What *Riley v. California* Means for Military Justice

Lindsay Windsor[*]

During the 2013 to 2014 term, the Court of Appeals for the Armed Forces (CAAF) considered a challenge to the warrantless search of a military member's cell phone.[1] In *United States v. Wicks*, the CAAF held that a warrant was required before the government could lawfully search all the text messages on the servicemember's phone, even though a private party had already seen some of them.[2] Four months later, on June 25, 2014, the Supreme Court issued a seminal opinion in *Riley v. California*,[3] which identified for the first time what privacy rights an individual has in his cell phone. The Court considered warrantless searches of a cell phone's content incident to a lawful arrest, and it held, in a unanimous decision, that such searches generally require a warrant.[4] This article compares the Supreme Court's *Riley* decision with the CAAF's *Wicks* decision and finds that they are complementary. It then evaluates how *Riley* changes Fourth Amendment jurisprudence and what that means for the military.

The Supreme Court's Decision in *Riley v. California*

The Supreme Court decided the appeals of two companion cases—each involving the search of a cell phone incident to a lawful arrest—in one opinion: an appeal from the California Supreme Court in *People v. Riley*,[5] and an appeal from the First Circuit decision in *United States v. Wurie*.[6] In each case, police officers seized the petitioner's cell phone upon arrest and searched the contents of the cell phone for evidence of criminal activity. In *Riley*, the criminal evidence that police seized from the cell phone was unrelated to the crime for which Riley was first arrested.[7] In *Wurie*, the accused was arrested for selling drugs.[8] A search of his cell phone call log eventually led police to his home apartment, where officers found more evidence of drug dealing as well as a firearm.[9] Each trial court denied the petitioner's motion to suppress the evidence obtained as a result of the warrantless cell phone search.

A warrantless search incident to a lawful arrest is a well-established exception to the Fourth Amendment's warrant requirement.[10] In *Chimel v. California*[11] the Supreme Court ruled that warrantless searches of the area in the "possession" or "control" of an arrestee are reasonable within the Fourth Amendment for two reasons: they ensure officer safety by securing weapons and other contraband, and they prevent the destruction of evidence.[12] The Court applied this reasoning in *United States v. Robinson* to hold that police may search an arrestee's person incident to a lawful arrest without a warrant.[13]

The Court in *Riley* specifically rejected these rationales as applied to searches of the contents of cell phones incident to a lawful arrest. First, the digital data contained within the phone poses no physical threat to an arresting officer.[14] The Court's rejection of the second *Chimel* rationale—destruction of evidence—in the cell phone context is the most remarkable. There, the Court engaged modern technological considerations in an unprecedented way to evaluate the "reasonableness" which lies at the core of Fourth Amendment jurisprudence.[15] Recognizing a dearth of "precise guidance from the founding era," the Court applied a broad balancing test, weighing "the degree to which [a search] intrudes upon an individual's privacy, and . . . the degree to which it is needed for the promotion of legitimate governmental interests."[16] The Court acknowledged that some evidence of crimes may be destroyed as a result of its decision—perhaps by remote wiping of the device or data encryption—but that the government's interest in law enforcement must be balanced against the individual's privacy interest. For cell phones, this privacy interest is profound due to the immense capacity

---

[*] Lindsay Windsor is a law clerk for the Honorable Scott Stucky of the U.S. Court of Appeals for the Armed Forces. She holds a B.A. from Cornell University, and an M.A. in Security Studies and a J.D. from Georgetown University. The views expressed herein are my own and do not represent the views of the Court of Appeals for the Armed Forces or the U.S. Government.

[1] United States v. Wicks, 73 M.J. 93 *reconsideration denied*, 73 M.J. 264 (C.A.A.F. 2014).

[2] *Id.*

[3] 134 S. Ct. 2473, 2477, 189 L. Ed. 2d 430 (2014).

[4] *See id*.

[5] D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013) (unpublished).

[6] 728 F.3d 1, 16 (1st Cir. 2013).

[7] *Riley*, 134 S. Ct. at 2481.

