

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES,
Appellee,

v.

SAMUEL A. WICKS,
Technical Sergeant (E-6), USAF
Appellant.

Crim. App. No. Misc. Dkt. No. 2013-08
USCA Dkt. No. /AF

SUPPLEMENT TO PETITION FOR GRANT OF REVIEW

JA RAI A. WILLIAMS, Major, USAF
Appellate Defense Counsel
USCAAF Bar No. 33615
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd, Ste 1100
Joint Base Andrews NAF, MD 20762
(240) 612-4770
jarai.williams@pentagon.af.mil

CHRISTOPHER D. JAMES, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 34081
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Road, Suite 1100
Joint Base Andrews, MD 20762
(240) 612-4770
Christopher.James@pentagon.af.mil

Counsel for Appellant

TABLE OF CONTENTS

Table of Authorities.....ii
Issue Presented.....1
Statement of Statutory Jurisdiction.....2
Statement of the Case.....2
Statement of Facts.....3
Summary of the Argument.....11

Argument

**THE AIR FORCE COURT OF CRIMINAL APPEALS ERRED BY FINDING LAW
ENFORCEMENT’S REPEATED WARRANTLESS SEARCHES OF APPELLANT’S
IPHONE DID NOT VIOLATE THE FOURTH AMENDMENT.....12**

Appendices:

United States v. Wicks, Misc. Dkt. No. 2013-08 (A.F. Ct. Crim.
App. 24 June 2013) (unpub. op.).

United States v. Wurie,
--- F.3d ---, No. 11-1792 (1st Cir. 2013)

TABLE OF AUTHORITIES

	Page(s)
CASES	
<i>United States v. Cote</i> , 72 M.J. 41 (C.A.A.F. 2013)	16
<i>United States v. Daniels</i> , 60 M.J. 69 (C.A.A.F. 2004)	15, 16
<i>United States v. Donnes</i> , 947 F.2d 1430 (10th Cir. 1991)	20
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984)	13
<i>United States v. Kinney</i> , 953 F.2d 863 (4th Cir. 1992)	20
<i>United States v. Lopez de Victoria</i> , 66 M.J. 67 (C.A.A.F. 2008)	1
<i>United States v. Rodriguez</i> , 60 M.J. 239 (C.A.A.F. 2004)	12
<i>United States v. Rouse</i> , 148 F.3d 1040 (8th Cir. 1998)	20
<i>United States v. Runyan</i> , 275 F.3d 449 (5th Cir. 2001)	16, 17, 20
<i>United States v. Simpson</i> , 904 F.2d 607 (11th Cir. 1990)	16, 20
<i>United States v. Taylor</i> , 41 M.J. 168 (C.M.A. 1994)	15
<i>United States v. Wurie</i> , --- F.3d ---, No. 11-1792 (1st Cir. 2013)	17, 18, 19
<i>Walter v. United States</i> , 447 U.S. 649 (1980)	13
STATUTES	
Article 31, UCMJ.....	9, 11
Article 36(a), UCMJ.....	15

Article 67, UCMJ.....1
Article 92, UCMJ.....2
Article 120, UCMJ.....2
Article 134, UCMJ.....2
Article 62, UCMJ.....1, 3

OTHER AUTHORITIES

U.S. Const. art. I, § 8, cl. 14.....15
Military Rules of Evidence 311(a).....15, 16

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES,)	SUPPLEMENT TO PETITION
<i>Appellee,</i>)	FOR GRANT OF REVIEW
v.)	
)	USCA Dkt. No. /AF
Technical Sergeant (E-6))	
SAMUEL A. WICKS,)	Crim. App. No. 2013-08
USAF,)	
<i>Appellant.</i>)	

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

Introduction

COMES NOW Appellant, Technical Sergeant Samuel A. Wicks, by and through his undersigned counsel, and pursuant to Rule 21 of this Honorable Court's Rules of Practice and Procedure submits this supplement to his petition for grant of review.

Issue Presented

WHETHER THE AIR FORCE COURT OF CRIMINAL APPEALS ERRED BY FINDING LAW ENFORCEMENT'S REPEATED WARRANTLESS SEARCHES OF APPELLANT'S IPHONE DID NOT VIOLATE THE FOURTH AMENDMENT.

Statement of Statutory Jurisdiction

The Air Force Court of Criminal Appeals (AFCCA) reviewed this case pursuant to Article 62, Uniform Code of Military Justice (UCMJ). Appellant filed a timely petition for grant of review, bringing this case within this Court's statutory jurisdiction under Article 67, UCMJ. See *United States v. Lopez de Victoria*, 66 M.J. 67 (C.A.A.F. 2008).

Statement of the Case

On 19 December 2012, charges were referred against Appellant. (Charge Sheet, R. at 19.1-19.3). The charges consisted of: three specifications of violating Article 92, UCMJ (violating lawful general regulation); one specification of violating Article 120, UCMJ (committing indecent conduct); and one specification of violating Article 134, UCMJ (impeding an investigation). *Id.*

On 5 February 2013, trial defense counsel filed a motion to suppress the evidence obtained in Appellant's cell phone (an iPhone) and any derivative evidence of that search. (App. Ex. X). On 19 February 2013, the military judge conducted a preliminary hearing with respect to the motion to suppress. (R. at 112). On 20 February 2013, the military judge granted the defense motion and suppressed the evidence from the cell phone analysis and all derivative evidence. (App. Ex. XXXIII). That same day, the military judge granted trial counsel's request to reconsider his ruling. (R. at 227). After considering additional testimony, the military judge provided findings on the record, upholding his earlier ruling to suppress the evidence. (R. at 289-97). In addition, the military judge supplemented his ruling with written findings. (App. Ex. XL).

On 21 February 2013, the government filed its notice of appeal. (App. Ex. XLI).

On 24 June 2013, AFCCA granted the government's appeal under Article 62 and vacated the ruling of the military judge. *United States v. Wicks*, Misc. Dkt. No. 2013-08 (A.F. Ct. Crim. App. 24 June 2013) (unpub. op.) [Appendix A].

Statement of Facts

Appellant is a military training instructor (MTI) assigned to Joint Base San Antonio (JBSA)-Lackland, TX. (R. at 64). Appellant and TSgt Ronda Roberts, also an MTI assigned to JBSA-Lackland, were involved in a personal relationship. (R. at 64). In November 2010, while Appellant was at TSgt Roberts' residence, TSgt Roberts viewed some text messages on Appellant's cell phone, an iPhone, without his permission. (R. at 65, 96). The following month, Appellant and TSgt Roberts ended their personal relationship. (R. at 66).

In May 2011, TSgt Roberts took Appellant's cell phone, without his permission, from the "CQ" desk at Appellant's place of duty. (R. at 67, 96). TSgt Roberts again examined some text messages on Appellant's cell phone. (R. at 69). TSgt Roberts saw text messages between Appellant and a few women whom she believed to be trainees. (R. at 69, 96-97). TSgt Roberts believed these women to be trainees because she recognized the partial names associated with the text messages—specifically "D.W." and "B"—as well as photographs of these women attached to the text messages. (R. at 69). TSgt Roberts also saw a

sexually explicit video sent to an unknown person who she believed to be a trainee via text message. (R. at 69). The same day that TSgt Roberts took Appellant's cell phone, her supervisor asked if she had seen the phone. (R. at 67-68, 101-02). Appellant also asked her the same question. (R. at 68, 101-02). TSgt Roberts lied and told both of them "no." (R. at 68). TSgt Roberts did not believe either her supervisor or Appellant suspected her of stealing the cell phone. (R. at 205). Appellant later sent an e-mail to members of his squadron inquiring about his missing cell phone. (App. Ex. XXVI).

Shortly after stealing Appellant's cell phone, TSgt Roberts went on leave. (R. at 70, 102, 203). Upon returning from leave, TSgt Roberts claimed that she confronted Appellant with what she saw his cell phone without mentioning the cell phone or the fact that she stole the cell phone. (R. at 70, 102, 202-03). According to TSgt Roberts, Appellant acknowledged sending the text messages and told TSgt Roberts to get out of his face. (R. at 70, 102, 202-03).

Eight months after TSgt Roberts took Appellant's cell phone, Detective Arlene Rico, Security Forces Office of Investigations (SFOI), interviewed TSgt Roberts. (R. at 87-88, 122). The interview was the result of TSgt Roberts making contact with SFOI through her first sergeant and in response to a general inquiry about whether any personnel had information

about possible MTI misconduct. (R. at 87-88, 122, 127). Prior to this interview, SFOI did not suspect Appellant of engaging in any MTI misconduct. (R. at 123).

During the interview, TSgt Roberts told Detective Rico the partial names ("D.W." and "B") of the women she believed to be trainees and the video sent to an unknown woman. (R. at 122, 138). TSgt Roberts also told Detective Rico she could provide "evidence." (R. at 73, 123). After interviewing TSgt Roberts, Detective Rico consulted with personnel from the advising legal office. (R. at 141). She purportedly secured flight rosters from the past five years for trainees assigned to the 331st Training Squadron (331 TRS) containing the last names, "W," "S," and "B." (R. at 256-57, 266, 269). However, she did not learn of "S" until after she received the cell phone from TSgt Roberts and reviewed the text messages. (R. at 256-57, 266, 269).

TSgt Roberts could not find Appellant's cell phone, as she moved between the time she took his cell phone and Detective Rico's interview. (R. at 73, 90-91). TSgt Roberts said she told Detective Rico that she could not find Appellant's cell phone. (R. at 98). Detective Rico said TSgt Roberts never told her. (R. at 124). TSgt Roberts eventually located the SIM card from Appellant's cell phone and provided it to Detective Rico. (R. at 73, 123). TSgt Roberts maintained she told Detective Rico that it was from Appellant's cell phone. (R. at 98).

Detective Rico testified TSgt Roberts told her it belonged to someone else but contained Appellant's cell phone information.¹ (R. at 129).

After receiving Appellant's SIM card, Detective Rico again consulted the legal office and sent it to the Bexar County Sheriff's Office for analysis. (R. at 141-42, 123). She learned that no information could be obtained from the card. (R. at 123). So at Detective Rico's urging, TSgt Roberts found Appellant's cell phone and provided it to Detective Rico. (R. at 90, 124). According to Detective Rico, TSgt Roberts told her the cell phone belonged to another person and contained information from Appellant's cell phone. (R. at 124-26). Detective Rico did not complete paperwork to indicate that TSgt Roberts (or anyone else) consented to a search of the cell phone. (R. at 131, 145).

After TSgt Roberts provided her with the cell phone, Detective Rico reviewed all of his text messages by "scrolling" through the phone "until something caught [her] attention." (R. at 267). TSgt Roberts was not there when Detective Rico randomly scrolled through the text messages and did not show Detective Rico the specific messages she reviewed. (R. at 99, 147). Then Detective Rico, for a third time, consulted the

¹ TSgt Roberts told Detective Rico that she downloaded the information from his cell phone to a computer and saved it in an iTunes account. (R. at 129).

legal office. (R. at 131, 133-34). During this third consultation, Detective Rico informed the legal office that there was a lot of information on the cell phone. (R. at 147). Detective Rico left the office with the impression that the legal office believed the information on the cell phone to be "really important" and that she was to obtain that information. (R. at 131). No one discussed the need for a search authorization. (R. at 131, 133-34). Moreover, Detective Rico would not have secured a search authorization because, at the time this conduct occurred, it was not her practice to do so. (R. at 131-32, 136).

Subsequently, Detective Rico provided Appellant's cell phone to the same civilian police agency for an extraction of all information from the phone. (R. at 124, 134, 163). Detective Mike Allen, the civilian investigator who conducted the extraction, believed the examination of the phone was being conducted pursuant to a grant of consent. (R. at 160-61, App. Ex. XXV). Detective Allen conducted the examination and provided the results to SFOI. (R. at 163-64, 125). The information Detective Rico received from Detective Allen's analysis showed that Appellant's information was the only data located on the phone. (R. at 136). Consequently, according to Detective Rico, she felt uncomfortable with the steps taken. (R. at 136). However, SFOI sent the cell phone to Global

Compusearch for further analysis. (R. at 125).

Senior Airman (SrA) L.B. attended basic military training (BMT) from December 2010 until February 2011. (R. at 113). She then attended technical training at various locations for approximately 19 months. (R. at 113). Appellant was SrA L.B.'s BMT instructor. (R. at 113). She maintained contact with Appellant for about two months after graduation. (R. at 114). It was after this time that SrA L.B. stated Appellant called her to tell her a co-worker took his cell phone and to tell anyone who may question her that she had no contact with him after she graduated from BMT. (R. at 114). Nine months later, Detective Rico interviewed her. (R. at 115).

