCMJ]."[150]

---

[144] *Id.* pt. IV, ¶ 16(c)(a)(iv).
[145] United States v. New, 55 M.J. 95, 106 (C.A.A.F. 2001) (citing United States v. Hughey, 46 MJ 152, 154 (C.A.A.F. 1997)); United States v. Nieves, 44 M.J. 96, 98 (C.A.A.F. 1996).
[146] United States v. Ranney, 67 M.J. 297, 302 (C.A.A.F. 2009), *overruled on other grounds*, United States v. Phillips, 74 M.J. 20, 23 (C.A.A.F. 2015) (holding that the ultimate offense doctrine under Article 90, UCMJ, is limited to the language of the *MCM* rather than more expansive applications in prior case law including *Ranney*).
[147] United States v. Lee, 25 M.J. 457, 460 (C.M.A. 1988) ("[I]t is well established that if appellant was a suspect at the time of this inquiry, Article 31 precludes this regulation or orders purportedly based thereon from being used to compel him to incriminate himself."); United States v. Reed, 24 M.J. 80 (C.M.A. 1987); United States v. Lavine, 13 M.J. 150, 151 (C.M.A. 1982)).
[148] United States v. Landwehr, 18 M.J. 355, 356–57 (C.M.A. 1984).
[149] United States v. Phillips, 74 M.J. 20, 23 (2015).
[150] MCM, *supra* note 108, pt. IV, ¶ 16(c)(2)(iv).

*Phillips* made clear that the ultimate offense doctrine under Article 90, UCMJ, is limited to this language in the *MCM* rather than prior judicial formulations.[151]

In *Landwehr*, the Court of Military Appeals ruled that "an order given solely for the purpose of increasing the punishment for not performing a pre-existing duty should not be made the grounds of an Article 90 violation, but should instead be charged under Article 92 . . . ."[152] But *Landwehr* presupposes a situation in which the initial duty would be enforceable only under Article 92, UCMJ (i.e., it was not a specific order from a superior officer to the accused). In such a case, the subsequent order would increase the maximum punishment from a bad conduct discharge and six months' confinement[153] to a dishonorable discharge and five years' confinement.[154] Most military judges will be commissioned officers superior to the accused, so the purpose of enhancing punishment would not apply. Moreover, even if the accused outranked the judge, the accused could still face five years' confinement and a dishonorable discharge under Articles 131b or 131f(2), UCMJ.[155] Thus, the accused would likely face a charge with the same maximum punishment, and the Government would likely concede to merging the charges for sentencing, as courts view this concession as evidence that the Government is not seeking to unfairly punish the accused.[156] Therefore, although a subsequent superior officer's order is likely unnecessary to prosecute the accused, neither would it be an unlawful basis for prosecution.

In sum, a military judge's order to the accused to obey a subpoena would serve as the basis for prosecution under Articles 90 or 92(2), UCMJ. Nevertheless, in light of the lack of case law addressing violations of a judge's order, if the Government obtains such an order compelling compliance, the Government could also seek a commander's order to

---

[151] *Phillips*, 74 M.J. at 23.
[152] *Landwehr*, 18 M.J. at 356–57.
[153] MCM, *supra* note 108, pt. IV, ¶ 16(d)(2).
[154] *Id.* ¶ 18(d)(2).
[155] *Id.* ¶¶ 83(d), 87(d)(2).
[156] United States v. Hohenstein, No. ACM 37965 2014 CCA LEXIS 179, at *24–27 (A.F. Ct. Crim. App. Mar. 20, 2014) ("We find no evidence of prosecutorial overreaching or abuse, particularly in light of the fact that trial counsel conceded the Specifications should be merged for sentencing if the members convicted the appellant of both offenses. In sum, under *Campbell*, the military judge properly exercised his discretion by deferring his ruling on unreasonable multiplication of charges until the members returned their verdict, and then merging the specifications for sentencing rather than dismissing them.").

compel compliance as a basis for future prosecution without running afoul of the ultimate offense doctrine set forth in the *MCM*, *Phillips*, and *Landwehr*.[157]

*2. Obstructing Justice Under Article 131b, UCMJ*

Disobeying a judge's order to comply with a subpoena to provide a device in an unencrypted state could also constitute obstruction of justice under Article 131b, UCMJ. The text of Article 131b, UCMJ, which replaced the previous Article 134, UCMJ, offense, provides that:

> Any person subject to this chapter who engages in conduct in the case of a certain person against whom the accused had reason to believe there were or would be criminal or disciplinary proceedings pending, with intent to influence, impede, or otherwise obstruct the due administration of justice shall be punished as a court-martial may direct.[158]

Obstructing justice is comprised of three elements: (1) that the accused wrongfully do an act (2) in the case of the accused or another person whom the accused has reason to believe there would be criminal or disciplinary proceedings pending (3) with the intent to influence, impede, or otherwise obstruct the due administration of justice.[159] In the Article 30a, UCMJ, subpoena scenario, the accused would have the opportunity to move to quash and litigate the lawfulness of the subpoena, so the judge would settle whether disobedience is "wrongful." Having a device seized and having been served the pre-referral subpoena, the accused could have little doubt that there would be criminal proceedings pending. Finally, because the accused would know the purpose of the subpoena was to gather evidence, the intent to impede justice would be apparent from disobeying a judge's order compelling compliance.

Case law strongly suggests that disobedience of a military judge's order enforcing a subpoena would be factually sufficient for an obstruction conviction. The most analogous case is the Navy-Marine Corps Court of Criminal Appeals decision of *United States v. Watkins*.[160] In that case, the appellant was convicted of obstruction of justice for interfering with the

---

[157] *Id.*
[158] UCMJ art. 131b (2019).
[159] *Id.*
[160] United States v. Watkins, No. 201700246, 2019 CCA LEXIS 71, at *47–48 (N-M. Ct. Crim. App. Feb. 21, 2019).

Government's attempts to serve a subpoena on his spouse.[161] The evidence of the wrongfulness of the appellant's conduct included web searches such as "dodging being served a subpoena," web history researching the hotel where his spouse hid from Government agents, and violations of a military protective order prohibiting contact with his spouse.[162] The appellate court affirmed the factual and legal sufficiency of the appellant's obstruction conviction. The CAAF reversed, but not on the grounds that the conviction for obstruction of justice was factually or legally insufficient.[163] Rather, it found error in the trial judge's refusal to allow the appellant to dismiss his civilian defense counsel, thus denying the appellant the right of counsel of his choice.[164]

Given that the accused's interference with lawful process on a witness to obtain evidence can constitute obstruction, direct disobedience of a subpoena to the accused would also constitute obstruction. Indeed, the corrupt motive of obstruction can criminalize what might otherwise be a lawful act such as moving one's family member to a new residence (as in *Watkins*) or advising a person to invoke Article 31, UCMJ, rights.[165] In the case of disobedience of a judge's lawful order, the accused may not rely on such conduct being lawful sans the corrupt context. Thus, an accused's disobedience of a judge's order to comply with an Article 30a, UCMJ, subpoena could be punishable as obstruction of justice under Article 131b, UCMJ.

### *3. Prevention of Authorized Seizure of Property Under Article 131e, UCMJ*

Disobeying a judge's order to comply with a subpoena would not violate the proscription in Article 131e, UCMJ, on prevention of authorized seizure of property. Article 131e, UCMJ, provides:

---

[161] *Id.*
[162] *Id.*
[163] *Id.*
[164] *Id.*
[165] *Watkins*, 2019 CCA LEXIS 71 at *47; Cole v. United States, 329 F.2d 437, 443 (9th Cir. 1964) ("We hold the constitutional privilege against self-incrimination is an integral part of the due administration of justice. . . . A witness violates no duty to claim it, but one who . . . advises with corrupt motive . . . to take it, can and does himself obstruct or influence the due administration of justice.").

> Any person subject to this chapter who, knowing that one or more persons authorized to make searches and seizures are seizing, are about to seize, or are endeavoring to seize property, destroys, removes, or otherwise disposes of the property with intent to prevent the seizure thereof shall be punished as a court-martial may direct.[166]

Disobeying a judge's order would meet neither the first nor the third elements of the offense. The first element requires that agents "were seizing, about to seize, or endeavoring to seize certain property."[167] In most cases involving compelled decryption, agents will have already seized the property before the accused is served a subpoena. The third element requires intent to prevent the seizure;[168] as with the first element, the seizure will have already occurred when the accused is served a subpoena.

Disobeying a judge's order arguably also fails to satisfy the second element as well, which requires that the accused "destroys, removes, or otherwise disposes of the property."[169] The *Military Judges' Benchbook* instructions define "dispose of" as "an unauthorized transfer, relinquishment, getting rid of, or abandonment of the property."[170] The failure to decrypt a device does not prevent the seizure of the device. So, failure to decrypt does not fall neatly within this definition. The *Benchbook* instructions go on to state, "[p]roperty may be considered 'destroyed' if it has been sufficiently injured to be useless for the purpose for which it was intended, even if it has not been completely destroyed."[171] Wrongfully leaving a device locked certainly renders such property "useless for the purpose for which it was intended" because every such use requires it to be unlocked, but it is not clear that leaving a device locked constitutes "injuring" the device.

The case law addressing Article 131e, UCMJ, and the analogous pre-MJA 2016 offense under Article 134, UCMJ, does not address decryption. Rather, such cases involve various means of disposing of or concealing physical evidence.[172] Thus, absent case law extending the language of

---

[166] UCMJ art. 131e (2019).
[167] MCM, *supra* note 108, ¶ 86(b)(1).
[168] *Id.* ¶ 86(b)(3).
[169] *Id.*
[170] *Electronic Benchbook 2.14.9*, U.S. ARMY JUDGE ADVOC. GEN.'S CORPS para. 3a-55e-1, https://www.jagcnet.army.mil/EBB (Mar. 15, 2022).
[171] *Id.*
[172] *See, e.g.*, United States v. Rogers, No. 20190032, 2019 CCA LEXIS 399, *5 (A. Ct. Crim. App. Oct. 8, 2019).

Article 131e, UCMJ, to decryption, disobeying an order to decrypt a device would likely not be punishable as prevention of authorized seizure of property under Article 131e, UCMJ.

*4. Noncompliance with Procedural Rules by Failing to Comply with the Code Under Article 131f(2), UCMJ*

A Service member disobeying a judge's order to comply with an Article 30a, UCMJ, subpoena would violate Article 131f(2), UCMJ, which applies where a Service member "knowingly and intentionally fails to enforce or comply with any provision of this chapter regulating the proceedings before, during, or after trial of an accused."[173] Military courts have consistently described Article 131f(2), UCMJ, as applying prior to referral. As the Navy Court explained in *United States v. Dossey*, the word "proceedings" in the old Article 98, UCMJ, is "broader than a particular court-martial" and "Article 98 explicitly refers to proceedings before and after trial, rather than simply referring to the 'proceedings of a court-martial.'"[174] Along the same lines, the CAAF observed in *United States v. McCoy* that a trial counsel wrongfully advising CID agents to withhold Article 31, UCMJ, rights advisement during an investigation would violate Article 98, UCMJ, by failing to comply with Article 31, UCMJ.[175] Likewise, in *United States v. Allen*,[176] the Court noted that the legislative history of Article 32, UCMJ, describes the failure to order an Article 32, UCMJ, investigation, which is by nature a pre-referral act, as a violation of the old Article 98, UCMJ. These three cases thus clarify that Article 131f(2), UCMJ, applies to pre-referral conduct.