[8] *Id.*

[9] *Id.*

[10] *Id.* at 2482 (citing Weeks v. United States, 232 U.S. 383, 392 (1914)) (noting that this exception has been "well accepted" since 1914).

[11] 395 U.S. 752, 760 (1969).

[12] *Id.* at 762–63.

[13] 414 U.S. 218 (1973).

[14] *Riley*, 134 S. Ct. at 2485.

[15] *Id.* at 2486–87.

[16] *Id.* at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

of a cell phone to store all manner of personal information.[17] Consequently, the Court held that requiring a warrant for a cell phone search in most circumstances is worth the minimal "impact on the ability of law enforcement to combat crime."[18]

In conducting the balancing test, the Court first discounted law enforcement concerns regarding evidence destruction by listing common-sense arguments undermining the government's assertions that cell phone evidence may be destroyed after the seizure of the cell phone.[19] The instances of remote wiping and data encryption are not prevalent, the Court observed; rather, such events are largely anecdotal.[20] Arrestees will have limited opportunities to encrypt or to wipe data remotely from their cell phones in the time between arrest and the cell phone search pursuant to a warrant.[21] The Court explained that during arrest proceedings, officers are engaged in other pressing matters such as securing the scene, and they will only turn to the contents of the phone later in the process. This delay alone provides enough time for the remote wiping or encryption of data that the government fears; therefore, searching the contents of the phone incident to arrest is not likely to have an impact if the accused is privy to such methods.[22] Moreover, police have access to technical solutions which minimize the risk of technical destruction or blocking of cell phone data.[23]

The Court next discussed the privacy interest individuals have in their cell phones. It recognized that the digital data stored on a cell phone is categorically different from physical objects and devoted over a thousand words of the opinion to explaining the vast capabilities of modern cell phones and how they differ from physical objects like a wallet or a purse.[24] Among the specific differences it listed are:

1) The quantity of data a cell phone can hold, which would be the physical equivalent of a large physical storage unit which the Court has held requires a warrant to search.[25]

2) The many different types of data on a cell phone, including photographs, text messages, Internet browsing history, a calendar, phone book, etc.

3) The pervasiveness of cell phones in society and of cell phones being carried on the person, especially as compared to personal notes or diaries which historically would rarely be found on a person.

4) The qualitative scope of data a cell phone can store, such as historic location information and downloaded apps, compared to the limitations of physical records.[26]

Cell phones contain "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate."[27] The Court concluded that, due to this vast trove of diverse data, "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."[28] "Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[29]

The Fourth Amendment in the Military and *United States v. Wicks*

The search and seizure protections of the Fourth Amendment generally apply to military members.[30] Some Fourth Amendment protections, such as the requirement that a warrant be supported by oath or affirmation, are not applicable in the military.[31] Yet military courts have consistently held that the Supreme Court's jurisprudence about the reasonableness of a search also applies to military searches.[32]

The reasonable expectation of privacy for a servicemember, though, is diminished in certain circumstances. Military members are governed by the Supreme Court's general rule that a standard of

[17] *See id.* at 2489–91.

[18] *Id.* at 2493.

[19] *Riley*, 134 S. Ct. at 2486–88.

[20] *Id.* at 2486–87.

[21] *Id.* at 2487.

[22] *Id.*

[23] *Id.* (describing technical solutions such as turning off the cell phone or placing it in a "Faraday bag," an enclosure "that isolates the phone from radio waves.").

[24] *Id.* at 2484, 2489–91.

[25] United States v. Chadwick, 433 U.S. 1, 15 (1977) (holding that a 200–pound, locked footlocker could not be searched incident to arrest), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565 (1991).

[26] *Riley*, 134 S. Ct. at 2489–91.

[27] *Id.* at 2490.

[28] *Id.* at 2491 (emphasis in original).

[29] *Id.* at 2493.

[30] United States v. Paige, 7 M.J. 480, 484 (C.M.A. 1979).

[31] United States v. McCarthy, 38 M.J. 398, 401 (C.M.A. 1993).