During the interview, Detective Rico had a stack of documents which contained the text messaged communications between Appellant and SrA L.B. (R. at 140). The documents were the product of the extraction of the cell phone. *Id.* Detective Rico stated she did not believe that she showed the texts to SrA L.B. but she referred to them. *Id.* SrA L.B. stated Detective Rico showed her copies of the text messages. (R. at 118). SrA L.B. confirmed everything Detective Rico already knew from the text messages. (R. at 116, 117). Prior to this interview, SrA L.B. did not receive any solicitations to provide information about misconduct that occurred while she was at BMT. (R. at 118). Furthermore, she did not and was not planning to initiate

contact with anyone about her interactions with Appellant. (R. at 119).

Detective Rico used the results of the cell phone extraction to conduct her investigation. (R. at 125).

Detective Rico agreed that the results of her investigation and the charged offenses were primarily from what she learned from TSgt Roberts and her analysis of Appellant's cell phone. (R. at 128).

Eight months after she interviewed SrA L.B., Detective Rico advised TSgt Roberts of her Article 31, UCMJ rights for stealing Appellant's cell phone. (R. at 103, 132). She did this at the legal office's recommendation. (R. at 132).

In addition to these facts, Appellant offers the following timeline:

- **November 2010:** TSgt Roberts observed the text messages on Appellant's cell phone without Appellant's consent. (R. at 65, 96).
- **December 2010:** TSgt Roberts and Appellant ended their personal relationship. (R. at 66).
- **May 2011:** TSgt Roberts took Appellant's cell phone from a desk while at work. That same day both her supervisor and Appellant asked her if she saw Appellant's cell phone. She denied seeing Appellant's cell phone. Appellant sent e-mails and questions to others in his unit in search of his cell phone. (R. at 67-68, 96, 101-02, App. Ex. XXVI).
- **May or June 2011:** TSgt Roberts confronted Appellant about him sending text messages to "W" and "B." She said Appellant admitted to sending them. (R. at 70, 102, 202-03).

- **May or June 2011:** According to SrA L.B., Appellant called her and told her not to say anything about their prior communications. (R. at 114).
- **10 January 2012:** Detective Rico interviewed TSgt Roberts after TSgt Roberts made contact with the Security Forces Office of Investigations through the first sergeant. TSgt Roberts told Detective Rico about her observations of Appellant's cell phone. She told her that she had the information from the phone. There were discrepancies regarding in what form TSgt Roberts told Detective Rico she had the information. (R. at 71-72, 87-88, 98, 122-24, 138).
- **10 or 11 January 2012:** Detective Rico consulted the legal office. (R. at 141).
- **11 January 2012:** TSgt Roberts provided a SIM card from Appellant's cell phone to Detective Rico. Detective Rico believed the SIM card belonged to someone else but had the contents Appellant's cell phone contents downloaded to the card. (R. at 73, 123, 129).
- **11 or 12 January 2012:** Detective Rico consulted the legal office a second time. (R. at 141-42).
- **11 or 12 January 2012:** Detective Rico sent the SIM card to a civilian police agency for an analysis, but no information could be found on the card. (R. at 123, 141-42).
- **12 January 2012:** Detective Rico purportedly obtained flight rosters for the previous five years for trainees assigned to 331 TRS with the last names starting with "W," "S," and "B." (R. at 252, 256, 257, 266, 269).
- **17 January 2012:** TSgt Roberts provided Appellant's cell phone to Detective Rico. Detective Rico believed the cell phone belonged to someone else but had the contents of Appellant's cell phone downloaded to the phone. (R. at 124-26).
- **17 or 18 January 2012:** Detective Rico reviewed random text messages on the cell phone and consulted with personnel from the legal office for a third time, stating there was a lot of information on the cell phone. The legal office left Detective Rico with the impression that it was really important to get the information. Detective Rico then sent

off the cell phone to a civilian police agency for an extraction of all of the information on the cell phone. (R. at 99, 124, 131, 133-34, 147-48, 267).

- **18 January 2012:** The civilian police agency extracted the contents of phone. (R. at 124, 163-64, App. Ex. XXV).
- **12 March 2012:** After reviewing the information the civilian police agency extracted, Detective Rico interviewed SrA L.B., specifically using that extracted information during the interview. (R. at 116-18, 125, 128, 140).
- **28 March 2012:** Appellant's cell phone was shipped to Global Compusearch, a computer forensics company. (R. at 125, 228).
- **November 2012:** Detective Rico advised TSgt Roberts of her rights pursuant to Article 31, UCMJ. (R. at 103, 132).
- **20 February 2013:** At the request of trial counsel, an employee of Global Compusearch conducted an examination of Appellant's cell phone. The employee searched 45,000-60,000 text messages for three particular phone numbers. Trial counsel used the results of the examination to argue the motion for reconsideration of the military judge's ruling to suppress evidence. (R. at 227, 245, 247, 292).

Why There is Good Cause to Grant the Petition

Relying on Fifth and Eleventh Circuit jurisprudence, AFCCA incorrectly decided Appellant's case. In doing so, it overlooked case law from other circuits in direct conflict with the case law it cited. This is a question of law which has not been, but should be settled by this Honorable Court. AFCCA's reliance on these two circuits despite a lack of consensus among the circuit courts regarding the scope of a private search warrant this Honorable Court's review.

The Military Judge Did Not Err

The military judge found that Appellant's Fourth Amendment rights were violated when: (1) Detective Rico's warrantless search exceeded TSgt Roberts' private search; (2) the civilian police agency conducted a full extraction of all of the contents on Appellant's iPhone without a search authorization; and (3) Global Compusearch further analyzed the 45,000-60,000 text messages on Appellant's iPhone without a search authorization. (R. at 220; App. Ex. XXXIII, para. 39; App. Ex. XL, paras. 40, 56, 58, 59). A military judge abuses his discretion "on a motion to suppress if factual findings are clearly erroneous or if the law is applied erroneously." *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004). The military judge did not err.

A. Detective Rico unlawfully expanded the scope of the private search

The Government failed to prove that Detective Rico relied on TSgt Roberts' private search when she reviewed Appellee's text messages. Instead, the evidence shows Detective Rico randomly perused Appellee's text messages and enlisted the aid of a civilian investigator and a private company to engage in an expansive search of all of Appellee's private information on the cell phone – without proper authorization to do so – therefore unlawfully expanding the scope of the private search. Without a search authorization, Detective Rico was permitted to conduct

the same specific search that TSgt Roberts did. "The additional invasions of [Appellee's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *United States v. Jacobsen*, 466 U.S. 109, 116 (1984); see also *Walter v. United States*, 447 U.S. 649, 657 (1980). Continuing with that logic, the Supreme Court held, the logic follows "[i]f a properly authorized official search is limited by the particular terms of its authorization, at least the same kind of strict limitation must be applied to any official use of another person's privacy." *Walter*, 447 U.S. at 657.

Detective Rico randomly and generally scrolled through Appellee's numerous text messages searching for and finding more information than TSgt Roberts provided to her. (R. at 267). Because Detective Rico's search of Appellee's cell phone went beyond the scope of the private search, it infringed Appellee's legitimate expectation of privacy and was a search within the meaning of the Fourth Amendment. Moreover, the extraction of *all* of the contents of the cell phone further violated Appellee's Fourth Amendment privacy rights.

B. The excluded evidence would not have been inevitably discovered

The Government had not met its burden of proving by a preponderance of the evidence that the information revealed by

the numerous, unlimited searches of Appellee's cell phone would have been inevitably discovered by a lawful manner. Even after consulting the servicing legal office, Detective Rico made no effort to secure a warrant though probable cause existed to search the text messages on the cell phone.

Moreover, Detective Rico testified that she would not have secured a search authorization because, at the time this conduct occurred, it was not her practice to do so. (R. at 131-32, 136). Even if the government could have sought a probable cause search authorization, it cannot in hindsight say it would have discovered the excluded evidence if it had sought a search authorization since Detective Rico's testimony directly contradicts this proposition.

The independent source doctrine also does not apply. The only "independent information" the Government had about SrA L.B. was her last name and the fact that Appellee may have communicated with her via text message. Other information received by SrA L.B. - i.e. the telephone call from Appellant that took place after his phone was stolen - was through the use of the text messages, which was the result of the illegal search. In fact, Detective Rico admitted that the results of her investigation and the charged offenses were primarily from what she learned from TSgt Roberts and her analysis of Appellee's cell phone. (R. at 125, 128). The military judge

concluded “[b]ut for the illegal actions by the Government in conducting multiple warrantless, general searches of the phone containing the accused’s personal information, she would not have been interviewed or confronted with the text messages by Detective Rico about her relationship with the accused.” (App. Ex. XL, para. 60). Thus, there was no independent source of the evidence relied on by the Government.

C. Military Rule of Evidence (M.R.E.) 311(a) required exclusion of the evidence

M.R.E. 311(a) provides, “Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against the accused[.]” “Under the Military Rules of Evidence, which implement the Fourth Amendment, evidence illegally seized by government agents from a protected place is inadmissible.” *United States v. Daniels*, 60 M.J. 69, 70 (C.A.A.F. 2004) (quoting *United States v. Hester*, 47 M.J. 461, 463 (C.A.A.F. 1997)); see also M.R.E. 311(a), UCMJ. Thus, M.R.E. 311(a) requires exclusion since the search violated the Fourth Amendment. The President adopted M.R.E. 311(a) pursuant to his power under Article 36(a), UCMJ. *United States v. Taylor*, 41 M.J. 168, 170 (C.M.A. 1994). Article 36(a) is a congressional delegation of its constitutional authority. U.S. Const. art. I, § 8, cl. 14.

Whatever the limits of the application of the exclusionary rule are in a civilian criminal court, M.R.E. 311(a) requires its application in a military court. See *Daniels*, 60 M.J. at 72-73 (finding because a warrantless search was unlawful the military judge erred in receiving the results from that search into evidence at trial); see also *United States v. Cote*, 72 M.J. 41, 46 (C.A.A.F. 2013) (finding that the military judge did not abuse her discretion in suppressing evidence obtained from an unreasonable search). Thus, the error of allowing such unlawful evidence to be used against Appellant at his court-martial materially prejudices his substantial, constitutional rights.

AFCCA Erred

AFCCA found error with the military judge's conclusions of law. *Wicks*, slip op. at 5-6. In finding error, however, AFCCA acknowledged there were no military cases addressing the specific question of "whether law enforcement officials are limited to only examining the files inspected by the private party or whether all data . . . on the electronic device is within the scope of the initial private search and thus can be obtained by law enforcement." *Wicks*, slip op. at 6.

Consequently, AFCCA relied on *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001) and *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990). AFCCA's reliance on *Runyan* is misplaced. In *Runyan*, the Fifth Circuit acknowledged the "lack

of consensus among [its] sister circuits" regarding Appellant's issue. *Runyan*, 275 F.3d at 461.

Likening Detective Rico's search of the text messages on Appellant's iPhone to that of a closed container search, AFCCA held the military judge incorrectly interpreted the law when he found that Detective Rico's search had to exactly mirror TSgt Roberts's search in order to be lawful. In addition, AFCCA found that the further extraction by the civilian law enforcement agency **of all of the data** located on Appellant's iPhone as well as the **45,000-60,000** text messages extracted by Global Compusearch was not an unconstitutional expansion on the original private search. *Wicks*, slip op. at 8 (emphasis added).

In *Runyan*, the Fifth Circuit compared the floppy discs containing images of child pornography to that of a closed container used to conceal its contents from plain view. *Runyan*, F.3d at 458. The discs at issue in *Runyan* were closed containers; Appellant's iPhone is a computer. In *United States v. Wurie*, --- F.3d ---, No. 11-1792 (1st Cir. 2013) [Appendix B], the First Circuit examined the question of whether the police, after seizing a cell phone from an individual's person as part of his lawful arrest, can search the phone's data without a warrant. *Wurie*, slip op. at 1. The First Circuit rejected the argument that appellant's cell phone was "indistinguishable from other kinds of personal possessions . . .

. that fall within the search incident to arrest exception to the Fourth Amendment's warrant requirement." *Id.* at 6. The First Circuit stated:

In reality, "a modern cell phone is a computer," and "a computer ... is not just another purse or address book." *Flores-Lopez*, 670 F.3d at 805. The storage capacity of today's cell phones is immense. Apple's iPhone 5 comes with up to sixty-four gigabytes of storage, see Apple, iPhone, Tech Specs, <http://www.apple.com/iphone/specs.html> (last visited May 16, 2013), which is enough to hold about "four million pages of Microsoft Word documents," Charles E. MacLean, *But, Your Honor, a Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L.Rev. 37, 42 (2012). That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records. See *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir.2013) (en banc) ("The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities."). It is the kind of information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest. See *Chimel*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685. Indeed, modern cell phones provide direct access to the home in a more literal way as

well; iPhones can now connect their owners directly to a home computer's webcam, via an application called iCam, so that users can monitor the inside of their homes remotely. Flores-Lopez, 670 F.3d at 806. "At the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though a house contains data." *Id.* In short, individuals today 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 that the government has invoked. See *id.* at 805 (rejecting the idea that a cell phone can be compared to other items carried on the person, because today's cell phones are "quite likely to contain, or provide ready access to, a vast body of personal data").