Failing to obey a judge's order to comply with a subpoena constitutes failure to "comply with any provision of [the UCMJ] regulating the proceedings before, during, or after trial of an accused,"[177] thus satisfying the first element of Article 131f(2), UCMJ. In *United States v. McElhinney*,

---

[173] UCMJ art. 131f(2) (2016).
[174] United States v. Dossey, 66 M.J. 619, 624 (N-M. Ct. Crim. App. 2008). Under MJA 2016, the old Article 98, UCMJ, was renumbered as the current Article 131f, UCMJ, so the case law references the former. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5401, 130 Stat. 2000, 2938 (2016).
[175] United States v. McCoy, 31 M.J. 323, 324 (C.A.A.F. 1999).
[176] United States v. Allen, 5 U.S.C.M.A. 626, 633 (C.M.A. 1955).
[177] UCMJ art. 131f(2).

a military judge ordered the Government to produce witnesses.[178] The Court of Military Appeals wrote, citing the old Article 98, UCMJ, "[s]ince the judge's original decision was then nonappealable, the convening authority was bound in law to honor it . . . or, if he did not desire to do so, he had the option to dismiss the charges."[179] While this language is dicta, it is the most authoritative guidance available, and there is no authority contradicting *McElhinney*. There has not been a case involving an actual prosecution under Article 98, UCMJ, for failure to obey a judge's order. In fact, there has not even been a case where the accused was convicted of violating the prohibition in either Article 131f(1), UCMJ, on causing unnecessary delay in disposing of a case or Article 131f(2), UCMJ, on failing to enforce or comply with any provision of the UCMJ, leading one judge to describe the old Article 98, UCMJ, as an "illusory remedy."[180]

The first element would be the only controversial element in a prosecution under Article 131f(2), UCMJ, for disobedience of a judge's order to obey an Article 30a, UCMJ, subpoena. The second element (i.e., that the accused had a duty to comply) would be evident from the judge's order under RCM 309. The third and fourth elements (i.e., knowledge of the duty and intentionally failing to comply) would be clear from the judge's issuing the order to the accused and the accused's failure to comply.[181]

Like Articles 131b and 90, UCMJ, the maximum punishment under Article 131f(2), UCMJ, is a dishonorable discharge, total forfeiture, and confinement for five years.[182] Thus, in most cases, in light of the likelihood of multiple charges being merged for sentencing, the choice to proceed under Article 131f(2), UCMJ, alone or in conjunction with other charges would not affect the maximum punishment in sentencing.

---

[178] United States v. McElhinney, 21 U.S.C.M.A. 436, 439 (C.M.A. 1972).
[179] *Id.*
[180] United States v. Ward, 48 C.M.R. 588, 589 (C.M.R. 1974) (Lynch, J., concurring) ("Article 98, however, provides only an illusory remedy in view of the 23 years that the Code has been in operation and the absence of a single reported case involving a charge laid under Article 98 being prosecuted. In this case, in particular, Article 98 provides only a questionable remedy in view of the fact that the accused would have been one of the most senior Flag Officers in command in the Coast Guard, and the substance of the charge would be simply post-trial delay of the Supervisory Authority's action after conviction.").
[181] MCM, *supra* note 108, ¶ 87(b)(2)(c)–(d).
[182] *Id.* ¶ 87(d)(2).

*5. Conduct Unbecoming an Officer Under Article 133, UCMJ*

If the accused is an officer, refusing to obey a judge's order to obey a subpoena could constitute conduct unbecoming under Article 133, UCMJ. Conduct unbecoming is "behavior in an official capacity which, in dishonoring or disgracing the person as an officer, seriously compromises the officer's character as a gentleman, or action or behavior in an unofficial or private capacity which, in dishonoring or disgracing the officer personally, seriously compromises the person's standing as an officer."[183] "[A]cts of dishonesty, unfair dealing, indecency, indecorum, lawlessness, injustice, or cruelty" may qualify.[184] "[C]onduct need not be a violation of any other punitive article of the Code, or indeed a criminal offense at all, to constitute conduct unbecoming an officer."[185] There is authority for conduct designed to hide harmful facts constituting conduct unbecoming. In *United States v. Daniels*, the AFCCA upheld a conviction for conduct unbecoming where the accused asked another person to misrepresent the basis for a leave request to hide the fact that the accused was in jail.[186]

Unlike Article 134, UCMJ, a more specific offense does not preempt Article 133, UCMJ. Rather, "[a]n accused can be charged with either an Article 133, UCMJ, offense or the enumerated punitive article based on the same underlying conduct, provided the conduct is, in fact, unbecoming an officer and a gentleman."[187]

The maximum punishment under Article 133, UCMJ, is dismissal, forfeiture of all pay and allowances, and "and confinement for a period not in excess of that authorized for the most analogous offense for which a

---

[183] *Id.* ¶ 90(c)(2). Section 542 of the National Defense Authorization Act for Fiscal Year 2022 removes the "and a gentleman" language from Article 133, UCMJ, but there is no indication that this amendment changes the applicability of the article. National Defense Authorization Act for the Fiscal Year 2022, Pub. L. No. 117-81, § 542, 135 Stat. 1541, 1709 (2021).

[184] *Id.*

[185] United States v. Forney, 67 M.J. 271, 275 (C.A.A.F. 2009).

[186] *United States v. Daniels* had a robust appellate history involving *United Sates v. Briggs* and the statute of limitations, but this history did not question the Air Force Court of Criminal Appeals' holding regarding the factual sufficiency of the conduct unbecoming conviction. *United States v. Daniels*, No. ACM 39407, 2019 WL 2560041, at *5 (A.F. Ct. Crim. App. June 18, 2019), *aff'd*, 79 M.J. 199 (C.A.A.F. 2019), *cert. granted sub nom.* United States v. Collins, 140 S. Ct. 519 (2019), and *rev'd and remanded sub nom.* United States v. Briggs, 141 S. Ct. 467 (2020), and *vacated*, No. 19-0345/AF, 2021 WL 495963 (C.A.A.F. Jan. 25, 2021), and *review denied*, 79 M.J. 252 (C.A.A.F. 2019), and *rev'd and remanded*, No. 19-0345/AF, 2021 WL 495963 (C.A.A.F. Jan. 25, 2021).

[187] United States v. Conliffe, 67 M.J. 127, 133 n.2 (C.A.A.F. 2009).

punishment is prescribed in this Manual, or, if none is prescribed, for 1 year."[188] Each of the most analogous offenses—Articles 131b and 131f(2), UCMJ—have the same maximum confinement of five years.[189]

*6. Contempt of Court Under Article 134, UCMJ*

In the case of disobedience of a judge's order to comply with a subpoena, the conduct would meet the elements for prosecution under Article 134, UCMJ, but it would be preempted by Articles 90, 131b, and 131f(2), UCMJ. The *MCM*'s discussion of RCM 809 states that "a person subject to the UCMJ who commits contempt may be tried by court-martial or otherwise disciplined under Article 134 for such misconduct in addition to or instead of punishment for contempt."[190] The "punishment for contempt" is the military judge's contempt authority in Article 48, UCMJ. The discussion does not specify any particular type of contemptuous behavior, and this reference appears in the discussion as opposed to the text of the *MCM* enacted by the President. Thus, the preemption rule provided by the President supersedes the discussion where the conduct at issue is covered by a more specific punitive article.

Contempt of court is not an enumerated offense under Article 134, UCMJ. Thus, contempt would be prosecuted as a general offense for conduct prejudicial to good order and discipline and/or conduct of a nature to bring discredit upon the service. While no case specifically addresses disobedience of a subpoena under Article 134, UCMJ, case law concerning obstruction of justice when that offense fell under Article 134, UCMJ, indicates that failure to obey a subpoena would be conduct prejudicial to good order and discipline.[191] In *United States v. Watkins*, the Article 134, UCMJ, obstruction case discussed in Section VI.B.2 above, the accused's efforts to frustrate service of a subpoena on his spouse were "prejudicial to good order and discipline in the armed forces and was of a nature to bring

---

[188] MCM, *supra* note 108, ¶ 90(d).
[189] *Id.* ¶¶ 83(d), 87(d)(2).
[190] *Id.* R.C.M. 809 discussion.
[191] Prior to MJA 2016, obstructing justice was a specified offense under Article 134, UCMJ. 2016 MCM, *supra* note 119, pt. IV, ¶ 96. The Military Justice Act of 2016 added obstructing justice as Article 131b, UCMJ, and removed that offense from the purview of Article 134, UCMJ. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5445, 130 Stat. 2000, 2956 (2016).

discredit upon the armed forces."[192] Military courts have also held that disobeying court orders satisfied the Article 134, UCMJ, terminal element. In *United States v. Dominguez*, failure to appear in civilian court as ordered in a ticket summons was service discrediting because the appellant "flouted judicial authority by failing to appear" and his contempt toward a court proceeding was "injurious to the military's reputation."[193]

The common threads of disobedience and obstruction in any prosecution raise the issue of preemption in light of the specified prohibitions in Articles 90, 131b, and 131f(2), UCMJ. "The preemption doctrine prohibits application of Article 134 to conduct covered by Articles 80 through 132."[194] In the case of disobedience of a judge's order to compel decryption, a prosecution for contempt of court under Article 134, UCMJ, would likely be preempted by Articles 90, 92(2), 131b, and 131f(2), UCMJ. These articles would not bar all contempt of court prosecutions under Article 134, UCMJ. Disruptive behavior in a court, for example, might be conduct not covered by another article and thus fall under Article 134, UCMJ. But, in the specific case of disobeying a judge's order to comply with a subpoena, several other articles would apply to the conduct. Contempt of court arguably protects a different interest (i.e., the court's authority) than do other articles, but the preemption doctrine applies to "conduct," not interest.[195]

In the event that prosecution under Article 134, UCMJ, was not preempted, because contempt of court is an unspecified offense under Article 134, UCMJ, the maximum punishment is determined under RCM 1003(c)(1)(B). Where the Article 134, UCMJ, offense is included in or "closely related" to another offense in the UCMJ, the maximum punishment is that of the included or related offense. If there is no included or closely related offense, the offense is punishable as authorized in the U.S. Code or by the custom of the service. The most closely related offenses to disobeying a judge's order enforcing a subpoena are "noncompliance with procedural rules by failing to comply with the Code" under Article 131f(2), UCMJ, and obstructing justice under Article 131b, UCMJ. Article 90, UCMJ, may be

---

[192] *See, e.g.*, United States v. Jones, 20 M.J. 38, 40 (C.M.A. 1985) ("It is clear that the willful destruction of contraband seized by commissioned officers of the armed forces prejudices good order and discipline. It does not matter how the evidence is ultimately used. Willful destruction of potential evidence harms the orderly administration of justice. The accused was properly charged, tried, and convicted.").

[193] United States v. Dominguez, No. ACM S28658, 1993 CMR LEXIS 587, at *3–4 (A.F.C.M.R. Dec. 13, 1993).

[194] MCM, *supra* note 108, ¶ 91(c)(5)(a).

[195] *Id.*

less specifically analogous, but the maximum punishment is the same, so the relative strength of the analogy is immaterial. The only case in which finding another provision more analogous would matter is the rare case where the military judge is not a superior officer to the accused so Article 92(2), UCMJ, could apply in lieu of Article 90, UCMJ. While applicable, Article 92(2), UCMJ, is not specific to the court-martial context like Articles 131f(2) and 131b, UCMJ, and is thus not the most closely related offense.