[32] *See, e.g.*, United States v. Cote, 72 M.J. 41 (C.A.A.F. 2013); United States v. Stevenson, 66 M.J. 15 (C.A.A.F. 2008); United States v. Springer, 58 M.J. 164 (C.A.A.F. 2003).

reasonableness, rather than probable cause, governs employers' "work-related, noninvestigatory intrusions as well as investigations of work-related misconduct."[33] For instance, it is presumed that a military member has "no reasonable expectation of privacy in the government computer provided to him for official use," though this presumption is rebuttable.[34]

In the military, commanders may authorize inspections of otherwise protected areas, such as cars or barracks, "to ensure the security, military fitness, or good order and discipline of the unit."[35] The inspection may include "an examination to locate and confiscate unlawful weapons and other contraband."[36] "[C]ompulsory random urinalysis" is also a permissible form of inspection.[37] Further, military members lack the same reasonable expectation of privacy in the room where they sleep that is afforded to civilians. The CAAF has held that servicemembers have some degree of "reasonable expectation of privacy in a shared barracks room that protects them from unreasonable government intrusions," but this privacy interest is not "coextensive" with the privacy interest in one's home.[38] Evidence of criminal activity revealed or seized in an inspection may be introduced at trial when relevant and not otherwise inadmissible.[39]

Like the Supreme Court in *Riley*, the CAAF in *Wicks* recognized an individual's privacy interest in the contents of his personal cell phone. Technical Sergeant (TSgt) Wicks' ex-girlfriend had pilfered his phone, scrolled through some of the text messages on it, and turned it over to military law enforcement when she learned that he was under investigation for engaging in inappropriate relationships.[40] The Government seized, searched, and analyzed all the text messages on the phone.[41] It found evidence in the text messages that TSgt Wicks was conducting inappropriate relationships, and sought to admit that evidence at TSgt Wicks' trial.[42] The Government argued the evidence was admissible under the private search doctrine, since some of the text messages had already been viewed by a private party.[43]

The CAAF rejected this argument and held that the fruits of the cell phone search were inadmissible.[44] While the private search doctrine allows the Government to use evidence that a private party has already viewed, that authority is bounded: the Government may not significantly expand the scope of a private search.[45] In this case, the private search uncovered only a few text messages and the Government searched and analyzed over 45,000 text messages from TSgt Wicks' phone.[46] In addition to evidence of criminal activity, the Government's search uncovered personal information and deleted text messages.[47] The CAAF held that the Government thus had exceeded the scope of the private search "in both a qualitative and quantitative manner" in violation of the Fourth Amendment.[48]

In its analysis of the privacy interest an individual has in his cell phone, the CAAF observed that cell phones are "an electronic repository of vast amounts of data" and that "individuals 'store much more personal information on their cell phones than could ever fit in a wallet, address book, briefcase, or any of the other traditional containers.'"[49] Thus, the expectation of privacy a military member has in his cell phone contents is a reasonable one.[50] Unlike the Supreme Court in *Riley*, the CAAF did not then consider a balancing test between the Government's law enforcement interest and the particularized privacy interest in a cell phone. Instead, the CAAF turned directly to analysis of the private search doctrine in this case. It did, however, recognize that a military member has a reasonable expectation of privacy in

---

[33] O'Connor v. Ortega, 480 U.S. 709, 724 (1987) (plurality opinion).

[34] United States v. Larson, 66 M.J. 212, 215–16 (C.A.A.F. 2008) (finding that a servicemember did not rebut the presumption where, when the accused used the computer, "a banner appeared that stat[ing] that it was a DOD computer, it [was] for official use, not to be used for illegal activity," and use of the computer required the user to consent to monitoring); *see also* City of Ontario, Cal. v. Quon, 560 U.S. 746, 761 (2010) (holding that a city's search of the text message transcripts of an employee's city-issued pager was reasonable because it was for "a noninvestigatory, work-related purpose or for the investigation of work-related misconduct," and "justified at its inception because there were reasonable grounds for suspecting that the search was necessary for a noninvestigatory work-related purpose") (internal quotations omitted).

[35] MANUAL FOR COURTS-MARTIAL, UNITED STATES (2012) [hereinafter MCM], Military Rule of Evidence (M.R.E.) 313(b).