Wurie, slip op. at 6-7.

However, even if AFCCA properly treated Appellant's iPhone like a closed container, the Fifth Circuit concluded that the police's further examination of the discs exceeded the scope of the private search:

[T]he police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise. This guideline is sensible because it preserves the competing objectives underlying the Fourth Amendment's protections against warrantless police searches. A defendant's

expectation of privacy with respect to a container unopened by the private searchers is preserved unless the defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search. Moreover, this rule discourages police from going on "fishing expeditions" by opening closed containers. *Any evidence that police obtain from a closed container that was unopened by prior private searchers will be suppressed unless they can demonstrate to a reviewing court that an exception to the exclusionary rule is warranted because they were substantially certain of the contents of the container before they opened it.*

Runyan, 275 F.3d at 463-64 (emphasis added).

Moreover, AFCCA appeared to have relied on both *Runyan* and *Simpson* for the position that "the police do not exceed the scope of a private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties." *Runyan* 275 F.3d at 464; see also *Simpson*, 904 F.2d at 610.

However, several other circuits have indicated that police exceed the scope of a private search when they examine objects or containers that the private searchers did not examine. See *United States v. Rouse*, 148 F.3d 1040, 1041 (8th Cir. 1998); *United States v. Kinney*, 953 F.2d 863, 866 (4th Cir. 1992); *United States v. Donnes*, 947 F.2d 1430, 1434 (10th Cir. 1991).

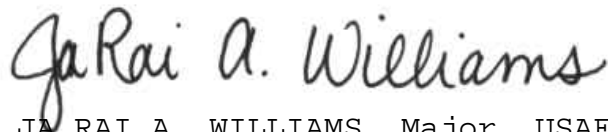
Thus, AFCCA's reliance on these two circuits despite the lack of consensus among the circuit courts requires this

Honorable Court's review of the matter. In addition, AFCCA's error in comparing an iPhone to a closed container instead of a computer can establish bad precedent for military justice practice if this Honorable Court decides against granting this petition.

Conclusion

WHEREFORE, Appellant requests this Honorable Court grant review of this issue.

Respectfully submitted,



JARAI A. WILLIAMS, Major, USAF
Appellate Defense Counsel
USCAAF Bar No. 33615
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Rd, Ste 1100
Joint Base Andrews NAF, MD 20762
(240) 612-4770
jarai.williams@pentagon.af.mil



CHRISTOPHER D. JAMES, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 34081
Air Force Legal Operations Agency
United States Air Force
1500 W. Perimeter Road, Suite 1100
Joint Base Andrews, MD 20762
(240) 612-4770
Christopher.James@pentagon.af.mil

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing was electronically mailed to the Court and to the Director, Air Force Government Trial and Appellate Counsel Division, on 26 June 2013.

A handwritten signature in cursive script, appearing to read "Christopher D. James".

CHRISTOPHER D. JAMES, Capt, USAF
Appellate Defense Counsel
CAAF Bar No. 34081
Appellate Defense Division
1500 W. Perimeter Road, Suite 1100
Joint Base Andrews NAF, MD 20762
(240) 612-4770
christopher.james@pentagon.af.mil

Appendix A

UNITED STATES AIR FORCE COURT OF CRIMINAL APPEALS

UNITED STATES,)	Misc. Dkt. No. 2013-08
Appellant)	
)	
v.)	
)	ORDER
Technical Sergeant (E-6))	
SAMUEL A. WICKS,)	
USAF,)	
Appellee)	Special Panel

Pursuant to Rule 21 of this Court’s Rules of Practice and Procedure, an Appeal Under Article 62, UCMJ, 10 U.S.C. § 862, was filed with this Court by counsel for the United States on the 13th day of March, 2013.

Background

The appellee is charged with: violating a lawful general regulation by wrongfully attempting to develop and conduct personal and/or sexual relationships with three female airmen while they were trainees and he was a military training instructor (MTI) at Lackland Air Force Base between 2010 and 2011; engaging in indecent conduct with one of those trainees by sending her a sexually explicit video-recording; and obstructing justice by telling one of the trainees to lie to investigators about her personal contact with the appellee.

At a pretrial session, the military judge suppressed all evidence found during an analysis of the appellee’s cellular phone as well as all derivative evidence. The military judge further held the Government had failed to satisfy its burden of showing that the evidence would have been inevitably discovered. After the military judge denied a Government request for reconsideration, the Government appealed the military judge’s ruling pursuant to Article 62, UCMJ.

Jurisdiction and Standard of Review

“Prosecution appeals are disfavored and are permitted only upon specific statutory authorization.” *United States v. Bradford*, 68 M.J. 371, 372 (C.A.A.F. 2010) (citing *United States v. Wuterich*, 67 M.J. 63, 70 (C.A.A.F. 2008)). The statute at issue in the present appeal authorizes the Government to appeal “[a]n order or ruling which excludes evidence that is substantial proof of a fact material in the proceeding,” in a court-martial

where a punitive discharge may be adjudged. Article 62(a)(1)(B), UCMJ; Rule for Courts-Martial (R.C.M.) 908(a) and (b).

We review a military judge's ruling on a motion to exclude evidence for an abuse of discretion. *Wuterich*, 67 M.J. at 77 (citation omitted). We review findings of fact under the clearly erroneous standard and conclusions of law de novo. *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004). In contrast to our powers of review under Article 66(c), UCMJ, 10 U.S.C. § 866, in ruling on Government appeals under Article 62, UCMJ, this Court "may act only with respect to matters of law." Article 62(b), UCMJ; R.C.M. 908(c)(2). We cannot find our own facts in addition to or contrary to the facts found by the military judge, nor can we substitute our interpretation of his facts. *United States v. Baker*, 70 M.J. 283, 287 (C.A.A.F. 2011); *United States v. Cossio*, 64 M.J. 254, 256 (C.A.A.F. 2007); *United States v. Pacheo*, 36 M.J. 530, 533 (A.F.C.M.R. 1992); *United States v. Terry*, 66 M.J. 514, 517 (A.F. Ct. Crim. App. 2008). When reviewing a ruling on a motion to exclude evidence, "we consider the evidence in the light most favorable to the prevailing party." *Id.* at 288 (quoting *United States v. Cowgill*, 68 M.J. 388, 390 (C.A.A.F. 2011) (quoting *United States v. Reister*, 44 M.J. 409, 415 (C.A.A.F. 1996))).

Facts

The appellee was a military training instructor (MTI) at Joint Base Lackland, Texas, whose duties included instructing new recruits during basic training. At one point, he developed a personal relationship with TSgt Roberts, a fellow MTI at Lackland. In November of 2010, while the two were at the appellee's house, TSgt Roberts began to look at text messages on the appellee's smart phone (phone) while he was asleep. The military judge did not make findings of fact about what TSgt Roberts specifically observed during that viewing. By early December 2010, TSgt Roberts and the appellee were no longer involved in a personal relationship.

In May 2011, the appellee left his phone on a desk in his duty station. Unbeknownst to the appellee, TSgt Roberts took the phone and looked at several text messages that suggested he had been in contact with former female trainees. She also saw pictures of several women who she recognized as prior trainees in the squadron, as well as a video recording of a male (who she believed to be the appellee) masturbating. TSgt Roberts kept the phone at her home and lied to the appellee when he asked if she knew where it was.

Approximately three weeks later, TSgt Roberts confronted the appellee about the information she had seen on his phone. He acknowledged sending the text messages and told TSgt Roberts to "get out of his face." The two parted company without any discussion about the whereabouts of the phone.

In the May-June 2011 time frame, the appellee contacted SrA LB and told her a co-worker had taken his phone and there might be an investigation. The appellee was SrA LB's MTI during basic training between December 2010 and February 2011 and the two had stayed in contact until April 2011. He told her not to worry and, if asked, to say she and the appellee had no contact after she graduated from basic training. Her impression was that the appellee was a little worried when he talked to her and was encouraging her not to say anything.¹

In January 2012, Detective AR, a Security Forces investigator, contacted TSgt Roberts concerning an ongoing investigation into MTI misconduct at Lackland. At the time of this meeting, the appellee was not suspected of wrongdoing. During the interview, TSgt Roberts told the detective that she had seen text messages on the appellee's phone that she believed was evidence of misconduct. TSgt Roberts told Detective AR that she had downloaded the contents of the appellee's phone onto her iTunes account while he was asleep. She also provided Detective AR with the last names of two prior trainees (SrA LB and A1C SW).² During the interview, TSgt Roberts told Detective AR that she had confronted the appellee about the information she discovered on the phone and that the appellee acknowledged having sent the text messages.

The next day, TSgt Roberts gave Detective AR the SIM card from the appellee's phone, but did not inform her of how she obtained the card. Although Detective AR did not know TSgt Roberts had stolen the phone and SIM card, she believed that the data belonged to the appellee and had been taken from him without his consent or knowledge. Detective AR spoke to the base legal office, but did not request a search authorization to review the contents of the phone. The SIM card was subsequently analyzed but no information was found.

On 17 January 2012, TSgt Roberts brought the appellee's phone to Detective AR. TSgt Roberts lied to the detective, saying it belonged to a third person. After TSgt Roberts left, Detective AR turned on the cell phone and reviewed an indeterminate number of text messages. When she did the search, Detective AR was unaware of specifically what text messages TSgt Roberts had previously seen.

The military judge found that Detective AR "did not mirror the actions" taken by TSgt Roberts and instead engaged in a "general search" of the phone. The detective testified that there were so many texts in the phone that she reviewed and scrolled through them until something caught her attention. She did not make copies of the messages she reviewed nor take notes about what she saw as she anticipated a full analysis and extraction of the phone would be conducted. During this initial review, Detective AR recalled seeing a text referencing an airman's name (Amn KS) and,

¹ Charges were referred, alleging the appellee had an improper relationship with SrA LB and also obstructed justice through this communication.

² Although charges were preferred involving A1C SW, they were not referred to trial.

through a review of flight rosters, determined the appellee had been the MTI for an airman by that name. She also saw a picture of a female airman dressed partially in a military uniform.³

Based on this review, Detective AR was able to corroborate some of the information provided by TSgt Roberts. She again spoke with the legal office for guidance and was told to get the information from the phone. There appears to have been no discussion concerning a need to obtain a search authorization before analyzing the phone's contents. The phone was sent to the Bexar County Sherriff's Office for forensic analysis. After reviewing the results, Detective AR realized the appellee was the only person whose information was on the phone (up to this point, TSgt Roberts had maintained that the phone belonged to someone other than the appellee).

On 28 March 2012, the phone was shipped to a commercial company for examination. An analyst searched the 45,000 text messages on the phone for texts involving three particular phone numbers and created a report. The information in his report reflected texts that would have been viewable by both TSgt Roberts and Detective AR and a small number that would not have been accessible as they were "deleted" items.⁴

Based on information contained within the texts, Detective AR spoke with Amn KS who said that SrA LB and the appellee had been involved in some type of personal relationship. In March 2012, Detective AR interviewed SrA LB in person. Detective AR brought the texts to the interview but did not show them to SrA LB. Rather, the detective referred to the text messages and SrA LB confirmed the information contained in the messages. SrA LB's perspective was that the investigators already had all the information and only sought her confirmation of the matters. Prior to that time, SrA LB had not reported any interactions with the appellee.

Military Judge's Conclusions of Law

The military judge concluded that TSgt Roberts was acting in her private capacity when she searched the appellee's phone in November 2010 and in seizing and searching the phone in May 2011. Accordingly, the military judge concluded TSgt Roberts' actions did not violate the appellee's Fourth Amendment⁵ rights, citing to *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (holding the Fourth Amendment is "wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private

³ Detective AR testified that, in the absence of any other information, once she became aware of the names of the three women (two of which were provided to her by TSgt Roberts based on her review of the phone and one of which she learned through her own review of the phone), her normal course of business would be to either call the women or send them a questionnaire asking about their knowledge of MTI misconduct. Based on their responses, Detective AR would have then decided whether to interview the women in person.

⁴ These phone numbers belonged to SrA LB (whose name had originally been provided to Detective AR by TSgt Roberts in her 10 January 2012 interview), and two other female airmen, AIC LR and SrA KR.

⁵ U.S. CONST. amend. IV.

individual not acting as an agent of the Government or with the participation or knowledge of any governmental official” (citations omitted)).