### C. Warrants of Attachment—Lawful, But Unnecessary, for Service Members

A military judge need not issue a warrant of attachment to the accused to enforce an Article 30a, UCMJ, subpoena. Rule for Court-Martial 309 provides military judges with the authority to "order the person or service provider to comply with the subpoena or order."[196] Having received such an order from a military judge, Articles 90, 131b, and 131f(2), UCMJ, would apply to a Service member with no need for an additional warrant.

Warrants of attachment are generally issued to obtain evidence or testimony from civilians.[197] Rule for Court-Martial 703(g)(3)(H)(i) states, "If the person subpoenaed neglects or refuses to appear or produce evidence, the military judge . . . may issue a warrant of attachment to compel the attendance of a witness or the production of evidence, as appropriate."[198] As the discussion of RCM 703(g)(3)(H)(i) explains, "a warrant of attachment is a legal order addressed to an official directing that official to have the person named in the order brought before a court" and "has as its purpose the obtaining of the witness' presence, testimony, or documents."[199] The rule thus does not exclude Service members—it is simply unnecessary. Service members may be compelled to attend courts-martial by order of their commander without the need to resort to warrants.[200] And, as the discussion further explains, when a civilian disobeys a subpoena, it is the

---

[196] *Id.* R.C.M. 309.

[197] *See, e.g.*, United States v. Williams, 23 M.J. 724, 726 (A.F.C.M.R. 1986) (providing that a civilian's refusal to appear gave the military judge authority to direct a warrant of attachment be issued); United States v. Harding, 63 M.J. 65, 66 (C.A.A.F. 2006) (noting that a warrant of attachment was issued to obtain evidence from a civilian but the U.S. Marshals did not enforce the warrant).

[198] MCM, *supra* note 108, R.C.M. 703(g)(3)(H)(i).

[199] *Id.* discussion.

[200] *Id.* R.C.M. 703(g)(1).

disobedience of the subpoena, not the warrant of attachment, that serves as a basis for prosecution.[201] So, too, with Service members, the disobedience triggers criminal liability under Articles 90, 131b, and 131f(2), UCMJ, not the warrant of attachment.

Warrants of attachment nevertheless might have some practical utility in securing compliance. There is nothing wrong with issuing a warrant of attachment for an active-duty Service member, but it is unnecessary. Thus, a military judge could issue a warrant of attachment to provide a second chance for compliance with the implicit threat of a document entitled "warrant." But nothing in the UCMJ or the RCMs requires the military judge to provide the accused with this second chance to comply.

## VII. The Foregone Conclusion Doctrine, the Fifth Amendment, and Article 31, UCMJ

### A. The Act of Production Doctrine and Foregone Conclusion Doctrine Generally

Under the act of production doctrine, an act qualifies for Fifth Amendment protection if the act is "testimonial, incriminating, and compelled."[202] A compelled act of production by the accused is "testimonial" if it would "'disclose the contents of his own mind' and therefore communicate a 'factual assertion' or 'convey[] information to the Government.'"[203]

The foregone conclusion doctrine, however, can render an act of production non-testimonial and thus not protected by the Fifth Amendment. As Professor Orin Kerr has explained: "The foregone conclusion doctrine teaches that when the testimonial aspect of a compelled act 'adds little or nothing to the sum total of the Government's information,' any implied testimony is a 'foregone conclusion' and compelling it does not violate the Fifth Amendment."[204]

The foregone conclusion doctrine has its roots in *United States v. Fisher*.[205] In *Fisher*, two taxpayers under investigation by the Internal

---

[201] *Id.* R.C.M. 703(g)(3)(H) discussion.
[202] Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 189 (2004).
[203] Kerr, *supra* note 2 (quoting Doe v. United States, 487 U.S. 201, 208, 210–11, 215 (1988)).
[204] *Id.* at 773 (quoting United States v. Fisher, 425 U.S. 391, 411 (1976)).
[205] *Fisher*, 425 U.S. 391 (1976).

Revenue Service (IRS) obtained from their accountants documents that they transferred to their lawyers.[206] Upon learning that the lawyers had the documents, the IRS served summonses on them that directed production of the documents.[207] The IRS also served summonses on the accountants to appear and testify regarding the documents.[208] The Supreme Court found that this compelled production did not violate the Fifth Amendment.[209] The act of production doctrine applied because production communicated that the documents (1) existed, (2) were in the target's possession, and (3) were authentic.[210] The foregone conclusion doctrine, however, rendered this act of production non-testimonial because the production "adds little or nothing to the sum total of the Government's information."[211] Such documents were the type "usually prepared by an accountant working on the tax returns of his client," so the existence of the documents and their location in the target's possession was a "foregone conclusion," and the authenticity of the documents could be independently confirmed by the accountants who created them.[212] Therefore, the Government did not rely on "truthtelling" by the taxpayers to prove the existence of the documents, the taxpayers' access to the documents, or the documents' authenticity. As a result, compelling production did not violate the taxpayers' constitutional rights because the production was not "testimony" but mere "surrender."[213]

The Supreme Court went on to address the foregone conclusion doctrine in three more cases lower courts frequently cite in applying the doctrine: *United States v. Doe* (*Doe I*),[214] *Doe v. United States* (*Doe II*),[215] and *United States v. Hubbell*.[216]

*Doe I* provides an example in which the Government was unable to prove that the testimonial aspects of a compelled act were a foregone conclusion. In *Doe I*, a grand jury investigating corruption in awarding Government contracts issued subpoenas directing Doe to turn over

---

[206] *Id.* at 394.
[207] *Id.* at 395.
[208] *Id.* at 394–95.
[209] *Id.* at 402.
[210] Kerr, *supra* note 2, at 773 (citing *Fisher*, 425 U.S. at 411–13).
[211] *Fisher*, 425 U.S. at 411.
[212] *Id.*
[213] *Id.*
[214] *United States v. Doe*, 465 U.S. 605 (1984) (*Doe I*).
[215] *Doe v. United States*, 487 U.S. 201 (1988) (*Doe II*).
[216] United States v. Hubbell, 530 U.S. 27 (2000).

telephone and business records from several sole proprietorships.[217] The Supreme Court found that the act of production compelled by the subpoenas was protected by the Fifth Amendment.[218] Like in *Fisher*, the act of production would communicate that the records existed, were in Doe's possession, and were authentic.[219] Unlike in *Fisher*, though, the district court and Third Circuit had determined that the Government did not know whether the documents sought were in Doe's possession or control, and the Supreme Court did not disturb these findings of fact.[220] Thus, the existence, possession, and authenticity of the documents in *Doe I* was not a foregone conclusion, so the Fifth Amendment privilege against self-incrimination applied.[221]

By contrast, in *Doe II*, compelling Doe to execute a consent directive allowing the release of records for bank accounts over which he might have control was not testimonial. In *Doe II*, a grand jury was investigating fraudulent manipulation of oil cargoes and tax evasion.[222] In response to a grand jury subpoena for records of transactions with banks in the Cayman Islands and Bermuda, Doe appeared, produced some records, and testified that no additional records were in his possession or control.[223] Doe claimed the Fifth Amendment privilege as to the existence and location of any other records. The grand jury then issued subpoenas to the foreign banks for records of accounts over which Doe had authority. The banks refused to comply, invoking bank secrecy laws in their home countries.[224] The district court then ordered Doe to execute a consent directive releasing records of accounts where Doe had a right of withdrawal. The directive did not name any specific account or even acknowledge the existence of any accounts—it simply applied to any accounts over which Doe had authority generally.[225] After Doe refused to sign the directive, the district court found Doe in contempt, and the Fifth Circuit affirmed. The Supreme Court affirmed, finding the consent directive not testimonial. As the Court explained, because the directive only generally provided consent for release of records in the event that any such records existed, the directive

---

[217] *Doe I*, 465 U.S. at 613–16.
[218] *Id.* at 616.
[219] *Id.* at 613 (citing *Fisher*, 425 U.S. at 410).
[220] *Id.* at 613–14.
[221] *Id.* at 616.
[222] *Doe II*, 487 U.S. 201.
[223] *Id.* at 202–03.
[224] *Id.* at 203.
[225] *Id.* at 206.

did not admit the existence of any accounts or that Doe controlled them.[226] Nor did the directive itself "admit the authenticity of any records produced by the bank."[227] Rather, if the Government received records in response, "the only factual statement made by anyone will be the bank's implicit declaration, by its act of production in response to the subpoena, that it believes the accounts to be petitioner's."[228] Therefore, the Court found that "As in *Fisher*, the Government is not relying upon the 'truthtelling' of Doe's directive to show the existence of, or his control over, foreign bank account records."[229]

*United States v. Hubbell*,[230] on the other hand, provides another example of the *Fisher* framework's application in a case in which the Government failed to prove that communicative aspects of the act of production were a foregone conclusion. Hubbell pleaded guilty to mail fraud and tax evasion.[231] As part of his plea bargain, he promised to provide the independent counsel in the Whitewater investigation "full, complete, accurate, and truthful information."[232] Investigating whether Hubbell had broken that promise, the independent counsel served Hummel a subpoena to produce eleven categories of documents before a grand jury.[233] Hubbell appeared before the grand jury and invoked his privilege against self-incrimination, refusing "to state whether there are documents within [his] possession, custody, or control responsive to the Subpoena."[234] The prosecutor served Hubbell an order "directing him to respond to the subpoena and granting him immunity 'to the extent allowed by law.'"[235] Hubbell produced 13,120 pages of documents, which led to a second prosecution for mail fraud, wire fraud, and tax offenses.[236] As in *Fisher*, the act of production doctrine applied because the production communicated that the documents "existed, were in his possession or control, and were authentic."[237] Unlike in *Fisher*, however, in *Hubbell* "the Government

---

[226] *Id.* at 215.
[227] *Id.*
[228] *Id.* at 218.
[229] *Id.* at 215.
[230] United States v. Hubbell, 530 U.S. 27 (2000).
[231] *Id.* at 30.
[232] *Id.*
[233] *Id.* at 31.
[234] *Id.*
[235] *Id.*
[236] *Id.*
[237] *Id.* at 36.

ha[d] not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent."[238] Thus, in *Hubbell*, the foregone conclusion doctrine did not apply, so the Fifth Amendment privilege applied to Hubbell's production. The immunity granted to Hubbell was coextensive with his Fifth Amendment privilege, so *United States v. Kastigar* required dismissal of the second prosecution unless the Government could show the indictment was obtained from wholly independent sources, which the Government could not do.[239]

### B. The Foregone Conclusion Doctrine and Compelled Decryption in Civilian Courts

The various Federal circuit,[240] Federal district,[241] and state court[242] opinions addressing compelled decryption agree that the foregone conclusion doctrine can apply. The Federal Circuits that have considered the issue have set out two differing tests for applying the foregone conclusion doctrine. These tests differ in terms of what conclusions must be foregone. The Third Circuit has suggested that the Government need only show the accused's ability to decrypt the device is a foregone conclusion.[243] The Eleventh Circuit, by contrast, also requires the Government to show with "reasonable particularity" what evidence will be found on the device.[244]

---

[238] *Id.* at 45.
[239] *Id.* (citing United States v. Kastigar, 406 U.S. 441 (1972)).
[240] *Compare* United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017), *with* United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335 (11th Cir. 2012).
[241] *See, e.g.*, United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 U.S. Dist. LEXIS 70649 (N.D. Cal. Apr. 26, 2018); United States v. Jimenez, No. 19-10278-RWZ, 2020 U.S. Dist. LEXIS 5198, at *2 (D. Mass. Jan. 13, 2020).
[242] *See, e.g.*, Commonwealth v. Gelfgatt, 11 N.E.3d 605 (Mass. 2014); State v. Johnson, 576 S.W.3d 205 (Mo. Ct. App. 2019); State v. Pittman, 452 P.3d 1011 (Or. 2019).
[243] *Apple MacPro Comput.*, 851 F.3d at 248 n.7.
[244] *Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335.