[36] United States v. Bowersox, 72 M.J. 71, 73 (C.A.A.F. 2013) *cert. denied*, 134 S. Ct. 319 (2013) (internal quotations and citations omitted).

[37] United States v. Campbell, 41 M.J. 177, 181 (C.M.A. 1994) (quoting United States v. Daskam, 31 M.J. 77, 79 (C.M.A. 1990)).

[38] *Bowersox*, 72 M.J. at 76.

[39] MCM, *supra* note 35, M.R.E. 313(a); United States v. Stuckey, 10 M.J. 347, 359–61 (C.M.A. 1981).

[40] United States v. Wicks, 73 M.J. 93, 96–97 (C.A.A.F. 2014).

[41] *Id.* at 98.

[42] *Id.* TSgt Wicks was charged, *inter alia*, with violating general regulations by conducting inappropriate relationships pursuant to Article 92, Uniform Code of Military Justice, 10 U.S.C. § 892 (2012). *Wicks*, 73 M.J. at 95.

[43] *Id.* at 99–100.

[44] *Id.* at 101.

[45] *Id.* at 100 (citing United States v. Jacobsen, 466 U.S. 109, 117 (1984)).

[46] *Id.* at 101.

[47] *Id.*

[48] *Id.*

[49] *Id.* at 99 (quoting United States v. Wurie, 728 F.3d 1, 9 (1st Cir. 2013)).

[50] *Id.* at 98–99.

his personal cell phone and that cell phones are unique for the purposes of Fourth Amendment analysis.

The Fourth Amendment in the Military After *Riley*

Though issued first, the *Wicks* decision is consistent with the Supreme Court's decision in *Riley*. While the CAAF analyzed the privacy doctrine exception to the warrant requirement and the Supreme Court considered the search incident to a lawful arrest exception, both came to the same conclusion: cell phones implicate a unique privacy interest that is protected under the Fourth Amendment.

The major implications of *Riley* are twofold. First, the opinion rejected the application of the Supreme Court's container search jurisprudence to cell phone searches. Instead, the Court affirmed a balancing test and held that test should weigh strongly in favor of an individual's privacy interest when it comes to cell phones. Second, *Riley* introduced an unprecedented perspective on the Fourth Amendment in light of modern technology and set a new standard for courts to apply when considering technological advancements that arise in Fourth Amendment cases.

Container Jurisprudence

Both the Supreme Court and the CAAF rejected a comparison of cell phones to the typical containers (e.g., boxes, cigarette packs, wallets) that have been the subjects of past Fourth Amendment jurisprudence. The Court has approved searches of the inside of a container incident to a lawful arrest on the justification that such containers may contain weapons or evidence.[51] In *United States v. Robinson*, the Court held that the search of the contents of a cigarette pack found on the arrestee's person was a reasonable warrantless search.[52] The Court has also recently upheld searches incident to arrest of passenger compartments in vehicles "when it is reasonable to believe evidence relevant to the crime of the arrest might be found in the vehicle."[53] Therefore, in both *Riley* and *Wicks*, the government argued this jurisprudence should be applied to permit the search of the contents of a cell phone, which might also contain relevant evidence.[54]

The prosecution sought the application of the container comparison because the Fifth and Eleventh Circuit Courts have applied this analysis to cell phones.[55] Each of those courts held that a more thorough search of a closed container is permissible without significantly exceeding the scope of an initial private search.[56] The lower court in *Wicks* was persuaded by this argument; it found that the private search of some of the text messages amounted to a search of a closed container, and the government's search was nothing more than a more thorough search thereof.[57] By analogizing the cell phone to a closed container like a box or compact disk, the lower court upheld the government's more thorough cell phone search.[58]

Both the Supreme Court and the CAAF declined to adopt this view. The CAAF rejected "container metaphors" in *Wicks*: "Because of the vast amount of data that can be stored and accessed, as well as the myriad ways they can be sorted, filed, and protected, it is not good enough to simply analogize a cell phone to a container."[59] For this reason, as well as the private quality of the content a cell phone may access, the information contained in a cell phone "is far more expansive than mere CDs or cardboard boxes."[60]