However, relying on *Jacobsen* and *Walter v. United States*, 447 U.S. 649 (1980), the military judge held, that “to the extent [the detective] exceeded the scope of TSgt Roberts’s review,” it was in violation of the Fourth Amendment as she was permitted under the law to “go only as far as th[at] private search.” The military judge considered the “scope” of TSgt Roberts’s review to be limited to only the items she actually observed, and it was unlawful for the detective to inspect other text messages without a search authorization. Because the Government was unable to show with sufficient specificity which text messages TSgt Roberts saw when she went through the phone, all evidence recovered by Detective AR from the appellee’s phone as well as any evidence derived from those texts (to include the information relating to SrA LB) was obtained in violation of the Fourth Amendment.⁶

The military judge also concluded the Government had not met its burden of showing that the information on the phone would have been inevitably discovered, given Detective AR’s lack of effort to secure a warrant or to even explore the possible ramifications of searching a stolen phone known to contain the appellee’s personal information.

Private and Government Search

Warrantless searches and seizures are presumptively unreasonable. *See, e.g., Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (warrantless searches presumptively unreasonable); *United States v. Daniels*, 60 M.J. 69, 71–72 (C.A.A.F. 2004) (citing *Camara v. Municipal Court of San Francisco*, 387 U.S. 523 (1967)). Mil. R. Evid. 311(a) provides that evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against the accused upon timely objection. The prosecution has the burden of establishing the admissibility of the evidence by a preponderance of the evidence. Mil. R. Evid. 311(e)(1). Derivative evidence obtained from the search may be admitted only if the military judge finds by a preponderance of the evidence that the evidence was not obtained as a result of an unlawful search or seizure, that the evidence ultimately would have been obtained by lawful means even if the unlawful search or seizure had not been made, or that the evidence was obtained with good faith reliance on the issuance of an authorization to search or seize. Mil. R. Evid. 311(e)(2).

Having reviewed the record, we find the military judge’s findings of fact “are well within the range of the evidence permitted under the clearly-erroneous standard.” *United*

⁶ We agree with the military judge’s finding that the appellee did not abandon his expectation of privacy simply because he did not file a police report after discovering the phone was stolen.

States v. Norris, 55 M.J. 209, 215 (C.A.A.F. 2001). We review his conclusions of law de novo. *United States v. Ayala*, 43 M.J. 296 (C.A.A.F. 1995).

We agree with the military judge's conclusion that TSgt Roberts's private searches of the appellee's phone do not implicate the Fourth Amendment, no matter how unreasonably she acted. *Jacobsen*, 466 U.S. at 113; *Walter*, 447 U.S. 649; *Reister*, 44 M.J. at 415-16; *United States v. Portt*, 21 M.J. 333, 334 (C.M.A. 1986) (where airman opened locker in private capacity and summoned law enforcement after finding evidence of drug use, "subsequent opening of the locker was simply a continuation of that entry"). Accordingly, we conclude that the exclusionary rule was not triggered by any private invasion of appellee's privacy.

Detective AR could view and the Government could take possession of the texts, photograph, and video-recording seen by TSgt Roberts without implicating Fourth Amendment concerns. *Burdeau v. McDowell*, 256 U.S. 465, 475-76 (1921) (Government may retain for use against owner incriminating documents which were stolen by private individuals, without governmental knowledge or complicity, and turned over to the Government).

However, we disagree with his conclusion that Detective AR's review of the text messages was limited to the precise messages seen by TSgt Roberts. When, as here, law enforcement personnel take possession of evidence from a third party following a private search, the Government's subsequent actions are examined and tested under the Fourth Amendment. *Jacobsen*, 466 U.S. at 115 ("additional invasions of [the owner's] privacy . . . must be tested by the degree to which they exceeded the scope of the private search"). The key question is whether law enforcement officials are limited to only examining files inspected by the private party (as the military judge found) or whether all readily observable data on the electronic device is within the scope of the initial private search and thus can be obtained by law enforcement.

We are unaware of any military cases addressing this specific question, but we adopt the reasoning and conclusion of the Fifth Circuit in an analogous case to find Detective AR did not exceed the scope of TSgt Roberts's private search. In *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001), Runyan's wife found several computer disks belonging to her husband. After viewing some of the disks and finding child pornography, she turned all the disks over to law enforcement. Detectives examined not only the files the wife had observed, but also examined the contents of all the seized evidence, to include disks the wife had not searched. During the search, additional child pornography was located on the disks that the wife saw.

The court likened a computer disk to a closed container and held that "[i]n the context of a closed container search . . . the police do not exceed the private search when they examine more items within a closed container than did the private searchers." *Id.* at

464. Applying the Eleventh Circuit's analysis in *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir.1990), the court stated that "[i]n the context of a search involving a number of closed containers, this suggests that opening a container that was not opened by private searchers would not necessarily be problematic if the police knew with substantial certainty, based on the statements of the private searchers, their replication of the private search, and their expertise, what they would find inside. Such an 'expansion' of the private search provides the police with no additional knowledge that they did not already obtain from the underlying private search and frustrates no expectation of privacy that has not already been frustrated." *Id.* at 463. The court concluded that "a defendant's expectation of privacy with respect to a container unopened by the private searchers is preserved unless the defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search." *Id.* at 463-64. Thus, the police do not engage in a new search for Fourth Amendment purposes each time they examine a particular item found within the container. *Id.* at 465.

We find the Fifth Circuit's reasoning to be persuasive and conclude the military judge incorrectly interpreted the law when he held that Detective AR's search had to exactly mirror TSgt Roberts's search in order to be lawful. We read the Supreme Court precedent to be more concerned with the scope of the private party's search and the corresponding frustration of the appellee's right to privacy rather than creating an uncompromising rule based only on examining the Government's success in precisely replicating the physical intrusion already perpetrated by the private party.

Detective AR's viewing of the appellee's phone is analogous to examination of the computer disks in *Runyan*. Before TSgt Roberts took the phone, the phone and its contents were akin to a "closed container" in which the appellee maintained a privacy interest. However, once TSgt Roberts breached the container by looking at the messages, the appellee's expectation of privacy with respect to all of the text messages (with the exception of the deleted texts) was frustrated. This fact is borne out by the appellee's own action in calling SrA LB and telling her that there might be an investigation as a result of the text messages.

Given that, Detective AR did not violate the Fourth Amendment when she viewed different text messages located on the phone. Detective AR's search was no different in character than the one conducted by TSgt Roberts, even though the individual text messages that were opened by the former may have been different.⁷

⁷ Our ruling is with respect only to the text messages maintained on the phone and that would have been available to both TSgt Roberts and Detective AR via a typical search consisting of opening the message. We find the appellee did not forfeit his expectation of privacy to content on the phone that was not included in the text messages (i.e. e-mails) or to deleted text messages that required additional software to examine. *See generally United States v. Walter*, 447 U.S. 649 (1980) (use of a film projector to view seized film was outside the scope of the private party's initial search).

To conclude otherwise would find a constitutional violation whenever law enforcement happens to see an item that the private searcher did not see and “would over-deter the police, preventing them from engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded.” *Runyan*, 275 F.3d at 465. It would also lead law enforcement to “waste valuable time and resources obtaining warrants based on intentionally false or mistaken testimony of private searches,” instead of confirming the validity of the private searcher’s claim prior to initiating that process. *Id.*

Similarly, the extraction of the text messages relating to the three women by the Sheriff’s Office and the commercial company was not an unconstitutional expansion on the original private search. Each non-deleted text extracted by those entities was viewable by TSgt Roberts when she conducted her private search, and therefore the appellee’s expectation of privacy in the texts was frustrated. Although the better practice would have been for Detective AR to seek a search warrant prior to having those text messages extracted, we do not find the extraction to have been unconstitutional.

Conclusion

We find that Detective AR’s search of the phone did not exceed the private party’s search in any manner that rendered it unconstitutional. The Fourth Amendment did not require Detective AR’s search and the evidence derived from it to be suppressed, and the judge’s ruling to the contrary was error.

On consideration of the Appeal by the United States under Article 62, UCMJ, it is by the Court on this 24th day of June, 2013,

ORDERED:

That the United States’ Appeal Under Article 62, UCMJ, is hereby **GRANTED**. The ruling of the military judge is vacated and the record is remanded for further proceedings.



FOR THE COURT


STEVEN LUCAS
Clerk of the Court

Appendix B

2013 WL 2129119

Only the Westlaw citation is currently available.
United States Court of Appeals,
First Circuit.

UNITED STATES of America, Appellee,
v.
Brima WURIE, Defendant, Appellant.

No. 11–1792. | May 17, 2013.

Synopsis

Background: Following denial of his motion to suppress the evidence obtained as a result of a warrantless search of his cell phone, defendant was convicted in the United States District Court for the District of Massachusetts, [Richard G. Stearns, J.](#), 612 F.Supp.2d 104, of possessing with intent to distribute and distributing cocaine base and with being a felon in possession of a firearm and ammunition, and he appealed.

Holding: The Court of Appeals, [Stahl](#), Circuit Judge, held that search-incident-to-arrest exception did not authorize the warrantless search of data on a cell phone seized from arrestee's person.

Denial of motion to suppress reversed; conviction vacated; remanded.

[Howard](#), Circuit Judge, filed dissenting opinion.

Appeal from the United States District Court for the District of Massachusetts, [Richard G. Stearns](#), U.S. District Judge.

Attorneys and Law Firms

Ian Gold, Assistant Federal Public Defender, for appellant.

[Michael R. Dreeben](#), Attorney, United States Department of Justice, with whom [Carmen M. Ortiz](#), United States Attorney, and [Kelly Begg Lawrence](#), Assistant United States Attorney, were on brief, for appellee.

Before [HOWARD](#), [STAHL](#), and [LIPEZ](#), Circuit Judges.

Opinion

[STAHL](#), Circuit Judge.

*1 This case requires us to decide whether the police, after seizing a cell phone from an individual's person as part of his lawful arrest, can search the phone's data without a

warrant. We conclude that such a search exceeds the boundaries of the Fourth Amendment search-incident-to-arrest exception. Because the government has not argued that the search here was justified by exigent circumstances or any other exception to the warrant requirement, we reverse the denial of defendant-appellant Brima Wurie's motion to suppress, vacate his conviction, and remand his case to the district court.

I. Facts & Background

On the evening of September 5, 2007, Sergeant Detective Paul Murphy of the Boston Police Department (BPD) was performing routine surveillance in South Boston. He observed Brima Wurie, who was driving a Nissan Altima, stop in the parking lot of a Lil Peach convenience store, pick up a man later identified as Fred Wade, and engage in what Murphy believed was a drug sale in the car. Murphy and another BPD officer subsequently stopped Wade and found two plastic bags in his pocket, each containing 3.5 grams of crack cocaine. Wade admitted that he had bought the drugs from "B," the man driving the Altima. Wade also told the officers that "B" lived in South Boston and sold crack cocaine.

Murphy notified a third BPD officer, who was following the Altima. After Wurie parked the car, that officer arrested Wurie for distributing crack cocaine, read him *Miranda* warnings, and took him to the police station. When Wurie arrived at the station, two cell phones, a set of keys, and \$1,275 in cash were taken from him.

Five to ten minutes after Wurie arrived at the station, but before he was booked, two other BPD officers noticed that one of Wurie's cell phones, a gray Verizon LG phone, was repeatedly receiving calls from a number identified as "my house" on the external caller ID screen on the front of the phone. The officers were able to see the caller ID screen, and the "my house" label, in plain view. After about five more minutes, the officers opened the phone to look at Wurie's call log. Immediately upon opening the phone, the officers saw a photograph of a young black woman holding a baby, which was set as the phone's "wallpaper." The officers then pressed one button on the phone, which allowed them to access the phone's call log. The call log showed the incoming calls from "my house." The officers pressed one more button to determine the phone number associated with the "my house" caller ID reference.

One of the officers typed that phone number into an online white pages directory, which revealed that the address associated with the number was on Silver Street in South Boston, not far from where Wurie had parked his car just before he was arrested. The name associated with the

address was Manny Cristal.

Sergeant Detective Murphy then gave Wurie a new set of *Miranda* warnings and asked him a series of questions. Wurie said, among other things, that he lived at an address on Speedwell Street in Dorchester and that he had only been “cruising around” in South Boston. He denied having stopped at the Lil Peach store, having given anyone a ride, and having sold crack cocaine.

*2 Suspecting that Wurie was a drug dealer, that he was lying about his address, and that he might have drugs hidden at his house, Murphy took Wurie’s keys and, with other officers, went to the Silver Street address associated with the “my house” number. One of the mailboxes at that address listed the names Wurie and Cristal. Through the first-floor apartment window, the officers saw a black woman who looked like the woman whose picture appeared on Wurie’s cell phone wallpaper. The officers entered the apartment to “freeze” it while they obtained a search warrant. Inside the apartment, they found a sleeping child who looked like the child in the picture on Wurie’s phone. After obtaining the warrant, the officers seized from the apartment, among other things, 215 grams of crack cocaine, a firearm, ammunition, four bags of marijuana, drug paraphernalia, and \$250 in cash.