*1. The Third Circuit*

The Third Circuit has suggested that the only conclusion that need be foregone is the accused's ability to decrypt the device.[245] Put another way, if the Government already has information sufficient to show that the accused can unlock a device, the accused may be ordered to do so. As the Third Circuit wrote in *United States v. Apple MacPro Computer*:

> [A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the Government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password for these devices."[246]

In *Apple MacPro Computer*, agents lawfully seized several encrypted devices that required passcodes to unlock.[247] Agents seized these devices pursuant to a valid search warrant executed at the appellant's home. The appellant refused unlock a computer, hard drives, and an application on a mobile phone. Forensic examination of the computer found one child pornography image, logs showing the computer had been used to visit sites with child exploitation titles, and evidence that the appellant had downloaded to the hard drives files known to be child pornography.[248] A witness had also seen the appellant unlock the computer and view child pornography on the computer.[249] The district court ordered the appellant to unlock the devices and held him in contempt when he claimed not to be able to remember the passwords.[250]

The Third Circuit, on plain-error review, affirmed.[251] As the Court explained, under the foregone conclusion doctrine, "the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a 'foregone conclusion' that 'adds little or nothing to the sum total of the Government's information.'"[252] The Third

---

[245] *Apple MacPro Comput.*, 851 F.3d at 248.
[246] *Id.* n.7.
[247] *Id.* at 242.
[248] *Id.* at 242–43.
[249] *Id.* at 248–49.
[250] *Id.* at 249.
[251] *Id.*
[252] *Id.* at 247.

Circuit affirmed the district court's finding that the decryption was non-testimonial because the Government had already established that "(1) the Government had custody of the devices; (2) prior to the seizure, [the appellant] possessed, accessed, and owned all devices; and (3) there are images on the electronic devices that constitute child pornography."[253] The Third Circuit went on to strongly suggest that the third point was unnecessary because the foregone conclusion doctrine would only apply to the control of the device implicit in the act of production—not the evidence that would later be obtained from the device.[254] But the Third Circuit did not have the occasion to so hold because the Government had presented evidence there was child pornography on the devices.[255]

*2. The Eleventh Circuit*

The Eleventh Circuit, on the other hand, has applied a more stringent test. *In re Grand Jury Subpoena Duces Tecum*[256] saw the Eleventh Circuit hold that a suspect can only be compelled to unlock his device via passcode if the Government can show with "reasonable particularity" what evidence will be found on the device.[257] In that case, a grand jury investigating child pornography charges issued a subpoena to the accused to decrypt electronic devices.[258] The Government, however, was unable to provide evidence showing that the drives contained child pornography or that the accused had access to the encrypted portions of the drives. The Government's expert in that case conceded that it was possible that the encrypted drives contained nothing.[259] The Eleventh Circuit, therefore, found that

> [n]othing in the record before [it] reveals that the Government knows whether any files exist and are located on the hard drives; what's more, nothing in the record illustrates that the Government knows with reasonable particularity that Doe is even capable of accessing the encrypted portions of the drives.[260]

---

[253] *Id.* at 248.
[254] *Id.* n.7.
[255] *Id.*
[256] *Doe (In re Grand Jury Subpoena Duces Tecum*), 670 F.3d 1335.
[257] *Id.* at 1346.
[258] *Id.* at 1337.
[259] *Id.* at 1346.
[260] *Id.*

*3. Subpoena Practice Under the Circuit Split*

The Third Circuit approach is better reasoned than the Eleventh Circuit approach. The Third Circuit in *Apple MacPro Computer* questioned the Eleventh Circuit's requirement that the Government articulate with reasonable particularity what would be found on the device. As the Third Circuit explained, the foregone conclusion doctrine focuses on only that which is implicit in the "act of production."[261] In decryption cases, the only testimony implicit in decryption is that the accused can decrypt the device. Put another way, the accused is only being compelled to unlock the device, and the only fact the act of unlocking communicates is the accused's ability to unlock, so the only "foregone conclusion" the Government should have to establish is the ability to unlock.

In analyzing the Third Circuit and the Eleventh Circuit approaches, Professor Kerr concluded that the Third Circuit approach is correct. As he explained:

> The Eleventh Circuit appears to have held that the Government can compel decryption only when it can first describe with reasonable particularity what decrypted files will be found on the device. This holding is incorrect. It erroneously equates the act of decrypting a device with the act of collecting and handing over the files it contains. The two acts may seem similar at first, but they have very different Fifth Amendment implications.[262]

Professor Kerr goes on to explain the differing Fifth Amendment implications of ordering decryption of a device on the one hand and ordering collection and production of files on the other as follows:

> If evidence is in a locked box, investigators might order a suspect to unlock the box and do no more. Investigators can then take over the search, investigating the contents of the box themselves and looking for the evidence. On the other hand, investigators might order a suspect to unlock the box and then execute the search himself on the Government's behalf. The suspect might be ordered to unlock the box, search it, find a particular set of documents described, and then bring those responsive documents to the Government.

---

[261] United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017).
[262] Kerr, *supra* note 2, at 770 (citations omitted).

> The first target role is unlocking; the second target role is unlocking and searching.
>
> . . . .
>
> When a suspect is ordered to produce a decrypted version of an electronic device, the compelled act ordinarily will be only to unlock the device. Any additional searching is the Government's job, and the Government need not know what it will find when it begins to look. Whether the Government knows enough about the incriminating evidence it hopes to find to describe it with reasonable particularity is simply irrelevant if the Government, not the target, is going to look for it. If the target doesn't have to search for the evidence the Government is seeking, the target doesn't need a specific description to establish a foregone conclusion.[263]

Thus, when drafting subpoenas, the Government should be careful to avoid an "implicit search requirement."[264] Such a requirement could be an order to take steps beyond simply producing an unlocked device, such as producing decrypted versions of certain files on the device. That implicit search request would move the production from *Fisher* to *Hubell* by relying on the accused's knowledge of particular files on the device.[265]

Although the Third Circuit approach is better reasoned, the circuit split remains. Prosecutors must thus choose between the Third Circuit and Eleventh Circuit approaches when drafting Article 30a, UCMJ, subpoenas. The more aggressive approach would be for the subpoena to simply compel surrender of the device in an unlocked state, like the subpoena in *Apple MacPro Computer*. Under this approach, the Government would simply use the subpoena to obtain the unlocked state and then conduct the search to the extent allowed by the search authorization. The more conservative approach would be for the subpoena to compel unlocking to allow inspection of only limited items that Government agents can describe with "reasonable particularity" based on *In re Grand Jury Subpoena Duces Tecum*. If the Government can show with "reasonable particularity" what will be found on the device, the Government may follow this approach if it wishes to avoid the Third Circuit versus Eleventh Circuit argument in motions practice.

---

[263] *Id.* at 787.
[264] *Id.* at 784.
[265] *Id.*

Under either the *Apple MacPro Computer* approach or the *In re Grand Jury Subpoena Duces Tecum* approach, the search following decryption must comply with the search authorization. Thus, regardless of whether the subpoena specifies the items to be inspected, the search of the device must be limited to the terms of the search authorization, which is itself limited by probable cause.

*4. The Originalist Approach*

Professor Kerr recently explored a different approach to compelled decryption based on an originalist understanding of the Fifth Amendment from the 1807 treason trial of Aaron Burr.[266] The evidence at issue in *United States v. Burr* was a letter encoded with a cypher.[267] Under an originalist understanding from *Burr*, the applicability of the Fifth Amendment to compelled disclosure of a password would depend on the evidence the Government seeks. Professor Kerr argues that *Burr* would not prevent compelled disclosure of a password if the Government were merely searching for evidence of a crime as opposed to material on the device that was itself contraband.[268] On the other hand, *Burr* would prevent compelled disclosure of a password where the Government sought evidence that itself was contraband, such as child pornography.[269] The distinction arises because disclosing a passcode in a contraband case would directly establish elements of the offense (i.e., knowledge or control of the contraband).[270] Disclosing a passcode in an evidence case, by contrast, would merely provide a link in the chain of evidence, which the Fifth Amendment would not protect under *Burr*.[271]

Regarding compelled entry of a password, Professor Kerr argues that the Fifth Amendment's application would depend on the choice of historic analogy.[272] If compelled entry was analogized to merely compelling a person to admit knowledge of the password, there would be no Fifth Amendment distinction between compelling disclosure of a password and

---

[266] Orin S. Kerr, *Decryption Originalism: The Lessons of* Burr, 134 HARV. L. REV. 905 (2021).
[267] *Id.* at 918–19.
[268] *Id.* at 913, 952–57.
[269] *Id.* at 913, 957–60.
[270] *Id.* at 958.
[271] *Id.* at 954.
[272] *Id.* at 960–61.

compelling entry of a password under *Burr*.[273] Thus, the same distinction between evidence cases and contraband cases would apply. If, on the other hand, compelled entry was analogized to a forcing the accused to produce the deciphered letter, the Fifth Amendment would bar compelled entry of a password entirely.[274]

Professor Kerr's analysis of *Burr* is comprehensive and could support an Article 30a, UCMJ, subpoena where the Government was seeking evidence of an offense as opposed to contraband in and of itself. Likewise, in the case of an Article 30a, UCMJ, subpoena seeking contraband, defense counsel might rely on Professor Kerr's analysis of *Burr*. Absent more recent military or civilian case law applying *Burr*, the Government would be well-advised to model Article 30a, UCMJ, subpoena practice on *Apple MacPro Computer* or *In re Grand Jury Subpoena* at the outset and argue *Burr* in the subsequent briefing.

Additionally, *Burr* may not apply to the accused's statutory Article 31, UCMJ, rights in the military justice system. *Burr* dealt only with claims of constitutional privilege. Article 31, UCMJ, is a later-enacted statute providing Service members with rights in addition to the Fifth Amendment (e.g., the guarantee in Article 31, UCMJ, of rights advisement even in non-custodial settings).[275] Thus, military case law since the 1956 enactment of Article 31, UCMJ, may supersede *Burr* with respect to Service members' statutory Article 31, UCMJ, rights. Indeed, Article 31, UCMJ, was enacted against the backdrop of Congress's understanding of the Fifth Amendment at that time. Additionally, Congress has not amended Article 31, UCMJ, since its 1956 enactment, despite decades of military case law and significant amendments to other provisions the UCMJ. Thus, revising Article 31, UCMJ, case law based on *Burr* may not be consistent with the intent of Congress when enacting Article 31, UCMJ, and confirmed by decades of declining to amend Article 31, UCMJ. Accordingly, even if civilian Federal courts revisited Fifth Amendment case law based on *Burr*, military courts might not correspondingly revisit Article 31, UCMJ, case law.

---

[273] *Id.* at 961.
[274] *Id.* at 913, 961.
[275] UCMJ art. 31 (1950).

C. The Foregone Conclusion Doctrine in Military Courts

Military appellate courts have not yet ruled on the specific question of the foregone conclusion doctrine and decryption in courts-martial. To date, three opinions have referenced the foregone conclusion doctrine in relation to decryption: the dissent (but not the majority) in *United State v. Mitchell*,[276] the AFCCA opinion (but not the CAAF opinion) in *United States v. Robinson*,[277] and the Army Court of Criminal Appeals' unpublished opinion in *United States v. Suarez*.[278] Nevertheless, applying the existing military case law reveals that the Article 30a, UCMJ, subpoena and the foregone conclusion doctrine remains a viable means of compelling decryption in courts-martial.