The Supreme Court rejected the comparison of a cell phone to a container as an "analogy [that] crumbles entirely" in consideration of the fact that the data accessible from a cell phone may actually be stored on remote servers.[61] The cell phone thus "contains" papers and effects beyond the physical proximity of an arrestee.[62] The Court likened the access of this remotely-stored data from a seized cell phone to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[63]

Following *Riley* and *Wicks*, military courts cannot analogize cell phones to containers in justifying cell phone searches. In this way, the Supreme Court's decision implicitly affirms the CAAF's holding in *Wicks* and guts all future arguments the government might make using a container analysis under the private search doctrine or when dealing with a search incident to arrest.

The Fourth Amendment in the Twenty-First Century

The Supreme Court in *Riley* went a step beyond any of its previous Fourth Amendment jurisprudence, and further than the CAAF in *Wicks*, by (1) explaining a modern view of the Fourth Amendment in the context of contemporary

---

[51] *See* United States v. Robinson, 414 U.S. 218, 234 (1973).

[52] *Id.*

[53] Arizona v. Gant, 556 U.S. 343, 335 (2009). *But see* United States v. Chadwick, 433 U.S. 1, 15 (1977 (holding that a 200-pound, locked footlocker could not be searched incident to arrest).

[54] *See* United States v. Robinson, 414 U.S. 218 (1973).

[55] United States v. Runyan, 275 F.3d 449 (5th Cir. 2011); United States v. Simpson, 904 F.2d 607 (11th Cir. 1990).

[56] *Runyan*, 275 F.3d 449; *Simpson*, 904 F.2d 607.

[57] United States v. Wicks, Misc. Dkt. No. 2013-08, 2013 WL 3336737, at *5–7 (A.F. Ct. Crim. App. June 24, 2013) (unpublished) (citing *Runyan*, 275 F.3d at 464).

[58] *Id*.

[59] United States v. Wicks, 73 M.J. 93, 102 (C.A.A.F. 2014).

[60] *Id*.

[61] Riley v. California, 134 S. Ct. 2473, 2491, 189 L. Ed. 2d 430 (2014).

[62] *Cf.* United States v. Robinson, 414 U.S. 218, 256 (1973).

[63] *Riley*, 134 S. Ct. at 2491.

technology, (2) engaging with modern technology, and (3) setting a new standard for courts faced with technically fact-dependent legal issues.

The watershed moment of the Supreme Court's *Riley* decision was the Court's conclusion that the spirit of the Fourth Amendment trumped its literal language in the context of technology not contemplated by the Founders. It acknowledged for the first time that the Founders of the Constitution did not give "precise guidance" on the application of the Fourth Amendment to cell phone searches.[64] In doing so, the Court departed from its reliance on original intent in its recent Fourth Amendment jurisprudence, acknowledging those limitations in the digital age. As recently as 2012, the Court quoted a common law case from 1765 in holding that the "physical intrusion" of attaching a GPS tracking device to petitioner's car "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[65] And in *Florida v. Jardines*, the Court quoted Blackstone's 1769 Commentaries to hold that the curtilege is within the protected area of the home where the government cannot use a drug-sniffing dog.[66] Now, in *Riley*, instead of relying on original definitions and understandings, the Court conjured the broader historical purpose of the amendment. Invoking the principle of freedom from British officers' general searches—the origin of the Constitution's warrant requirement—the Court wrote: "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[67]

Second, the Court demonstrated knowledge and understanding of technological applications of cell phones and technical solutions for law enforcement problems. It mentioned "geofencing," [68] "Faraday bags," [69] "cloud computing,"[70] and "e-mail[ing] warrant requests to judges' iPads." [71] This use of jargon is in stark contrast to the Supreme Court Justices' recent displays of unfamiliarity with the basic technologies of e-mail, text messaging, TV technology, and Facebook. [72] For a Court consistently criticized as Luddite, this opinion was a turning point. To master the listed concepts in *Riley*, at least to the degree of using technical terms accurately in an opinion, demonstrates engagement in modern society in a new and meaningful way.