Wurie was charged with possessing with intent to distribute and distributing cocaine base and with being a felon in possession of a firearm and ammunition. He filed a motion to suppress the evidence obtained as a result of the warrantless search of his cell phone; the parties agreed that the relevant facts were not in dispute and that an evidentiary hearing was unnecessary. The district court denied Wurie’s motion to suppress, *United States v. Wurie*, 612 F.Supp.2d 104 (D.Mass.2009), and, after a four-day trial, the jury found Wurie guilty on all three counts. He was sentenced to 262 months in prison. This appeal followed.

II. Analysis

In considering the denial of a motion to suppress, we review the district court’s factual findings for clear error and its legal conclusions de novo. *United States v. Kearney*, 672 F.3d 81, 88–89 (1st Cir.2012).

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” and provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The amendment grew out of American colonial opposition to British search and seizure practices, most notably the use

of writs of assistance, which gave customs officials broad latitude to search houses, shops, cellars, warehouses, and other places for smuggled goods. The Honorable M. Blane Michael, *Reading the Fourth Amendment: Guidance from the Mischief that Gave it Birth*, 85 N.Y.U. L.Rev. 905, 907–09 (2010); see generally William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning 602–1791* (2009).

James Otis, a lawyer who challenged the use of writs of assistance in a 1761 case, famously described the practice as “plac[ing] the liberty of every man in the hands of every petty officer” and sounded two main themes: the need to protect the privacy of the home (what he called the “fundamental ... Privilege of House”), Michael, *supra*, at 908 (citations and internal quotation marks omitted), and “the inevitability of abuse when government officials have the sort of unlimited discretion sanctioned by the writ,” *id.* at 909. The Supreme Court has described Otis’s argument as “perhaps the most prominent event which inaugurated the resistance of the colonies to the oppressions of the mother country.” *Boyd v. United States*, 116 U.S. 616, 625, 6 S.Ct. 524, 29 L.Ed. 746 (1886).

*3 Today, a warrantless search is *per se* unreasonable under the Fourth Amendment, unless one of “a few specifically established and well-delineated exceptions” applies. *Arizona v. Gant*, 556 U.S. 332, 338, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)) (internal quotation marks omitted). One of those exceptions allows the police, when they make a lawful arrest, to search “the arrestee’s person and the area within his immediate control.” *Id.* at 339 (quoting *Chimel v. California*, 395 U.S. 752, 763, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969)) (internal quotation marks omitted). In recent years, courts have grappled with the question of whether the search-incident-to-arrest exception extends to data within an arrestee’s cell phone.¹

A. The legal landscape

The modern search-incident-to-arrest doctrine emerged from *Chimel v. California*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969), in which the Supreme Court held that a warrantless search of the defendant’s entire house was not justified by the fact that it occurred as part of his valid arrest. The Court found that the search-incident-to-arrest exception permits an arresting officer “to search for and seize any evidence on the arrestee’s person in order to prevent its concealment or destruction” and to search “the area into which an arrestee might reach in order to grab a weapon or evidentiary items.” *Id.* at 763. The justifications underlying the exception, as articulated in *Chimel*, were protecting officer safety and ensuring the preservation of evidence. *Id.*

Four years later, in *United States v. Robinson*, 414 U.S.

218 (1973), the Supreme Court examined how the search-incident-to-arrest exception applies to searches of the person. Robinson was arrested for driving with a revoked license, and in conducting a pat down, the arresting officer felt an object that he could not identify in Robinson's coat pocket. *Id.* at 220–23. He removed the object, which turned out to be a cigarette package, and then felt the package and determined that it contained something other than cigarettes. Upon opening the package, the officer found fourteen capsules of heroin. *Id.* at 223. The Court held that the warrantless search of the cigarette package was valid, explaining that the police have the authority to conduct “a full search of the person” incident to a lawful arrest. *Id.* at 235.

Robinson reiterated the principle, discussed in *Chimel*, that “[t]he justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial.” *Id.* at 234. However, the Court also said the following:

The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect. A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification.

*4 *Id.* at 235.

The following year, the Court decided *United States v. Edwards*, 415 U.S. 800, 94 S.Ct. 1234, 39 L.Ed.2d 771 (1974). Edwards was arrested on suspicion of burglary and detained at a local jail. After his arrest, police realized that Edwards's clothing, which he was still wearing, might contain paint chips tying him to the burglary. The police seized the articles of clothing and examined them for paint fragments. *Id.* at 801–02. The Court upheld the search, concluding that once it became apparent that the items of clothing might contain destructible evidence of a crime, “the police were entitled to take, examine, and preserve them for use as evidence, just as they are normally permitted to seize evidence of crime when it is lawfully encountered.” *Id.* at 806.

The Court again addressed the search-incident-to-arrest exception in *United States v. Chadwick*, 433 U.S. 1, 97

S.Ct. 2476, 53 L.Ed.2d 538 (1977), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991), this time emphasizing that not all warrantless searches undertaken in the context of a custodial arrest are constitutionally reasonable. In *Chadwick*, the defendants were arrested immediately after having loaded a footlocker into the trunk of a car. *Id.* at 3–4. The footlocker remained under the exclusive control of federal narcotics agents until they opened it, without a warrant and about an hour and a half after the defendants were arrested, and found marijuana in it. *Id.* at 4–5. The Court invalidated the search, concluding that the justifications for the search-incident-to-arrest exception—the need for the arresting officer “[t]o safeguard himself and others, and to prevent the loss of evidence”—were absent. *Id.* at 14. The search “was conducted more than an hour after federal agents had gained exclusive control of the footlocker and long after respondents were securely in custody” and therefore could not “be viewed as incidental to the arrest or as justified by any other exigency.” *Id.* at 15.

Finally, there is the Supreme Court's recent decision in *Arizona v. Gant*, 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009). *Gant* involved the search of an arrestee's vehicle, which is governed by a distinct set of rules, *see id.* at 343, but the Court began with a general summary of the search-incident-to-arrest doctrine. Once again, the Court reiterated the twin rationales underlying the exception, first articulated in *Chimel*: “protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy.” *Id.* at 339 (citing *Chimel*, 395 U.S. at 763). Relying on those safety and evidentiary justifications, the Court found that a search of a vehicle incident to arrest is lawful “when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search.” *Id.* at 343.²

Courts have struggled to apply the Supreme Court's search-incident-to-arrest jurisprudence to the search of data on a cell phone seized from the person. The searches at issue in the cases that have arisen thus far have involved everything from simply obtaining a cell phone's number, *United States v. Flores-Lopez*, 670 F.3d 803, 804 (7th Cir.2012), to looking through an arrestee's call records, *United States v. Finley*, 477 F.3d 250, 254 (5th Cir.2007), text messages, *id.*, or photographs, *United States v. Quintana*, 594 F.Supp.2d 1291, 1295–96 (M.D.Fl.2009).

*5 Though a majority of these courts have ultimately upheld warrantless cell phone data searches, they have used a variety of approaches. Some have concluded that, under *Robinson* and *Edwards*, a cell phone can be freely searched incident to a defendant's lawful arrest, with no justification beyond the fact of the arrest itself. *E.g.*, *People v. Diaz*, 51 Cal.4th 84, 119 Cal.Rptr.3d 105, 244 P.3d 501 (Cal.2011). Others have, to varying degrees, relied on the need to preserve evidence on a cell phone.

E.g., United States v. Murphy, 552 F.3d 405, 411 (4th Cir.2009); *Finley*, 477 F.3d at 260; *Commonwealth v. Phifer*, 463 Mass. 790, 979 N.E.2d 210, 213–16 (Mass.2012). The Seventh Circuit discussed the *Chimel* rationales more explicitly in *Flores–Lopez*, assuming that warrantless cell phone searches must be justified by a need to protect arresting officers or preserve destructible evidence, 670 F.3d at 806–07, and finding that evidence preservation concerns outweighed the invasion of privacy at issue in that case, because the search was minimally invasive, *id.* at 809.

A smaller number of courts have rejected warrantless cell phone searches, with similarly disparate reasoning. In *United States v. Park*, No. CR 05–375 SI, 2007 WL 1521573 (N.D.Cal. May 23, 2007), for example, the court concluded that a cell phone should be viewed not as an item immediately associated with the person under *Robinson* and *Edwards* but as a possession within an arrestee’s immediate control under *Chadwick*, which cannot be searched once the phone comes into the exclusive control of the police, absent exigent circumstances, *id.* at *8. In *State v. Smith*, 124 Ohio St.3d 163, 920 N.E.2d 949 (Ohio 2009), the Ohio Supreme Court distinguished cell phones from other “closed containers” that have been found searchable incident to an arrest and concluded that, because an individual has a high expectation of privacy in the contents of her cell phone, any search thereof must be conducted pursuant to a warrant, *id.* at 955. And most recently, in *Smallwood v. State*, —So.3d —, 2013 WL 1830961 (Fla. May 2, 2013), the Florida Supreme Court held that the police cannot routinely search the data within an arrestee’s cell phone without a warrant, *id.* at *10. The court read *Gant* as prohibiting a search once an arrestee’s cell phone has been removed from his person, which forecloses the ability to use the phone as a weapon or to destroy evidence contained therein. *Id.*

B. Our vantage point

We begin from the premise that, in the Fourth Amendment context, “[a] single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront.” *Dunaway v. New York*, 442 U.S. 200, 213–14, 99 S.Ct. 2248, 60 L.Ed.2d 824 (1979). The Supreme Court has therefore rejected “inherently subjective and highly fact specific” rules that require “ad hoc determinations on the part of officers in the field and reviewing courts” in favor of clear ones that will be “readily understood by police officers.” *Thornton v. United States*, 541 U.S. 615, 623, 124 S.Ct. 2127, 158 L.Ed.2d 905 (2004); *see also New York v. Belton*, 453 U.S. 454, 458, 101 S.Ct. 2860, 69 L.Ed.2d 768 (1981) (“A highly sophisticated set of rules, qualified by all sorts of ifs, ands, and buts and requiring the drawing of subtle nuances and hairline distinctions, may be

the sort of heady stuff upon which the facile minds of lawyers and judges eagerly feed, but they may be literally impossible of application by the officer in the field.” (citation and internal quotation marks omitted)). As a result, when it upheld the warrantless search of the cigarette pack in *Robinson*, “the Court hewed to a straightforward rule, easily applied, and predictably enforced.” *Belton*, 453 U.S. at 459. Thus, we find it necessary to craft a bright-line rule that applies to all warrantless cell phone searches, rather than resolving this case based solely on the particular circumstances of the search at issue.³

*6 The government seems to agree, urging us to find that a cell phone, like any other item carried on the person, can be thoroughly searched incident to a lawful arrest.⁴ The government’s reasoning goes roughly as follows: (1) Wurie’s cell phone was an item immediately associated with his person, because he was carrying it on him at the time of his arrest (or at least he does not argue otherwise); (2) such items can be freely searched without any justification beyond the fact of the lawful arrest, *see Robinson*, 414 U.S. at 235; (3) the search can occur even after the defendant has been taken into custody and transported to the station house, *see Edwards*, 415 U.S. at 803;⁵ and (4) there is no limit on the scope of the search, other than the Fourth Amendment’s core reasonableness requirement, *see id.* at 808 n. 9.⁶

This “literal reading of the *Robinson* decision,” *Flores–Lopez*, 670 F.3d at 805, fails to account for the fact that the Supreme Court has determined that there are categories of searches undertaken following an arrest that are inherently unreasonable because they are never justified by one of the *Chimel* rationales: protecting arresting officers or preserving destructible evidence. *E.g., Gant*, 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485; *Chadwick*, 433 U.S. 1, 97 S.Ct. 2476, 53 L.Ed.2d 538. As we explain below, this case therefore turns on whether the government can demonstrate that warrantless cell phone searches, as a category, fall within the boundaries laid out in *Chimel*.

The government admitted at oral argument that its interpretation of the search-incident-to-arrest exception would give law enforcement broad latitude to search any electronic device seized from a person during his lawful arrest, including a laptop computer or a tablet device such as an iPad. The search could encompass things like text messages, *e.g., Finley*, 477 F.3d at 254, emails, *e.g., People v. Nottoli*, 199 Cal.App.4th 531, 130 Cal.Rptr.3d 884, 894 (Cal. Ct.App.2011), or photographs, *e.g., Quintana*, 594 F.Supp.2d at 1295–96, though the officers here only searched Wurie’s call log. *Robinson* and *Edwards*, the government claims, compel such a finding.