*1.* United States v. Mitchell

Although the parties and amici curiae in *United States v. Mitchell* submitted arguments regarding passcode entry as a compelled and testimonial act, the CAAF expressly declined to rule on this issue.[279] Instead, it applied MRE 305(c)(2) and *Edwards v. Arizona*[280] to hold that it was not permissible for investigators to first ask the accused for his passcode and then ask him to unlock his phone after his invocation of the right to counsel.[281] As the Court explained: "In light of this holding, we need not reach the question of whether the Government directly violated Appellee's Fifth Amendment privilege against compelled self-incrimination. We thus do not address whether Appellee's delivery of his passcode was 'testimonial' or 'compelled,' as each represents a distinct inquiry."[282] The CAAF's opinion in *United States v. Robinson*, which it decided shortly after *Mitchell*, added the caveat that it was permissible to ask for consent to search after a request for counsel and then ask for the passcode if the accused had first consented to a search.[283]

---

[276] United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017).
[277] United States v. Robinson, 76 M.J. 663, 669 (A.F. Ct. Crim. App. 2017), *aff'd*, 77 M.J. 303 (C.A.A.F. 2018).
[278] United States v. Suarez, No. 20170366, 2017 WL 4331014, at *2 (A. Ct. Crim. App. Sept. 27, 2017).
[279] *Mitchell*, 76 M.J. at 419.
[280] Edwards v. Arizona, 451 U.S. 477 (1981).
[281] *Mitchell*, 76 M.J. at 419.
[282] *Id.* (citing Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177, 189 (2004)).
[283] United States v. Robinson, 77 M.J. 303 (C.A.A.F. 2018).

In *Mitchell*, investigators sought to question the accused, who invoked his right to counsel.[284] Investigators then obtained a search authorization for the accused's mobile phone and seized the phone while the accused was in custody in his commander's office.[285] While still in the office, investigators saw that the phone was locked and asked the accused for his passcode.[286] When the accused refused, investigators asked him to unlock the phone, and the accused complied by entering the passcode three times: once to unlock the phone, then two more times to disable security features.[287] The CAAF applied the plain language of MRE 305(c)(2), which provides: "any statement made in the interrogation after such request [for counsel], or evidence derived from the interrogation after such request [for counsel], is inadmissible."[288] The CAAF suppressed the contents of the phone because it was evidence derived from interrogation after the accused requested counsel. As the Court explained, "The agents' initial request—'can you give us your PIN?'—is an express question, reasonably likely to elicit an incriminating response."[289] The follow-on request to unlock the phone with the passcode "was part of the same basic effort to convince Appellee to provide the information necessary for the Government to access and search the contents of his phone, and to help prove that he himself had the same ability . . . ."[290]

*Mitchell* thus would not bar a subpoena to compel decryption. Because the majority in *Mitchell* expressly declined to reach whether entry of the passcode was testimonial or compelled, it also did not reach the foregone conclusion doctrine. Rather, *Mitchell* was decided based on the *Edwards* and MRE 305(c)(2) issue; that is, the CAAF held that asking the accused for his passcode was a statement made in an interrogation after a request for counsel under MRE 305(c)(2). Indeed, the *Mitchell* majority does not mention the foregone conclusion doctrine, much less hold that a doctrine applied in Federal civilian courts since the Supreme Court decided *Fisher* in 1976 does not apply in the military. *Mitchell*'s only mention of the foregone conclusion doctrine comes in the dissent, which would have found it necessary to reach the questions of whether entering the passcode

---

[284] *Mitchell*, 76 M.J. at 415.
[285] *Id.* at 416.
[286] *Id.*
[287] *Id.*
[288] MCM, *supra* note 108, M.R.E. 305(c)(2).
[289] *Mitchell*, 76 M.J. at 418.
[290] *Id.*

was testimonial or incriminating and resolved those questions in the Government's favor. The majority, however, did not reach that question.

*2.* United States v. Robinson

The AFCCA in *United States v. Robinson* applied a line of foregone conclusion doctrine cases to investigators requesting a mobile phone passcode.[291] In *Robinson*, the accused invoked his right to counsel, then agents asked for consent to search his phone, which he provided; agents then asked for the passcode to execute the search, which the accused provided.[292] The AFCCA affirmed the trial court's denial of Robinson's motion to suppress, reasoning that "[b]ecause there was no dispute as to Appellant's ownership, dominion, or control over the phone, his knowledge of the passcode did not incriminate him. Investigators had no reason to believe that the passcode itself would be incriminating or communicate any information about the crime."[293] In reaching this conclusion, the AFCCA cited the Fourth Circuit's opinion in *United States v. Gavegnano* for the proposition that asking for a passcode did not violate the Fifth Amendment where "[a]ny self-incriminating testimony that he may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that [he] was the sole user and possessor of the computer."[294] Yet the AFCCA also found civilian case law regarding the foregone conclusion doctrine and compelled decryption "only marginally relevant to our analysis as the existence of an order to produce the information is not present in Appellant's case and there is no argument that Appellant's provision of his passcode was either compelled or mere acquiescence to an otherwise-valid order."[295]

The CAAF affirmed the AFCCA's holding. Though its reasoning differed from the AFCCA's, the CAAF majority did not criticize the lower court's reasoning or suggest that the foregone conclusion doctrine does not

---

[291] United States v. Robinson, 76 M.J. 663, 669 (A.F. Ct. Crim. App. 2017), *aff'd*, 77 M.J. 303 (C.A.A.F. 2018).
[292] *Id.* at 665.
[293] *Id.* at 671.
[294] *Id.* at 669 (alteration in original) (citing United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009)).
[295] *Id.* (citing United States v. Apple MacPro Comput., 851 F.3d 238 (3d Cir. 2017); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012)).

apply in the military. Instead, the CAAF reasoned that requesting a passcode after the appellant gave consent to search was "merely a natural and logical extension of the first permissible inquiry" under *United States v. Frazier*, in which the CAAF held that requests for consent are not interrogations and that consent to search is not a statement.[296] Judge Stucky's dissent in *Robinson* argued that *Mitchell* should control the outcome, but not because the foregone conclusion doctrine would not apply in the military. Rather, Judge Stucky simply would not have found the distinction between a consent search and a search authorization sufficient to distinguish *Robinson* from *Mitchell*.[297]

In a nutshell, the rules from the CAAF's opinions in *Mitchell* and *Robinson* are that after a request for counsel: (1) investigators may ask for consent to search a device, and, if the accused consents, investigators may ask for the passcode; (2) investigators may not ask for a passcode or for entry of a passcode without first asking for consent to search; and (3) investigators may not ask for a passcode or for entry of a passcode if the accused refuses consent to search. As explained in Section VII.C.4 below, these rules do not prevent obtaining the unlocked state of a device via subpoena in cases where the foregone conclusion doctrine applies.

*3.* United States v. Suarez

In *United States v. Suarez*, the Army Court of Criminal Appeals mentions civilian foregone conclusion doctrine case law in dicta without ruling on the issue.[298] The holding in *Suarez* was based on the accused making a statement without having been advised of his rights and without having waived his rights—not the foregone conclusion doctrine.[299] In *Suarez*, Army CID agents seized the accused's mobile phone pursuant to a search authorization. After seizing the phone, the agents asked the accused for his passcode, which he provided. Unlike in *Robinson*, the accused had not consented to a search prior to agents asking for the passcode.[300] The trial counsel conceded that agents asking for the passcode was a request for

---

[296] *Robinson*, 77 M.J. at 304 (quoting United States v. Frazier, 34 M.J. 135, 137 (C.M.A. 1992)).
[297] *Id.* at 307–08 (Stucky, J., dissenting).
[298] United States v. Suarez, No. 20170366, 2017 WL 4331014, at *2 (A. Ct. Crim. App. Sept. 27, 2017).
[299] *Id.* at *5.
[300] *Id.* at *1.

incriminating information that would trigger Article 31(b), UCMJ, and the Fifth Amendment.[301] The Army Court of Criminal Appeals thus denied the Government's Article 62, UCMJ,[302] appeal without reaching the foregone conclusion doctrine because the Government had waived the issue in the trial court.[303] The court went on to discuss *Mitchell* in dicta, stating that "[i]t is also unclear, whether *Mitchell* dispatched the foregone conclusion doctrine as a general matter or just based on the facts of that particular case."[304] In posing this question, the court cited to the Supreme Court's articulation of the foregone conclusion doctrine in *Fisher*, the Third Circuit's opinion in *Apple MacPro Computer*, and the Eleventh Circuit's opinion in *In re Grand Jury Subpoena Duces Tecum*.[305] The Army court, however, does not provide an answer to the question it poses, as the Government's waiver made reaching *Mitchell* and the foregone conclusion doctrine unnecessary.[306]

*4. Applying* Mitchell, Robinson, *and* Suarez *to Article 30a, UCMJ, Subpoenas*

The Article 30a, UCMJ, subpoena remains a lawful means to obtain the accused's device in an unencrypted state. In response to the question posed in *Suarez*, the CAAF in *Mitchell* did not rule that the foregone conclusion doctrine does not apply in the military. Rather, the CAAF applied the plain language of MRE 305(c)(2): "evidence derived from the interrogation after such request [for counsel], is inadmissible . . . unless counsel was present." Thus, at most, *Mitchell* stands for the proposition that the language of MRE 305(c)(2) would prevent the foregone conclusion doctrine from applying to the results of further interrogation after a request for counsel. Accordingly, the AFCCA's reasoning in *Robinson* might have been different after *Mitchell*, but not because *Mitchell* entirely bars the foregone conclusion doctrine from the military. Instead, the AFCCA in *Robinson* might merely have concluded that MRE 305(c)(2) rendered civilian case law such as

---

[301] *Id.* at *3.
[302] UCMJ art. 62 (2017).
[303] *Suarez*, No. 20170366, 2017 WL 4331014, at *5.
[304] *Id.* at *2 (citing United States v. Apple MacPro Comput., 851 F.3d 238 (3d Cir. 2017); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012)).
[305] *Id.*
[306] *Id.*

*United States v. Gavegnano* dealing with law enforcement continuing interrogations inapplicable.[307] As the AFCCA recognized, the case law dealing with court orders compelling decryption represent a distinct factual scenario.[308]

Serving an Article 30a, UCMJ, subpoena that directs the accused to provide a device in an unencrypted state is distinct from *Mitchell* in three ways. First, an Article 30a, UCMJ, subpoena would not direct the accused to provide a passcode to investigators. Rather, like in *Apple MacPro Computer*, such a subpoena would simply direct that the accused provide the device in an unlocked state at a future time.[309] How the accused accomplished this unlocking would be left to the accused. The provision of the device in an unlocked state is thus not a statement but a potentially testimonial act. The CAAF in *Mitchell* did not decide that providing a device in an unlocked state was *de facto* testimonial. Rather, the CAAF did not reach that question because the agents' request that the accused unlock the device followed both the invocation of the right to counsel and a request for the passcode and was thus further interrogation under MRE 305(c)(2).[310]

Second, a subpoena is not an interrogation. MRE 305(c)(2) suppresses only statements "made in the interrogation after such request [for counsel]." *Edwards* likewise bars only interrogation after a request for counsel. Thus, *Mitchell*'s holding based on both MRE 305(c)(2) and *Edwards* would not bar an Article 30a, UCMJ, subpoena. The most apposite civilian case is *Application of Martin*,[311] which involved a subpoena duces tecum to produce evidence. In *Martin*, the respondent moved to quash a subpoena to produce records and to attend a hearing and give testimony on the grounds that it violated the Fifth Amendment right against self-incrimination; the court denied the motion.[312] As the Court explained, the "mere service of a subpoena duces tecum cannot be equated with testifying as a witness against oneself."[313] Thus, it was "premature for the petitioner to invoke the Fifth Amendment until such time as he appears at a hearing before the