Third, by mastering the technology and engaging it in analysis of the Fourth Amendment, the Court set a fresh benchmark for both military and civilian courts. The Court clearly expects judges to understand the technical capabilities of cell phones, computers, and digital media at issue in any particular case, as well as the Fourth Amendment repercussions of those capabilities. Legal issues implicated by, for example, location data automatically gathered by an iPhone, wireless connectivity, use of Facebook, or aggregation of metadata must be analyzed in a technically accurate way. Comparisons of modern technology to physical objects considered by courts many decades ago are obsolete and must be rejected as technically and legally inaccurate.

For the military, the applicable Fourth Amendment analysis must also meet the contemporary capabilities of a modern military force. Cell phones provide an easy and transportable personal center of operations, containing all of a Soldier's most personal documents, contacts, and communications, wherever the Soldier goes. *Riley* suggests that the servicemember's strong privacy interest in the contents of a personal cell phone may be greater than the military's law enforcement interest in searching the contents of that cell phone, absent a warrant. In a search incident to a lawful arrest, the police have relatively broad authorities to intrude on protected areas for purposes of seizing weapons and preserving evidence, but even those interests are not sufficient to balance the personal privacy interest at stake with cell phones; likewise, the military has broad authorities to protect and discipline its members, but those interests are not sufficient to search the contents of a cell phone without a judicial determination of probable cause.

The more difficult case concerns the blend between personal and professional. The military provides devices with internet capability to servicemembers for mission purposes, such as government-issued Blackberrys, along with guidelines and agreements concerning how those ought to be used. Often, the guidelines provide no bright-line rule and permit some modicum of personal use provided that it does not interfere with work.[73] Many individuals stretch the rules in practice and conduct much personal business on government devices. On such devices, the servicemember likely has no reasonable expectation of privacy.[74] Even if a

---

[64] *Id.* at 2484.

[65] United States v. Jones, 132 S. Ct. 945, 949 (2012) (quoting Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765)).

[66] 133 S. Ct. 1409 (2013) (quoting 4 W. BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 223, 225 (1769)).

[67] *Riley*, 134 S. Ct. at 2495.

[68] *Id.* at 2486.

[69] *Id.* at 2487.

[70] *Id.* at 2491.

[71] *Id.* at 2493.

[72] *See, e.g.*, Adam Raymond, 8 Times the Supreme Court Was Bewildered by Technology, N.Y. MAG. (Apr. 23, 2014).

[73] *See, e.g.*, United States Office of Government Ethics, *Use of Government Equipment or Property* (noting that it is permitted for an employee to use her government telephone to call to arrange a car repair), http://www.oge.gov/Topics/Use-of-Government-Position-and-Resources/Use-of-Government-Equipment-or-Property/.

[74] *See* United States v. Larson, 66 M.J. 212, 215–16 (C.A.A.F. 2008). (finding that a servicemember did not rebut the presumption where, when the accused used the computer, "a banner appeared that stat[ing] that it was a DOD computer, it [was] for official use, not to be used for illegal activity," and use of the computer required the user to consent to monitoring); *see*

servicemember carefully compartmentalizes his personal and professional use of the cell phone—perhaps, for instance, by using his personal email only in the cell phone browser's "incognito" mode—the courts are likely to reject any sort of container analysis and find there remains no reasonable expectation of privacy in any personal use of the government device.

In the reverse scenario, Soldiers often use their personal cell phones to communicate with other units for military purposes. Such use implicates serious security concerns, but personal privacy interests are at stake too. If the personal cell phone becomes the default work cell phone, an individual's expectation of privacy in it may be reduced: the government's interest in protecting sensitive information could permit a search of otherwise private communications on the personal cell phone. It is therefore in the interests of both national security and personal privacy for servicemembers to distinguish clearly their personal and professional use of government and personal electronic devices.

also City of Ontario, Cal. v. Quon, 560 U.S. 746, 761 (2010) (holding that a city's search of the text message transcripts of an employee's city-issued pager was reasonable because it was for "a noninvestigatory, work-related purpose or for the investigation of work-related misconduct," and "justified at its inception because there were reasonable grounds for suspecting that the search was necessary for a noninvestigatory work-related purpose") (internal quotations omitted).