We suspect that the eighty-five percent of Americans who own cell phones and “use the devices to do much more than make phone calls,” Maeve Duggan & Lee Rainie, *Cell Phone Activities 2012*, Pew Internet & American Life

Project, 2 (Nov. 25, 2012), http://pewinternet.org/~media/Files/Reports/2012/PIP_CellActivities_11.25.pdf, would have some difficulty with the government's view that "Wurie's cell phone was indistinguishable from other kinds of personal possessions, like a cigarette package, wallet, pager, or address book, that fall within the search incident to arrest exception to the Fourth Amendment's warrant requirement."⁷ In reality, "a modern cell phone is a computer," and "a computer ... is not just another purse or address book." *Flores-Lopez*, 670 F.3d at 805. The storage capacity of today's cell phones is immense. Apple's iPhone 5 comes with up to sixty-four gigabytes of storage, see Apple, iPhone, Tech Specs, <http://www.apple.com/iphone/specs.html> (last visited May 16, 2013), which is enough to hold about "four million pages of Microsoft Word documents," Charles E. MacLean, *But, Your Honor, a Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Cell Phone Memory Searches Incident to Lawful Arrest*, 6 Fed. Cts. L.Rev. 37, 42 (2012).⁸

*7 That information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records. See *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir.2013) (en banc) ("The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities.")⁹ It is the kind of information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest. See *Chimel*, 395 U.S. 752, 89 S.Ct. 2034, 23 L.Ed.2d 685. Indeed, modern cell phones provide direct access to the home in a more literal way as well; iPhones can now connect their owners directly to a home computer's webcam, via an application called iCam, so that users can monitor the inside of their homes remotely. *Flores-Lopez*, 670 F.3d at 806. "At the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though a house contains data." *Id.*

In short, individuals today 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 that the government has invoked. See *id.* at 805 (rejecting the idea that a cell phone can be compared to other items carried on the person, because today's cell phones are "quite likely to contain, or provide ready access to, a vast body of personal data").¹⁰ Just as customs officers in the early colonies could use writs of assistance to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule would give law enforcement automatic access to "a virtual warehouse" of an individual's "most intimate communications and photographs without probable cause"

if the individual is subject to a custodial arrest, even for something as minor as a traffic violation. Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L.Rev. 183, 211 (2010). We are reminded of James Otis's concerns about "plac[ing] the liberty of every man in the hands of every petty officer." Michael, *supra*, at 908 (citation and internal quotation marks omitted).

It is true that *Robinson* speaks broadly, and that the Supreme Court has never found the constitutionality of a search of the person incident to arrest to turn on the kind of item seized or its capacity to store private information. In our view, however, what distinguishes a warrantless search of the data within a modern cell phone from the inspection of an arrestee's cigarette pack or the examination of his clothing is not just the nature of the item searched, but the nature and scope of the search itself.

*8 In *Gant*, the Court emphasized the need for "the scope of a search incident to arrest" to be "commensurate with its purposes," which include "protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy." 556 U.S. at 339; see also *Chimel*, 395 U.S. at 762-63 ("When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use ... [and] to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."). Inspecting the contents of a cigarette pack can (and, in *Robinson*, did) preserve destructible evidence (heroin capsules). It is also at least theoretically necessary to protect the arresting officer, who does not know what he will find inside the cigarette pack. Examining the clothing an arrestee is wearing can (and, in *Edwards*, did) preserve destructible evidence (paint chips). Thus, the searches at issue in *Robinson* and *Edwards* were the kinds of reasonable, self-limiting searches that do not offend the Fourth Amendment, even when conducted without a warrant. The same can be said of searches of wallets, address books, purses, and briefcases, which are all potential repositories for destructible evidence and, in some cases, weapons.

When faced, however, with categories of searches that cannot ever be justified under *Chimel*, the Supreme Court has taken a different approach. In *Chadwick*, the Court struck down warrantless searches of "luggage or other personal property not immediately associated with the person of the arrestee" that the police have "reduced ... to their exclusive control," because such searches are not necessary to preserve destructible evidence or protect officer safety. 433 U.S. at 15. Similarly, in *Gant*, the Court concluded that searching the passenger compartment of a vehicle once the arrestee has been secured and confined to a police car neither preserves destructible evidence nor protects officer safety. 556 U.S. at 335; see also *id.* at 339 ("If there is no possibility that an arrestee could reach into the area that law enforcement officers seek to search, both

justifications for the search-incident-to-arrest exception are absent and the rule does not apply.”). The searches at issue in *Chadwick* and *Gant* were general, evidence-gathering searches, not easily subject to any limiting principle, and the Fourth Amendment permits such searches only pursuant to a lawful warrant. See *Thornton*, 541 U.S. at 632 (Scalia, J., concurring) (“When officer safety or imminent evidence concealment or destruction is at issue, officers should not have to make fine judgments in the heat of the moment. But in the context of a general evidence-gathering search, the state interests that might justify any overbreadth are far less compelling.”).

We therefore find it necessary to ask whether the warrantless search of data within a cell phone can ever be justified under *Chimel*. See *Flores–Lopez*, 670 F.3d at 806–10 (considering whether either of the *Chimel* rationales applies to cell phone data searches); cf. *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir.1996) (upholding the warrantless search of a pager incident to arrest because of the risk of destruction of evidence). The government has provided little guidance on that question. Instead, it has hewed to a formalistic interpretation of the case law, forgetting that the search-incident-to-arrest doctrine does not describe an independent right held by law enforcement officers, but rather a class of searches that are only reasonable in the Fourth Amendment sense because they are potentially necessary to preserve destructible evidence or protect police officers. Indeed, the government has included just one, notably tentative footnote in its brief attempting to place warrantless cell phone data searches within the *Chimel* boundaries. We find ourselves unconvinced.

*9 The government does not argue that cell phone data searches are justified by a need to protect arresting officers. Wurie concedes that arresting officers can inspect a cell phone to ensure that it is not actually a weapon, see *Flores–Lopez*, 670 F.3d at 806 (“One can buy a stun gun that looks like a cell phone.”), but we have no reason to believe that officer safety would require a further intrusion into the phone’s contents. As we mentioned earlier, the officer who conducted the search in *Robinson* had no idea what he might find in the cigarette pack, which therefore posed a safety risk. The officers who searched Wurie’s phone, on the other hand, knew exactly what they would find therein: data. They also knew that the data could not harm them.

The government has, however, suggested that the search here was “arguably” necessary to prevent the destruction of evidence. Specifically, the government points to the possibility that the calls on Wurie’s call log could have been overwritten or the contents of his phone remotely wiped if the officers had waited to obtain a warrant.¹¹ The problem with the government’s argument is that it does not seem to be particularly difficult to prevent overwriting of calls or remote wiping of information on a cell phone today. Arresting officers have at least three options. First,

in some instances, they can simply turn the phone off or remove its battery. See *Flores–Lopez*, 670 F.3d at 808; *Diaz*, 119 Cal.Rptr.3d 105, 244 P.3d at 515 n. 24 (Werdegar, J., dissenting). Second, they can put the phone in a Faraday enclosure, a relatively inexpensive device “formed by conducting material that shields the interior from external electromagnetic radiation.” MacLean, *supra*, at 50 (citation and internal quotation marks omitted); see also *Flores–Lopez*, 670 F.3d at 809. Third, they may be able “to ‘mirror’ (copy) the entire cell phone contents, to preserve them should the phone be remotely wiped, without looking at the copy unless the original disappears.” *Flores–Lopez*, 670 F.3d at 809.

Indeed, if there is a genuine threat of remote wiping or overwriting, we find it difficult to understand why the police do not routinely use these evidence preservation methods, rather than risking the loss of the evidence during the time it takes them to search through the phone. Perhaps the answer is in the government’s acknowledgment that the possibility of remote wiping here was “remote” indeed. Weighed against the significant privacy implications inherent in cell phone data searches, we view such a slight and truly theoretical risk of evidence destruction as insufficient. While the measures described above may be less convenient for arresting officers than conducting a full search of a cell phone’s data incident to arrest, the government has not suggested that they are unworkable, and it bears the burden of justifying its failure to obtain a warrant. See *United States v. Jeffers*, 342 U.S. 48, 51, 72 S.Ct. 93, 96 L.Ed. 59 (1951). “[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment.” *Mincey v. Arizona*, 437 U.S. 385, 393, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978).

*10 Instead of truly attempting to fit this case within the *Chimel* framework, the government insists that we should disregard the *Chimel* rationales entirely, for two reasons.

First, the government emphasizes that *Robinson* rejected the idea that “there must be litigated in each case the issue of whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest.” 414 U.S. at 235. That holding was predicated on an assumption, clarified in *Chadwick*, that “[t]he potential dangers lurking in all custodial arrests” are what “make warrantless searches of items within the ‘immediate control’ area reasonable without requiring the arresting officer to calculate the probability that weapons or destructible evidence may be involved.” 433 U.S. at 14–15. For the reasons we just discussed, that assumption appears to be incorrect in the case of cell phone data searches. More importantly, however, we are not suggesting a rule that would require arresting officers or reviewing courts to decide, on a case-by-case basis, whether a particular cell phone data search is justified under *Chimel*. Rather, we believe that warrantless cell phone data searches are *categorically* unlawful under the

search-incident-to-arrest exception, given the government's failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence. We read *Robinson* as compatible with such a finding.

Second, the government places great weight on a footnote at the end of *Chadwick* stating that searches of the person, unlike "searches of possessions within an arrestee's immediate control," are "justified by ... reduced expectations of privacy caused by the arrest." 433 U.S. at 16 n. 10. The government reads that footnote as establishing an unlimited principle that searches of items carried on the person require no justification whatsoever beyond a lawful arrest, making *Chimel* irrelevant in this context. The *Chadwick* footnote is surely meant to reference similar language in *Robinson* explaining that, because the "custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment[,] ... a search incident to the arrest requires no additional justification." 414 U.S. at 235.

Yet the Court clearly stated in *Robinson* that "[t]he authority to search the person incident to a lawful custodial arrest" is "based upon the need to disarm and to discover evidence," *id.*, and *Chadwick* did not alter that rule. When the Court decided *Robinson* in 1973 and *Chadwick* in 1977, any search of the person would almost certainly have been the type of self-limiting search that could be justified under *Chimel*. The Court, more than thirty-five years ago, could not have envisioned a world in which the vast majority of arrestees would be carrying on their person an item containing not physical evidence but a vast store of intangible data—data that is not immediately destructible and poses no threat to the arresting officers.

*11 In the end, we therefore part ways with the Seventh Circuit, which also applied the *Chimel* rationales in *Flores-Lopez*. Though the court described the risk of evidence destruction as arguably "so slight as to be outweighed by the invasion of privacy from the search," it found that risk to be sufficient, given the minimal nature of the intrusion at issue (the officers had only searched the cell phone for its number). *Flores-Lopez*, 670 F.3d at 809. That conclusion was based, at least in part, on Seventh Circuit precedent allowing a "minimally invasive" warrantless search. *Id.* at 807 (citing *United States v. Concepcion*, 942 F.2d 1170 (7th Cir.1991)).

We are faced with different precedent and different facts, but we also see little room for a case-specific holding, given the Supreme Court's insistence on bright-line rules in the Fourth Amendment context. See, e.g., *Thornton*, 541 U.S. at 623. A series of opinions allowing some cell phone data searches but not others, based on the nature and reasonableness of the intrusion, would create exactly the "inherently subjective and highly fact specific" set of rules that the Court has warned against and would be extremely difficult for officers in the field to apply. *Id.* Thus, while

the search of Wurie's call log was less invasive than a search of text messages, emails, or photographs, it is necessary for all warrantless cell phone data searches to be governed by the same rule. A rule based on particular instances in which the police do not take full advantage of the unlimited potential presented by cell phone data searches would prove impotent in those cases in which they choose to exploit that potential.

We therefore hold that the search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person, because the government has not convinced us that such a search is ever necessary to protect arresting officers or preserve destructible evidence. See *Chimel*, 395 U.S. at 763. Instead, warrantless cell phone data searches strike us as a convenient way for the police to obtain information related to a defendant's crime of arrest—or other, as yet undiscovered crimes—without having to secure a warrant. We find nothing in the Supreme Court's search-incident-to-arrest jurisprudence that sanctions such a "general evidence-gathering search." *Thornton*, 541 U.S. at 632 (Scalia, J., concurring).¹²

There are, however, other exceptions to the warrant requirement that the government has not invoked here but that might justify a warrantless search of cell phone data under the right conditions. Most importantly, we assume that the exigent circumstances exception would allow the police to conduct an immediate, warrantless search of a cell phone's data where they have probable cause to believe that the phone contains evidence of a crime, as well as a compelling need to act quickly that makes it impracticable for them to obtain a warrant—for example, where the phone is believed to contain evidence necessary to locate a kidnapped child or to investigate a bombing plot or incident. See *United States v. Tibolt*, 72 F.3d 965, 969 (1st Cir.1995) (discussing the exigent circumstances exception).

C. The good-faith exception

*12 That leaves only the government's belated argument, made for the first time in a footnote in its brief on appeal, that suppression is inappropriate here under the good-faith exception to the exclusionary rule. See *United States v. Leon*, 468 U.S. 897 (1984). The government bears the "heavy burden" of proving that the good-faith exception applies, *United States v. Syphers*, 426 F.3d 461, 468 (1st Cir.2005), and it did not invoke the exception before the district court.