---

[307] *Compare* United States v. Robinson, 76 M.J. 663, 669 (A.F. Ct. Crim. App. 2017), *aff'd*, 77 M.J. 303 (C.A.A.F. 2018), *with* United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017).
[308] *Robinson*, 76 M.J. at 669.
[309] *Apple MacPro Comput.*, 851 F.3d 238.
[310] *Mitchell*, 76 M.J. at 419.
[311] Application of Martin, 188 N.Y.S.2d 566, 568 (N.Y. Sup. Ct. 1959).
[312] *Id.* at 567.
[313] *Id.*

Commission and is then required to respond to interrogation and to produce the records referred to in the subpoenas duces tecum."[314]

The Ninth Circuit in *United States v. Kilgroe* similarly held that service of a subpoena and the obligation to appear was not an interrogation requiring rights advisement.[315] In that case, Kilgroe was in-house counsel for a business where another employee was prosecuted for mail fraud. Kilgroe received a subpoena to testify at the employee's trial. During his testimony, Kilgroe made self-incriminating statements and was later prosecuted for mail fraud.[316] Kilgroe moved to suppress his statements on the grounds that he was not advised of his rights prior to testifying. The Ninth Circuit found no error in the trial court's denial of Kilgroe's motion to suppress. The subpoena merely created an "obligation to appear and testify truthfully."[317] This obligation did not itself "'constitute compulsion to give incriminating testimony' of the sort that implicates *Miranda*'s policies."[318] As the court explained, "[u]nlike custodial interrogation—which usually takes place without warning and, therefore, without the chance for reflection or legal advice—the subpoena gives the witness the opportunity in advance to obtain whatever counsel he deems appropriate and carefully contemplate his testimony."[319] The court went on to explain that the right against self-incrimination would apply at the hearing had Kilgroe been asked questions the answers to which would tend to incriminate him, explaining that "[Kilgroe] remains free, of course, to refuse to answer questions that would incriminate him" at such a proceeding.[320]

One can also glean from the lack of Federal civilian case law criticizing service of subpoenas on subjects of investigations that there is no constitutional issue with the practice. In *United States v. Kelly*, Federal prosecutors obtained a grand jury subpoena directed to an accused who had invoked his right to counsel.[321] While the subpoena in that case was not served, the Eighth Circuit provides no indication that a subpoena after invocation of the right to counsel was improper.[322] If such a subpoena were unlawful, surely the Eighth Circuit would have at least commented on that

---

[314] *Id.*
[315] United States v. Kilgroe, 959 F.2d 802 (9th Cir. 1992).
[316] *Id.* at 803.
[317] *Id.* at 804.
[318] *Id.* (quoting Miranda v. Arizona, 384 U.S. 436 (1966)).
[319] *Id.* at 804–05.
[320] *Id.* at 805 (citing United States v. Jenkins, 785 F.2d 1387, 1393 (9th Cir. 1986)).
[321] United States v. Kelly, 329 F.3d 624, 629 (8th Cir. 2003).
[322] *Id.*

matter, yet the Eighth Circuit appears wholly unconcerned with the procedure. Likewise, the two most cited cases concerning compelled decryption—the Third Circuit's *Apple MacPro Computer* and the Eleventh Circuit's *In Re Grand Jury Subpoena*—make no mention of service of a subpoena as a potential *Edwards* issue.[323] If there were a rule prohibiting service of a subpoena after invocation of rights, there would likely be some mention of that rule, but there is none.

Insofar as the foregone conclusion doctrine is concerned, there is no meaningful distinction between a civilian grand jury subpoena and an Article 30a, UCMJ, subpoena. The function of the subpoena is the same: directing the accused to provide a device in an unlocked state at some time after the service of the subpoena. Accordingly, a military court should consider the lack of Federal civilian case law questioning the practice of issuing a subpoena duces tecum to civilian defendants as indicative that such service does not raise an *Edwards* issue.

Third, even if serving a subpoena were somehow considered "further interrogation" after the invocation of the right to counsel, the Government could easily satisfy *Edwards* (and thus *Mitchell*) by serving the subpoena and providing the opportunity to comply in the presence of the accused's counsel. The right to counsel does not bar further interrogation outright; rather, it bars further interrogation without counsel present.[324] Indeed, MRE 305(c)(2) provides that statements made after a request for counsel are "inadmissible against the accused unless counsel was present for the interrogation."[325] Providing for the availability of counsel is also a matter of professional courtesy to defense counsel, who will likely be in the position of litigating a motion to suppress.

In most cases involving an investigative subpoena, the accused's right to counsel will arise only under the Fifth Amendment and Article 31, UCMJ, rights rather than the Sixth Amendment. The Sixth Amendment right to

---

[323] United States v. Apple MacPro Comput., 851 F.3d 238, 248 (3d Cir. 2017); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1345–46 (11th Cir. 2012).

[324] Edwards v. Arizona, 451 U.S. 477 (1981); Minnick v. Mississippi, 498 U.S. 146, 153 (1990) ("In our view, a fair reading of *Edwards* and subsequent cases demonstrates that we have interpreted the rule to bar police-initiated interrogation unless the accused has counsel with him at the time of questioning. Whatever the ambiguities of our earlier cases on this point, we now hold that when counsel is requested, interrogation must cease, and officials may not reinitiate interrogation without counsel present, whether or not the accused has consulted with his attorney.").

[325] MCM, *supra* note 108, M.R.E. 305(c)(2).

counsel does not attach until preferral of charges in the military justice system.[326] But applying the Sixth Amendment right to counsel would not change the outcome if a subpoena were served after preferral. Like MRE 305(c)(2) ("Fifth Amendment Right to Counsel"), the corresponding MRE 305(c)(3) ("Sixth Amendment Right to Counsel"), applies to "interrogation" after the accused requests or obtains counsel and includes the same "unless counsel was present for the interrogation" exception.[327]

### D. Biometric Decryption

The Article 30a, UCMJ, subpoena process may be used to obtain a device in an unlocked state regardless of the method of unlocking. Thus, in cases involving biometrics, the Government might elect the Article 30a, UCMJ, subpoena process, though it may prove impracticable for biometric decryption. Biometric decryption may automatically become disabled when a device has not been unlocked for a certain period of time or if it has been powered down and powered back up.[328] Thus, the biometric option may expire during the Article 30a, UCMJ, process.

Invoking the foregone conclusion doctrine may be unnecessary to compel biometric decryption. Courts are split as to whether biometric unlocking is a testimonial act that would require application of the foregone conclusion doctrine. But even those courts holding that biometric unlocking is a testimonial act recognize that the foregone conclusion doctrine can render such unlocking non-testimonial. Thus, the Government can bulletproof biometric unlocking by gathering evidence to show that the accused's ability to unlock the device is a foregone conclusion.

#### *1. Whether Biometric Decryption is a Testimonial Act*

Military appellate courts have not yet ruled on whether biometric decryption is a testimonial act protected by the Fifth Amendment. Civilian courts are split on whether biometric decryption implicates the Fifth Amendment. Several Federal district courts and state courts have held that biometric data, such as fingerprints and facial recognition, are not

---

[326] United States v. Kerns, 75 M.J. 783, 788 n.1 (A.F. Ct. Crim. App. 2016).
[327] *Compare* MCM, *supra* note 108, M.R.E. 305(c)(2), *with* M.R.E. 305(c)(3).
[328] *See, e.g.*, APPLE INC., FACE ID SECURITY 2 (2017).

testimonial and thus not protected by the Fifth Amendment.[329] These cases reason that the biometric information used to unlock the device (e.g., the accused's face or fingerprints) do not themselves communicate anything. For these courts, facial characteristics and fingerprints are simply physical characteristics displayed to the world, and any evidence that might result from recognizing these characteristics is not testimony inherent in the characteristics. The Northern District of Illinois, for example, argued for focusing the Fifth Amendment analysis on the compelled act at issue. As that court explained in *In re Search Warrant Application*, the fact that biometric data may lead to an incriminating inference does not make such data itself testimony.[330]

The cases holding biometric decryption is not testimonial rely on a series of Supreme Court cases holding that displays of physical characteristics are not testimonial in other contexts: fingerprinting,[331] photographing,[332] appearing in a line-up for visual identification,[333] saying a phrase during a line-up for voice identification,[334] providing a voice exemplar,[335] providing a handwriting exemplar,[336] and putting on clothing to test fit.[337] Most relevant are the holdings that appearing for a lineup, photographing, and fingerprinting are not testimonial because facial recognition and fingerprints are the most common biometric methods for decrypting mobile phones.

On the other hand, several U.S. district courts have held that biometric decryption is testimonial in nature.[338] These cases reason that unlocking a

---

[329] *See* Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014); *In re* Search Warrant Application, 279 F. Supp. 3d 800 (N.D. Ill. 2017); *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 539 (D.D.C. 2018); State v. Diamond, 905 N.W.2d 870 (Minn. 2018); *In re* Search of a White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785 (D. Idaho 2019); United States v. Barrera, 415 F. Supp. 3d 832 (N.D. Ill. 2019).

[330] *In re Search Warrant Application*, 279 F. Supp. 3d at 805.

[331] Schmerber v. California, 384 U.S. 757, 764 (1966); United States v. Wade, 388 U.S. 218, 222 (1967).

[332] *Schmerber*, 384 U.S. at 764; *Wade*, 388 U.S. at 222.

[333] *Wade*, 388 U.S. at 222 (holding that appearing for a line-up was not testimonial because "[i]t is compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have.").

[334] *Id.*

[335] United States v. Dionisio, 410 U.S. 1 (1973).

[336] Gilbert v. California, 388 U.S. 263 (1967).

[337] Holt v. United States, 218 U.S. 245 (1910).

[338] *See In re* Application for a Search Warrant, 236 F. Supp. 3d 1066 (N.D. Ill. 2017); *In re* Search of a Residence in Oakland, 354 F. Supp. 3d 1010 (N.D. Cal. 2019); United States

device with biometric data communicates information that the suspect had unlocked the device before, had set up the security on the device, and had control over the device. These cases also rely on the Supreme Court's articulation in *Riley v. California* of the importance of mobile phones in modern society and the volume of information stored on such devices to argue that biometric decryption is not the equivalent of the biometric displays for identification in prior Supreme Court cases.[339]

The opinions finding biometrics testimonial fail to distinguish what the compelled act itself communicates as opposed to the evidence that might be inferred from the device's reaction to the compelled act. As the U.S. District Court for the District of Columbia explained in *In re Search of [Redacted] Washington, D.C.*,[340] only the present unlocking is compelled—not any past use of the device—so the accused's prior conduct is not relevant to the Fifth Amendment inquiry. And, as the Northern District of Illinois explained in *United States v. Barrea*, the Supreme Court's applying the Fourth Amendment warrant requirement to mobile phones in *Riley* did not eliminate precedent holding that displays of physical characteristics were not testimonial.[341] Indeed, as the Supreme Court has warned lower courts, "If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions."[342] Thus, just as a witness identifying an accused from a line-up or mugshot does not render the act of appearing in the line-up or mugshot testimonial, neither should an electronic device reacting to the accused's face make the display testimonial. Likewise, just as a hit in a fingerprint database as a result of compelled fingerprinting does not render the fingerprinting testimonial, a mobile device recognizing the accused's fingerprint should not render the application of the accused's finger testimonial. In either case, agents are simply applying the accused's physical characteristic to an electronic sensor lawfully in the Government's possession.

---

v. Sealed Warrant, 2019 U.S. Dist. LEXIS 147836 (N.D. Cal. Aug. 16, 2019); United States v. Wright, 431 F. Supp. 3d 1175 (D. Nev. 2020).

[339] *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1073–74 (citing Riley v. California, 573 U.S. 373 (2014)).

[340] *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 539 n.12 (D.D.C. 2018).

[341] United States v. Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019).

[342] Rodriguez de Quijas v. Shearson/Am. Express, Inc., 490 U.S. 477, 484 (1989).

*2. Biometric Decryption as a Foregone Conclusion*

Even courts that consider biometric decryption testimonial also recognize that the foregone conclusion doctrine applies and can render the use of biometrics non-testimonial in a particular case. For instance, the District Court for the Northern District of California has held that biometric decryption is testimonial but that the Government could compel biometric unlocking if a "particular individual's ability to unlock a particular electronic device is a foregone conclusion."[343]

So, before taking steps to unlock a device with biometrics, agents should be able to articulate how they already know the phone belongs to the accused and that the accused can unlock it. Sources of such evidence may include: (1) surveillance of the accused; (2) the origin of the phone (e.g., if the accused had the phone on their person or in their vehicle); (3) calling or texting the accused's personal phone number obtained from a co-worker or a recall roster to see if the phone reacts;[344] (4) witnesses who have seen the accused unlock the device; (5) witnesses, including the victim, who have seen the accused use their phone; (6) the accused's fingerprints on the phone;[345] (7) statements of the accused, if available; and (8) evidence of a person's regular use of the device because "[i]ndividuals ordinarily must know the password of devices they regularly use."[346] The Government would be well-advised to draw from as many of these sources as possible.

If foregone conclusion doctrine evidence is not available, the Government should still pursue biometric unlocking because the better-reasoned cases find biometric unlocking non-testimonial. If foregone conclusion doctrine evidence can be found, however, the Government can eliminate litigation risk to the mobile phone unlocking by gathering such evidence prior to compelled biometric unlocking.

*3. Determining if Biometrics Are Enabled*

Military courts have not yet ruled on whether asking if biometrics are enabled would be impermissible interrogation under *Mitchell* or a permissible preliminary question incident to an authorized search under

---

[343] United States v. Sealed Warrant, 2019 U.S. Dist. LEXIS 147836, at *7–11 (N.D. Cal. Aug. 16, 2019).
[344] Kerr, *supra* note 2, at 783.
[345] *Id.*
[346] *Id.*

*United States v. Poole*.[347] In *Poole*, the AFCCA found the question, "Do you have a cell phone?" was proper, as it "was designed to assist in the execution of the search warrant and not to elicit an incriminating response."[348] As it further explained, "We find the rationale of our sister service court applicable in this case that certain preliminary questions to assist in the execution of a search authorization do not require rights advisement where the questions were 'mere preliminary vocal aids to the ongoing legal search.'"[349] The AFCCA distinguished *Mitchell* on the grounds that *Poole* did not involve custodial interrogation or invocation of rights.[350] Likewise, in *United States v. Neely*, agents asked an Airman for his locker key and to identify his locker after he had invoked his right to counsel.[351] The AFCCA found no Fifth or Sixth Amendment violations because the identification "was only preliminary assistance in the search, which defined and limited its area, and which could have been readily defined and localized without his assistance."[352] The questions and the accused's answers were thus "not within the protection of Article 31."[353]

Because courts have not ruled on asking whether biometrics are enabled, Government agents ideally should determine that fact without asking the accused. This information can come from the phone itself (e.g., if the phone's lock screen displays whether biometrics are enabled). This information could also come from witnesses who have seen the accused unlock the device with biometrics.

*4. The Adequacy of Biometric Unlocking*

Biometric unlocking may also prove inadequate for investigative purposes. In some cases, forensic extraction tools may not work unless a device's security features such as automatic re-locking are disabled. Some mobile phones require entering a passcode to disable these security features.

---

[347] United States v. Poole, No. ACM 39308, 2019 CCA LEXIS 235, at *17–18 (A.F. Ct. Crim. App. May 15, 2019).
[348] *Id.*
[349] *Id.* at *6 (quoting United States v. Bradley, 50 C.M.R. 608, 621 (N.C.M.R. 1975)).
[350] *Id.* n.4 (citing United States v. Mitchell, 76 M.J. 413 (C.A.A.F. 2017)).
[351] United States v. Neely, 47 C.M.R. 780, 782 (A.F.C.M.R. 1973).
[352] *Id.*
[353] *Id.*; *see Bradley*, 50 C.M.R. at 621 (holding that no Article 31, UCMJ, rights warning was required before law enforcement asked a Sailor subject to a lawful search if he had any money, directed him to remove the money from his wallet and count it, and seized money with a particular serial number as evidence).

If biometric unlocking alone will not enable the Government to perform the necessary search, then the Government should utilize the Article 30a, UCMJ, subpoena process to compel production of the device in an unlocked state with such security features disabled.

## VIII. Alternatives to the Article 30a, UCMJ, Investigative Subpoena

Provided that the foregone conclusion doctrine applies, Article 30a, UCMJ, is not the only lawful means to compel an accused to decrypt an electronic device. There are four other means available to the Government in cases where a passcode is necessary to decrypt the device. First, a superior officer may order an accused to surrender a device in a decrypted state without any action by a court. Second, the convening authority may authorize Government counsel to issue pre-referral subpoenas. Third, the Government may obtain evidence for an Article 32, UCMJ, preliminary hearing by means of a military judge-issued investigative subpoena or a Government counsel-issued investigative subpoena authorized by the GCMCA. Fourth, after referral, trial counsel may issue a subpoena to the accused. While all of these options could be lawful under the foregone conclusion doctrine, the Article 30a, UCMJ, subpoena provides the most orderly process for litigating the accused's rights. In cases where biometric decryption is possible, a fourth option of using reasonable force to compel biometric decryption may be available and may be most practical if biometric decryption will become impossible before Article 30a, UCMJ, litigation can be resolved.

### A. The Commander's Order—Lawful, But No Immediate Avenue for Relief

So long as the foregone conclusion doctrine applies, a superior officer's order to the accused to provide a lawfully seized device in an unencrypted state would be lawful. The foregone conclusion doctrine does not require a particular means of compulsion—it simply determines whether the accused's Fifth Amendment rights apply to the compulsion.[354]

The Government should nevertheless select the Article 30a, UCMJ, process in most cases. Article 30a, UCMJ, provides the accused with the

[354] *See generally* discussion *supra* Part VII.

motion to quash to obtain a ruling on the lawfulness of the subpoena. The superior officer's order, by contrast, requires the accused to decide whether to risk future prosecution for disobeying the order without an immediate avenue for relief. If the accused disobeys a superior officer's order, the only practical avenue for relief is to litigate the issue in a later prosecution under Article 90, UCMJ. Air Force Instruction ("AFI") 90-301 provides that punishments under the UCMJ are not appropriate for the Inspector General system.[355] Likewise, AFI 51-505 provides that Article 138, UCMJ,[356] review is not appropriate for matters related to disciplinary action under the UCMJ where "the petitioner may seek redress through other forums which provide the petitioner notice, opportunity to be heard, and review by an appellate authority."[357] Article 131f, UCMJ, is not practically available to the accused, and it would not apply in any event. The CAAF in *United States v. McElhinney* noted that the convening authority's refusal to order production of witness would violate Article 131f(2), UCMJ, only after a final court order directing production of witnesses.[358] A superior officer's order to the accused, by contrast, would be issued prior to a judge's order with the good faith belief that the foregone conclusion doctrine rendered the order lawful. Thus, the officer would not have "knowingly and intentionally" violated a provision of the UCMJ under Article 131f(2) except in the unlikely event an officer acted after a judge's order to the contrary.[359]

In sum, while the foregone conclusion doctrine could render a commander's order lawful, the Government should nonetheless prefer the Article 30a, UCMJ, subpoena in most cases. There may be circumstances, however, where time is of the essence and the Government simply cannot wait for the Article 30, UCMJ, process. Moreover, as Professor Schlueter notes, "providing for judicial rulings and relief before the referral of charges may actually delay the proceedings if the parties are permitted to appeal a judge's pre-referral ruling through extraordinary writs to a service appellate court."[360] If Article 30a, UCMJ, litigation and appellate review render the

---

[355] U.S. DEP'T OF AIR FORCE, INSTR. 90-301, INSPECTOR GENERAL COMPLAINTS RESOLUTION para. 2.3, tbl.3.7 (20 Dec. 2018) (C1, 30 Sept. 2020).
[356] UCMJ art. 138 (1950).
[357] U.S. DEP'T OF AIR FORCE, INSTR. 51-505, COMPLAINTS OF WRONGS UNDER ARTICLE 138, UNIFORM CODE OF MILITARY JUSTICE para. 1.3.3.8 (4 Apr. 2019).
[358] United States v. McElhinney, 21 U.S.C.M.A. 436, 439 (C.M.A. 1972).
[359] UCMJ art. 131f (2016).
[360] Schlueter, *supra* note 42, at 48.

pre-referral subpoena impractical due to delay, the superior officer's order may be preferable.

B. Convening Authority Authorized Investigative Subpoena Under Article 46, UCMJ—Lawful and Timely, But Enforcement and Relief Inevitably Require Judicial Intervention

Article 46(d)(2), UCMJ, and RCM 703(g)(3)(D)(v) allow the GCMCA to authorize Government counsel to issue pre-referral investigative subpoenas. Such a subpoena directed to the accused, however, will almost certainly require judicial intervention for enforcement or relief. Article 46(e), UCMJ, provides the procedures for relief from subpoenas issued under that article, stating that:

> If a person requests relief from a subpoena or other process under this section (article) on grounds that compliance is unreasonable or oppressive or is prohibited by law, a military judge detailed in accordance with section 826 or 830a of this title (article 26 or 30a) shall review the request and shall—
>
> (1) order that the subpoena or other process be modified or withdrawn, as appropriate; or
>
> (2) order the person to comply with the subpoena or other process.[361]

Rule for Courts-Martial 703(g)(3)(G) concerning relief from subpoenas mirrors Article 46(e), UCMJ, providing that:

> (G) Relief. If a person subpoenaed requests relief on grounds that compliance is unreasonable, oppressive, or prohibited by law, the military judge or, if before referral, a military judge detailed under Article 30a shall review the request and shall—
>
> (i) order that the subpoena be modified or quashed, as appropriate; or
>
> (ii) order the person to comply with the subpoena.[362]

Thus, in the case of a GCMCA-authorized pre-referral investigative subpoena issued by counsel for the Government, an Article 30a, UCMJ, proceeding will become necessary given the near certainty that the accused

---

[361] UCMJ art. 46(e) (2016).
[362] MCM, *supra* note 108, R.C.M. 703(g)(3)(G).

will request relief from the subpoena. Under RCM 905(j), the recipient of the subpoena could request relief from the convening authority,[363] but such a request is without prejudice to a later request for relief from a military judge, so the accused would almost certainly pursue judicial relief if the convening authority declined to grant relief. Therefore, given the near inevitability of judicial intervention, the Government would be well advised to pursue a judicially issued Article 30a, UCMJ, subpoena from the outset.