This is not a case in which an intervening change in the law made the good-faith exception relevant only after the district court issued its opinion. E.g., *Davis v. United States*, — U.S. —, — — —, 131 S.Ct. 2419, 2425–26, 180 L.Ed.2d 285 (2011); *United States v. Sparks*, 711 F.3d 58, 61–62 (1st Cir.2013); *United States v. Lopez*, 453

F. App'x 602, 605 (6th Cir.2011); *see also United States v. Curtis*, 635 F.3d 704, 713–14 (5th Cir.2011) (applying the good-faith exception “to a search that was legal at the time it was conducted but has been rendered illegal by an intervening change in the law”); *United States v. McCane*, 573 F.3d 1037, 1044 (10th Cir.2009) (finding that “a police officer who undertakes a search in reasonable reliance upon the settled case law of a United States Court of Appeals, even though the search is later deemed invalid by Supreme Court decision, has not engaged in misconduct”). The government emphasizes that we may affirm the district court’s suppression ruling on any ground made manifest by the record. *United States v. Doe*, 61 F.3d 107, 111–12 (1st Cir.1995). In this case, however, we do not believe that ground should be one with respect to which the government bore the burden of proof and entirely failed to carry that burden below, despite the fact that the issue was ripe for the district court’s review.¹³

III. Conclusion

Since the time of its framing, “the central concern underlying the Fourth Amendment” has been ensuring that law enforcement officials do not have “unbridled discretion to rummage at will among a person’s private effects.” *Gant*, 556 U.S. at 345; *see also Chimel*, 395 U.S. at 767–68. Today, many Americans store their most personal “papers” and “effects,” U.S. Const. amend. IV, in electronic format on a cell phone, carried on the person. Allowing the police to search that data without a warrant any time they conduct a lawful arrest would, in our view, create “a serious and recurring threat to the privacy of countless individuals .” *Gant*, 556 U.S. at 345; *cf. United States v. Jones*, — U.S. —, —, 132 S.Ct. 945, 950, 181 L.Ed.2d 911 (2012) (“At bottom, we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’” (quoting *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001))).

We therefore *reverse* the denial of Wurie’s motion to suppress, *vacate* his conviction, and *remand* for further proceedings consistent with this opinion.

HOWARD, Circuit Judge, dissenting.

*13 Undoubtedly, most of us would prefer that the information stored in our cell phones be kept from prying eyes, should a phone be lost or taken from our hands by the police during an arrest. One could, individually, take protective steps to enhance the phone’s security settings with respect to that information, or for that matter legislation might be enacted to make such unprotected information off-limits to finders or to the police unless they first obtain a warrant to search the phone. But the question

here is whether the Fourth Amendment *requires* this court to abandon long-standing precedent and place such unprotected information contained in cell phones beyond the reach of the police when making a custodial arrest. I think that we are neither required nor authorized to rule as the majority has.

Instead, this case requires us to apply a familiar legal standard to a new form of technology. This is an exercise we must often undertake as judges, for the Constitution is as durable as technology is disruptive. In this exercise, consistency is a virtue. Admittedly, when forced to confront the boundaries not only of the Fourth Amendment, but also of the technology in question, it is not surprising that we would look beyond the case at hand and theorize about the long-term effects of our decision. Yet the implications of our decisions, while important, are ancillary to our constitutionally defined power to resolve each case as it appears before us. Having scrutinized the relevant Supreme Court decisions, as well as our own precedent, I find no support for Wurie’s claim that he had a constitutional right protecting the information obtained during the warrantless search. Nor do I believe that we possess the authority to create such a right. Therefore, I respectfully dissent.

The facts are clear: the police conducted a valid custodial arrest of Wurie; the cell phone was on Wurie’s person at the time of the arrest; after seeing repeated calls to Wurie’s cell phone from “my house,” the police flipped it open and, pressing two buttons, retrieved the associated number.

We have long acknowledged that police officers can extract this type of information from containers immediately associated with a person at the time of arrest. In *United States v. Sheehan*, 583 F.2d 30 (1st Cir.1978), police arrested a suspected bank robber and then searched his wallet, which included a piece of paper bearing several names and telephone numbers. *Id.* at 30–31. The police officers copied this piece of paper, which action Sheehan challenged as an unconstitutional seizure. The claim is made that *Sheehan* is inapposite to the present case because it concerned a challenge to the seizure, not the search. We, however, did not address the warrantless search in *Sheehan* because its legality was beyond dispute. Judge Coffin, for the court, noted as an initial matter that “[a]ppellant concedes, *as he must*, that his arrest was lawful and that therefore the search of his wallet was legal.” *Id.* (emphasis added). It is not as though *Sheehan* left the legality of the search unresolved; rather, the court considered the issue uncontroversial, and therefore provided no elaboration. *See also United States v. Uricoechea-Casallas*, 946 F.2d 162, 165–66 (1st Cir.1991) (upholding the warrantless search of a wallet incident to a custodial arrest).

*14 *Sheehan* was no outlier. Courts have regularly upheld warrantless searches of nearly identical information in a range of “containers.” *E.g., United States v. Ortiz*, 84 F.3d

977, 984 (7th Cir.1996) (telephone numbers from a pager); *United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir.1993) (address book kept inside a wallet); *United States v. Molinaro*, 877 F.2d 1341, 1346–47 (7th Cir.1989) (phone numbers on slips of paper found in a wallet); *United States v. Holzman*, 871 F.2d 1496, 1504–05 (9th Cir.1989) (address book), *abrogated on other grounds by Horton v. California*, 496 U.S. 128, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990).

The police officers' limited search of one telephone number in Wurie's call log was even less intrusive than the searches in these cases. The police observed, in plain view, multiple calls from "my house"—a shorthand similar to what millions of cell phone owners use to quickly identify calls instead of the number assigned by the service provider—to Wurie's cell phone. Only then did they initiate their search and only for the limited purpose of retrieving the actual phone number associated with "my house." The police did not rummage through Wurie's cell phone, unsure of what they could find. Before they had even begun their search, they knew who was calling Wurie and how many times the person had called. The additional step of identifying the actual telephone number hardly constituted a further intrusion on Wurie's privacy interests, especially since that information is immediately known to the third-party telephone company. See *United States v. Flores-Lopez*, 670 F.3d 803, 807 (7th Cir.2012) (holding that the police could retrieve an arrestee's cell phone number from his phone without a warrant, in part, because "the phone company knows a phone's number as soon as the call is connected to the telephone network; and obtaining that information from the phone company isn't a search because by subscribing to the telephone service the user of the phone is deemed to surrender any privacy interest he may have had in his phone number") (citing *Smith v. Maryland*, 442 U.S. 735, 742–43, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)); see also Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 Santa Clara L.Rev. 183, 210 (suggesting a rule that permits the warrantless search of "call lists and text message addressees" pursuant to an arrest). This case fits easily within existing precedent.

Nor are there any other persuasive grounds for distinguishing this case from our previous decisions. That the container the police searched was a cell phone is not, by itself, dispositive, for "a constitutional distinction between 'worthy' and 'unworthy' containers would be improper." *United States v. Ross*, 456 U.S. 798, 822, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982). We made a similar observation in *United States v. Eatherton*, 519 F.2d 603 (1st Cir.1975), where we upheld the warrantless search of a briefcase incident to an arrest. *Id.* at 610–11. We recognized that a briefcase had some unique characteristics, but explicitly rejected any analysis turning on the nature of the searched container: "While a briefcase may be a different order of container from a cigarette box, it is not easy to rest a

principled articulation of the reach of the fourth amendment upon the distinction.... [W]hile [such a distinction] may have analytical appeal, it does not presently represent the law." *Id.* at 610 (citations omitted).

*15 Even assuming that cell phones possess unique attributes that we must consider as part of our analysis, none of those attributes are present in this case. Though we do not know the storage capacity of Wurie's cell phone, we know that the police did not browse through voluminous data in search of general evidence. Nor did they search the "cloud,"¹⁴ or other applications containing particularly sensitive information. Instead, they conducted a focused and limited search of Wurie's electronic call log. If the information that they sought had been written on a piece of paper, as opposed to stored electronically, there would be no question that the police acted constitutionally, so I see no reason to hold otherwise in this case. The constitutionality of a search cannot turn solely on whether the information is written in ink or displayed electronically.

The issue of warrantless cell phone searches has come before a number of circuits. *E.g.*, *Flores-Lopez*, 670 F.3d at 803–10; *United States v. Curtis*, 635 F.3d 704, 712 (5th Cir.2011); *Silvan W. v. Briggs*, 309 F. App'x 216, 225 (10th Cir.2009) (unpublished); *United States v. Murphy*, 552 F.3d 405, 411 (4th Cir.2009). None of them have adopted the majority's categorical bar on warrantless cell phone searches. Instead, they unanimously have concluded that the cell phone searches before them did not violate the Fourth Amendment.

I reach the same conclusion here. Wurie's cell phone was on his person at the time of the arrest. The information that the police looked at was of a character that we have previously held searchable during a custodial arrest. Wurie has made no convincing argument for why this search is any different than the search for phone numbers kept in a wallet or an address book. Thus, I see no reason to look for complications where none exist; Wurie has not shown a violation of his Fourth Amendment rights.

In my view, there is another rationale, apparent from the record, for upholding this search: the risk that others might have destroyed evidence after Wurie did not answer his phone. Wurie received repeated calls from "my house" in the span of a few minutes after his arrest. His failure to answer these phone calls could have alerted Wurie's confederates to his arrest, prompting them to destroy further evidence of his crimes. The majority asserts that this scenario would be present "in almost every instance of a custodial arrest," giving police an ever-ready justification to search cell phones. *Supra* at 23 n. 11. On the contrary, the justification is based on the specific facts of this case. The fact that "my house" repeatedly called Wurie's cell phone provided an objective basis for enhanced concern that evidence might be destroyed and thus gave the police a valid reason to inspect the phone. See *United States v.*

Chimel, 395 U.S. 752, 762–63, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969).

This additional reason for affirmance is not a novel one. *United States v. Gomez*, 807 F.Supp.2d 1134 (S.D.Fla.2011), presents a comparable example. In that case, police officers, after observing multiple phone calls from the same number to an arrested drug dealer’s cell phone, first answered the ringing cell phone and thereafter communicated to the caller via text message while posing as the arrestee, which led to the discovery of additional evidence. *Id.* at 1139. The district court denied a motion to suppress this evidence, holding the police acted according to “the exigencies commensurate with the Defendant’s ringing cell phone.” *Id.* at 1152; *see also United States v. De La Paz*, 43 F.Supp.2d 370, 375–76 (S.D.N.Y.1999) (admitting evidence—under the exigent circumstances exception—obtained when the police answered an arrestee’s cell phone and heard multiple callers identify the arrestee by his drug dealer moniker). The police action in this case is analogous—arguably less invasive—and a further reason why Wurie’s constitutional challenge founders on the specific facts of this case.

*16 Granted, my fact-specific view does not comport with the all-or-nothing approach adopted by the majority and some state courts, *see Smallwood v. State*, No. SC11–1130, 2013 WL 1830961 (Fla. May 2, 2013); *State v. Smith*, 124 Ohio St.3d 163, 920 N.E.2d 949 (Ohio 2009). But I find the competing rationale unpersuasive.¹⁵ Most pointedly, for the reasons explained above, Wurie himself suffered no constitutional violation during the search. If we are to fashion a rule, it cannot elide the facts before us. “The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case.” *Sibron v. New York*, 392 U.S. 40, 59 (1968). Yet the competing analysis focuses on hypothetical searches that have not emerged in any case or controversy before this court. Those scenarios may one day form the basis of our reasoning in another case, but they cannot govern our analysis of Wurie’s claim.

The majority gets around this problem by requiring the government to “demonstrate that warrantless cell phone searches, as a category, fall within the boundaries laid out in *Chimel*.” *Supra* at 16. It cites *United States v. Chadwick*, 433 U.S. 1, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991), and *Arizona v. Gant*, 556 U.S. 332, 129 S.Ct. 1710, 173 L.Ed.2d 485 (2009), to support this approach. The Supreme Court did hold on those two occasions, neither of which involved the search of items held by the arrestee, that certain types of searches require a warrant because they lack any *Chimel* justification. But the Supreme Court has not extrapolated from those cases a general rule that the government justify each category of searches under *Chimel*, nor a requirement that the appellate courts conduct

this sort of analysis.

Indeed, if the Supreme Court wishes us to look at searches incident to arrest on a categorical basis, it is curious that the Court has offered absolutely no framework for defining what constitutes a distinct category. Each arrest has its own nuances and variations, from the item searched (as in this case) to the officer’s control over it (as was the case in *Chadwick*), and there could be infinite distinct categories of searches based on these variations. Yet no relevant criteria are articulated for establishing these categories. That is not a good way to impose this new paradigm, under which every arrestee is now invited to argue that his search falls into some distinct category and therefore must be justified under *Chimel*.