### C. Subpoena for Production of Evidence During the Article 32, UCMJ, Process—Lawful, But Too Late and with No Immediate Avenue for Relief in the Article 32, UCMJ, Process

In most cases, the Government should proceed with investigative subpoena practice well before the Article 32, UCMJ, preliminary hearing. The preliminary hearing superficially resembles a civilian grand jury in that the preliminary hearing officer (PHO) makes a probable cause determination.[364] But the Article 32, UCMJ, process is untimely when compared with the civilian grand jury process. An Article 32, UCMJ, hearing is not available until after preferral of charges, at which point investigative work ideally will have been completed.[365] Moreover, in some cases, it might not be possible to even get to an Article 32, UCMJ, hearing without obtaining an unencrypted electronic device. An Article 32, UCMJ, hearing comes after preferral, and the Service member preferring charges must certify that they have investigated the matters set forth in the charges and that such matters are true to the best of their knowledge and belief.[366] The Government might not reach this threshold absent evidence obtained from an encrypted electronic device.

The investigative subpoena powers used to obtain evidence for a preliminary hearing are the same powers that could be utilized earlier in an investigation.[367] Delaying the use of such powers until a preliminary hearing offers no advantages. The Article 32, UCMJ, preliminary hearing itself does not provide a forum to obtain a ruling on the merits of a subpoena. Indeed, the PHO has no authority to rule on the merits of a motion to quash

---

[363] *Id.* R.C.M. 905(j).
[364] UCMJ art. 32 (2016).
[365] *Id.*
[366] MCM, *supra* note 108, R.C.M. 307(b)(2).
[367] *Id.* R.C.M. 405(h)(3)(B)(i).

a subpoena or impose any penalty on an uncooperative respondent.[368] Enforcement of a subpoena issued to a Service member will thus inevitably fall to a military judge's contempt powers, a subsequent court-martial, or both.

Therefore, prosecutors are unlikely to delay investigative subpoena practice until an Article 32, UCMJ, preliminary hearing as a means of addressing encrypted devices. These disadvantages, however, would not render investigative subpoenas relating to an Article 32, UCMJ, hearing unlawful. Like any other pre-referral investigative subpoena, the lawfulness of the subpoena would depend on the applicability of the foregone conclusion doctrine.

### D. Trial Counsel Subpoena After Referral—Lawful, But Too Late

After referral, trial counsel detailed to a court-martial may also issue subpoenas, but such subpoenas come even later in the military justice process than subpoenas related to Article 32, UCMJ, hearings.[369] As a result, trial counsel subpoenas after referral, although lawful, are even less useful as an investigative tool than subpoenas authorized by a GCMCA in connection with an Article 32, UCMJ, proceeding.

### E. Use of Force to Compel Biometric Decryption

A subpoena or order will not be the Government's only option in cases involving biometric decryption. Biometric decryption may automatically become disabled when a device has not been unlocked for a certain period of time or if it has been powered down and powered back up.[370] Thus, if a device can be unlocked with biometrics, time may be of the essence in unlocking the device.

Where agents have lawful authority to conduct a search and seizure, agents may use reasonable force to execute that search and seizure.[371] To avoid Fifth Amendment concerns, Opher Schweiki and Youli Lee of the Department of Justice recommend that agents obtain biometric decryption

---

[368] UCMJ art. 32.
[369] MCM, *supra* note 108, R.C.M. 703(g)(3)(D)(ii).
[370] *See, e.g.*, APPLE INC., *supra* note 328.
[371] *See* Graham v. Connor, 490 U.S. 386, 394 (1989) (providing that the Fourth Amendment reasonableness standard governs claims of excessive force during searches and seizures).

with as little action by the accused as possible.[372] Thus, agents ideally should determine what method of biometric decryption to apply without asking the accused. Additionally, agents should also hold the phone up to the accused for facial recognition or select the finger used for fingerprint identification if possible.[373]

Schweiki and Lee also recommend the Government obtain a search warrant specifically authorizing the use of the accused's biometrics to unlock a device. They note that the Fourth Amendment generally "does not require specificity as to how the warrant will be executed" beyond the Fourth Amendment's reasonableness requirement.[374] They nevertheless recommend obtaining specific authorization language out of an abundance of caution in light of the novelty of compelled decryption case law and a recent opinion by the District Court for the District of Columbia stating that the judge "expect[ed] that, absent exigent circumstances, the government will continue to seek prior authorization for the compelled use of an individual's biometric features to unlock digital devices even where the search of such devices is permitted by a warrant."[375]

### F. The Article 30a, UCMJ, Subpoena and Order and the Rights of the Accused

The prospect of a military judge issuing a subpoena and ordering the accused to produce evidence under Article 30a, UCMJ, raises concerns for the rights of the accused. The UCMJ has reflected Congress's concern for the rights of the accused since its inception. For example, Congress enacted Article 31, UCMJ, requiring rights advisement for the accused in 1956—a decade before the Supreme Court decided *Miranda v. Arizona* in 1966.[376] Yet an Article 30a, UCMJ, subpoena to compel decryption is merely a part of the search and seizure process, where the Fourth Amendment and MRE

---

[372] Opher Shweiki & Youli Lee, *Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments*, 67 DEP'T JUST. J. FED. L. & PRAC. 23, 39 (2019).
[373] *Id.*
[374] *Id.* at 27–28 (citing Dalia v. United States, 441 U.S. 238, 247–48 (1979)).
[375] *Id.* at 32 (quoting *In re* Search of [Redacted] Wash., D.C., 317 F. Supp. 3d 523, 533 n.8 (D.D.C. 2018)).
[376] Miranda v. Arizona, 384 U.S. 436 (1966); *see* United States v. Mayo, No. Army 20140901, 2017 CCA LEXIS 239, at *20–23 (A. Ct. Crim. App. June 16, 2017) (describing that Congress's enactment of court-martial voting provisions was based on concerns about unlawful command influence).

311 already protect the rights of the accused. Moreover, applying the foregone conclusion doctrine in the military justice system merely places the accused in the same position as the recipient of a subpoena in a civilian Federal court. Accordingly, the Article 30a, UCMJ, subpoena process should generally be used as the forum to litigate the rights of the accused in cases involving compelled decryption.

## IX. Admissibility of the Accused's Conduct at Trial

The admissibility of the accused's actions will depend on whether (1) the accused's actions were voluntary or compelled and (2) the accused consents or refuses to decrypt the device. If the accused voluntarily consents to a search and decrypts the device, that action will be admissible against the accused. In such a case, the accused will have waived the right against self-incrimination. The Government could thus use the accused's conduct as evidence of ownership and control of the device.

If the accused refuses to decrypt a device voluntarily, that refusal will not be admissible against the accused because it would be treated as an invocation of rights. Just as an accused's request for a lawyer or invocation of the right to remain silent is inadmissible against the accused, so too would the invocation of the right against self-incrimination in response to a voluntary request to decrypt a device be inadmissible.[377]

If the accused is compelled to provide a device in an unencrypted state, the act of providing the device in that state will not be admissible against the accused to show ownership or control of the device.[378] But the Government's evidence used to prove up the foregone conclusion doctrine in motions practice would be admissible to show the accused's ownership of the device because such evidence was gathered independent of any compulsion.

If, on the other hand, the accused refuses to comply with a judge's order to decrypt a device, such refusal would be admissible against the accused. Once a judge has ruled on the validity of the subpoena, the accused's

---

[377] MCM, *supra* note 108, M.R.E. 301(f)(2); United States v. Riley, 47 M.J. 276, 279–80 (C.A.A.F. 1997).

[378] United States v. Davis, 767 F.2d 1025, 1040 (2d Cir. 1985) ("Judge Conner's carefully crafted order specifically provided that the Government could not use the directive as an admission that the bank accounts existed, that Davis had control over them, or for any other purpose. These limitations on the use of the direction obviate any claim of testimonial compulsion.").

conduct is not a proper invocation of rights but deliberate disobedience of a court order to frustrate an investigation. As such, the accused's conduct would be admissible as evidence of consciousness of guilt much like other conduct to frustrate a lawful search or seizure. Military and civilian courts recognize that "an inference of consciousness of guilt can be drawn from the destruction of evidence is well-recognized in the law."[379]

## X. Conclusion

As the MJRG report recommended, MJA 2016 created a military investigative subpoena practice based on the model of civilian investigative subpoena practice. Thus, just as Federal civilian practitioners employ grand jury subpoenas to compel decryption, so too should military practitioners use Article 30a, UCMJ, subpoenas to compel decryption. Such practice will avoid the incongruous situation in which different evidence might be available to prosecutors in a court-martial as opposed to a Federal district court. While issuing a subpoena to the accused will be a new practice for many judge advocates, it is not a novelty to Federal civilian prosecutors, and military courts can draw on a substantial body of Federal civilian case law.

Digital evidence is already common in courts-martial, and it will only become more ubiquitous. Such evidence is not limited to cases in which data on a device is itself contraband. In many cases, messages, photos, videos, application data, and other data may serve as evidence of an offense where the digital data itself is not contraband. The Article 30(a), UCMJ, subpoena will allow prosecutors to level the playing field with the defense's utilization of RCM 703 to access victim mobile devices. It is common in courts-martial for the defense to request that the Government compel crime victims to surrender data from their mobile phones and to issue subpoenas for that purpose. The defense can then utilize the threat of remedies under RCM 703 to compel access to data on a victim's device if the prosecution is to proceed, functionally compelling decryption by the victim. The Article 30a, UCMJ, subpoena now gives the Government a tool in the investigative stage to compel the accused to provide a device in an unencrypted state when executing the lawful authority to search and seize.

---

[379] United States v. Moran, 65 M.J. 178, 188 (C.A.A.F. 2007); *see* Sullivan v. Gen. Motors Corp., 772 F. Supp. 358, 360 (N.D. Ohio 1991); State v. Strub, 355 N.E.2d 819, 825 (Ohio Ct. App. 1975); United States v. Howard, 228 F. Supp. 939, 942 (D. Neb. 1964).

Effective use of the Article 30a, UCMJ, subpoena will require judge advocates to work closely with investigators during the investigative stage of a case. In particular, judge advocates can work with investigators on how to lay the factual groundwork for the foregone conclusion doctrine. Judge advocates must keep in mind that the Government will bear the burden of putting on evidence establishing the foregone conclusion doctrine in motions practice. In the military context, such evidence may be more readily available than in the civilian context. In the case of mobile phones, for example, the Government will know where the accused works and have access to both co-workers and the workplace, potentially enabling surveillance of phone use or interviewing witnesses of phone use.

In the event that an accused disobeys a military judge's order to provide a device in an unencrypted state, prosecutors should aggressively pursue such disobedience either in a separate court-martial or by adding additional charges to the case at bar. The lack of civil contempt in military courts is a disadvantage relative to civilian courts. Indeed, confinement for civil contempt in civilian courts can be lengthy.[380] But the availability of UCMJ articles with a maximum punishment of up to five years confinement and a dishonorable discharge in criminal prosecutions nevertheless provides the military justice system with significant consequences for noncompliance.

This article recommends the Article 30a, UCMJ, judicial subpoena process over the other lawful processes available. The most significant advantage of the judicially issued Article 30a, UCMJ, subpoena process is providing the defense with an immediate forum in which to litigate the lawfulness of the subpoena. But the foregone conclusion doctrine is agnostic as to the means of compulsion. Thus, if Article 30a, UCMJ, practice becomes practically untenable, the Government might elect more expedient means of obtaining a device in an unencrypted state.

---

[380] *E.g.*, Chadwick v. Janecka, 312 F.3d 597 (3d Cir. 2002) (permitting civil contempt confinement of over seven years).