Thus, either we are drastically altering the holding in *United States v. Robinson*, 414 U.S. 218 (1973), by forcing the government to provide a *Chimel* rationale for practically every search, or we are putting ourselves in the position of deciding, without any conceptual basis, which searches are part of a distinct “category” and which are not. This runs the risk of spreading confusion in the law enforcement community and multiplying, rather than limiting, litigation pertaining to these searches.

*17 It is argued that the categorical approach flows from the Supreme Court’s opinion in *Gant*, which reaffirmed “the fundamental principles established in the *Chimel* case regarding the basic scope of searches incident to lawful custodial arrests.” *Gant*, 556 U.S. at 343 (quoting *New York v. Belton*, 453 U.S. 454, 460, 101 S.Ct. 2860, 69 L.Ed.2d 768 n.3 (1981)). *Gant* did take a categorical, *Chimel*-based approach to the search in question, but its usefulness for our analysis should not be overstated.

As the government points out, the Supreme Court cases treat searches of the arrestee and the items on the arrestee—as is the case here—as either not subject to the *Chimel* analysis, or at a least subject to a lower level of *Chimel* scrutiny. These cases, unlike *Chimel* and *Gant*, are on point with Wurie’s case, and we are not free to disregard them in favor of the principles enunciated in *Gant*. As an inferior court, we are cautioned against “conclud[ing] [that] more recent cases have, by implication, overruled an earlier precedent.... [I]f 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.” *Agostini v. Felton*, 521 U.S. 203, 237, 117 S.Ct. 1997, 138 L.Ed.2d 391 (1997) (internal quotation marks and alterations omitted).

In *Robinson*, the Supreme Court drew a sharp distinction between two types of searches pursuant to an arrest: searches of the arrestee and searches of the area within his control. “The validity of the search of a person incident to a lawful arrest has been regarded as settled from its first

enunciation, and has remained virtually unchallenged.... Throughout the series of cases in which the Court has addressed the second [type of search,] no doubt has been expressed as to the unqualified authority of the arresting authority to search the person of the arrestee.” *Robinson*, 414 U.S. at 224–25. The Supreme Court did state that the basis of this authority is “the need to disarm and to discover evidence,” *id.* at 235, but in the next sentence clarified that “[a] custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification,” *id.*

Indeed, the Court could not rely on a *Chimel* justification in *Robinson*, as the arresting officer conceded that he “did not in fact believe that the object in [Robinson]’s coat pocket was a weapon” and that he gave no thought to the destruction of evidence either. *Id.* at 251 (Marshall, J., dissenting) (quoting the arresting officer’s testimony: “I didn’t think about what I was looking for. I just searched him.”). *Robinson* may not have rejected *Chimel* in the context of searches of an arrestee and items on the arrestee, but it did establish that these searches differ from other types of searches incident to arrest.

*18 The Supreme Court reiterated *Robinson*’s holding in *United States v. Edwards*, 415 U.S. 800, 94 S.Ct. 1234, 39 L.Ed.2d 771 (1974), in which the Court upheld the search and seizure of an arrestee’s clothing ten hours after he was arrested. While most of the analysis focused on the timing of the search, the opinion assumed that law enforcement could “tak[e] from [the arrestee] the effects in his immediate possession that constituted evidence of crime. This was and is a normal incident of a custodial arrest....” *Id.* at 805; see also *id.* at 803 (“[B]oth the person and the property in his immediate possession may be searched at the station house after the arrest has occurred....”). Once again, the Supreme Court was unconcerned with the existence or nonexistence of *Chimel* rationales. The opinion barely discussed them, and the government did not seek to prove that they were present. *Id.* at 811 n. 3 (Stewart, J., dissenting) (“No claim is made that the police feared that Edwards either possessed a weapon or was planning to destroy the paint chips on his clothing. Indeed, the Government has not even suggested that he was aware of the presence of the paint chips on his clothing.”).

Even in *Chadwick*, where the Supreme Court did require the police to obtain a warrant for a category of searches, it continued to treat the search of an arrestee and items immediately associated with him as independently justified by “reduced expectations of privacy caused by the arrest.” *Chadwick*, 433 U.S. at 16 n. 10. Thus, the holding in *Chadwick* applied only to “luggage or other personal property not immediately associated with the person of the arrestee.” *Id.* at 15 (emphasis added). These cases, taken together, establish that items immediately associated with the arrestee—as a category—may be searched without any *Chimel* justification. The majority seeks a bright-line rule

to govern cell phone searches, but denies the fact that such a rule—covering all items on the arrestee’s person—already exists.

But even if searches of items on an arrestee required *Chimel* justifications, I cannot see why cell phones fail to meet this standard if wallets, cigarette packages, address books, briefcases, and purses do. The attempt is made to distinguish cell phones from these other items, but those distinctions do not hold up under scrutiny.

One argument is that these other items, unlike cell phones, all theoretically could contain “destructible” evidence, which justifies examining them. But the evidence in a cell phone is just as destructible as the evidence in a wallet: with the press of a few buttons, accomplished even remotely, cell phones can wipe themselves clean of data. Any claim that the information is not destructible strikes me as simply wrong.¹⁶ Perhaps what is meant is that the cell phone data is no longer destructible once it is within the exclusive control of law enforcement officers. But even accepting that the likelihood of destruction is reduced to almost zero once the officers are in control of a cell phone, this is equally true of cigarette packages, wallets, address books, and briefcases. Drugs do not disappear into thin air; weapons do not flee of their own accord. If that is the basis for the reasoning, then a warrant should be required before searching any object within the exclusive control of the police. I do not think that the majority is arguing for this rule, but I cannot see any other outcome under its analysis. Ironically, cell phones arguably pose a greater *Chimel* risk than most other items because, unlike cigarette packages or wallets, the evidence contained in cell phones remains destructible even after the police have assumed exclusive control of the phone via remote wiping.¹⁷

*19 Another argument is that because cell phone searches are not “self-limiting,” they always require a warrant. The majority does not precisely define the term “self-limiting,” but I gather that it refers to the danger that cell phones, because of their vast storage capabilities, are susceptible to “general, evidence-gathering searches.” *Supra* at 21 (citing *Thornton v. United States*, 541 U.S. 615, 632, 124 S.Ct. 2127, 158 L.Ed.2d 905 (2004) (Scalia, J., concurring)). As an initial matter, this has never been the focus of Supreme Court cases discussing the search incident to arrest exception for items immediately associated with the arrestee.¹⁸ Thus, I am reluctant to give it much weight in assessing Wurie’s constitutional claim.

Nonetheless, if we are concerned that police officers will exceed the limits of constitutional behavior while searching cell phones, then we should define those limits so that police can perform their job both effectively and constitutionally. Instead, the majority has lumped all cell phone searches together, even while perhaps acknowledging that its broad rule may prohibit some otherwise constitutional searches. *Supra* at 28 (“Thus, while the search of Wurie’s call log was less invasive than

a search of text messages, emails, or photographs, it is necessary for all warrantless cell phone data searches to be governed by the same rule.”). But this need not be the solution. We can draw the appropriate line for cell phone searches, just as we have done in other contexts. For instance, a body search, like a cell phone search, is not inherently self-limiting. A frisk can lead to a strip search, which can lead to a cavity search, which can lead to x-ray scanning. But this parade of horrors has not come to pass because we have established the constitutional line, and conscientious law enforcement officers have largely adhered to it. See *Swain v. Spinney*, 117 F.3d 1, 5–9 (1st Cir.1997) (holding that police officers may not conduct a strip search of an arrestee incident to the arrest); see also *Roberts v. Rhode Island*, 239 F.3d 107, 113 (1st Cir.2001) (holding that indiscriminate strip searches of misdemeanor arrestees during administrative processing at a detention facility violated the Fourth Amendment). The majority has instead chosen to ignore this option in favor of a rule that sweeps too far.

Still, I share many of the majority’s concerns about the privacy interests at stake in cell phone searches. While the warrantless search of Wurie’s phone fits within one of our “specifically established and well-delineated exceptions,” *United States v. Camacho*, 661 F.3d 718, 724 (1st Cir.2011) (citations omitted) (internal quotation marks omitted), due to the rapid technological development of cell phones and their increasing prevalence in society, cell phone searches do pose a risk of depriving arrestees of their protection against unlawful searches and seizures. There must be an outer limit to their legality.

*20 In *Flores–Lopez*, Judge Posner suggested that courts should balance the need to search a cell phone against the privacy interests at stake.

[E]ven when the risk either to the police officers or to the existence of the evidence is negligible, the search is allowed, provided it’s no more invasive than, say, a frisk, or the search of a conventional container, such as Robinson’s cigarette pack, in which heroin was found. If instead of a frisk it’s a strip search, the risk to the officers’ safety or to the preservation of evidence of crime must be greater to justify the search.

Flores–Lopez, 670 F.3d at 809 (citations omitted). I believe that cell phone searches should follow this formula. That is not to say that the police must prove a risk to officer safety or destruction of evidence in every case. There is, inherent in every custodial arrest, some minimal risk to officer safety and destruction of evidence. Moreover, *Chadwick* states that the arrest itself diminishes the arrestee’s privacy rights over items “immediately

associated” with the arrestee. *Chadwick*, 433 U.S. at 15. But the invasion of the arrestee’s privacy should be proportional to the justification for the warrantless search.

This approach respects “the Fourth Amendment’s general proscription against unreasonable searches and seizures.” *Edwards*, 415 U.S. at 808 n. 9 (citations omitted) (internal quotation marks omitted). It is also consistent with the core reasonable limit that has been acknowledged in *Robinson*, which does not permit “extreme or patently abusive” searches, *Robinson*, 414 U.S. at 236, and its offspring, see, e.g., *Swain*, 117 F.3d at 5–9. The Supreme Court’s recent opinion in *Missouri v. McNeely*, — U.S. —, 133 S.Ct. 1552, — L.Ed.2d — (2013), shows that the reasonableness inquiry remains a touchstone of Fourth Amendment analysis. The Court held that, in the context of warrantless blood tests of drunk drivers, courts had to look to “the totality of the circumstances” to determine whether police officers’ reliance on the exigency exception was reasonable. *Id.* at 1558–63.

Similarly, while *Robinson*’s principles generally authorize cell phone searches, and certainly encompass the search in this case, there are reasonable limits to *Robinson* that we should not hesitate to enforce, especially in light of a cell phone’s unique technological capabilities, for “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” *Kyllo v. United States*, 533 U.S. 27, 33–34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

I find helpful the analysis in *United States v. Cotterman*, 709 F.3d 952 (9th Cir.2013) (en banc). In that case, the Ninth Circuit determined whether a warrantless forensic examination of a laptop computer during a border search violated the Fourth Amendment. The court conducted a reasonableness analysis, balancing the privacy interests of the individual against the sovereign’s interests in policing its borders. *Id.* at 960. It stated that, had the search only involved “turn[ing] on the devices and open[ing] and view[ing] image files ... we would be inclined to conclude it was reasonable.” *Id.* at 960–61. However, the invasive nature of the forensics examination, which included restoring previously deleted files, as well as “the uniquely sensitive nature of data on electronic devices,” *id.* at 966, convinced the court that the forensics examination was an unreasonable border search absent a showing of reasonable suspicion, *id.* at 968.

*21 A similar reasonableness analysis would restrain certain types of cell phone searches under *Robinson*. The inherent risks in a custodial arrest, along with the reduced privacy expectations of the arrestee, must be balanced against the wide range of private data available in a cell phone. But ultimately the question of what constitutes an unreasonable cell phone search should be left for another day. The majority has outlined some of the more troubling privacy invasions that could occur during a warrantless

search. So long as they remain in the hypothetical realm, I think it premature to draw the line. Suffice it to say that, for the reasons I have stated, the search in this case fell on the constitutional side of that line.¹⁹

I respectfully dissent.

Footnotes

- 1 On appeal, Wurie does not challenge the seizure of his phone, and he concedes that, under the plain view exception, see *United States v. Paneto*, 661 F.3d 709, 713–14 (1st Cir.2011), the officers were entitled to take notice of any information that was visible to them on the outside of the phone and on its screen (including, in this case, the incoming calls from “my house”).
- 2 The Court also concluded, “[a]lthough it does not follow from *Chimel*,” that “circumstances unique to the vehicle context justify a search incident to a lawful arrest when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.” *Gant*, 556 U.S. at 343 (citation and internal quotation marks omitted).
- 3 The dissent, advocating a case-by-case, fact-specific approach, relies on *Missouri v. McNeely*, — U.S. —, 133 S.Ct. 1552, — L.Ed.2d — (2013), which rejected a *per se* rule for warrantless blood tests of drunk drivers. But *McNeely* involved the exigent circumstances exception to the warrant requirement, and courts must “evaluate each case of alleged exigency based ‘on its own facts and circumstances.’” *Id.* at 1559 (quoting *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357, 51 S.Ct. 153, 75 L.Ed. 374 (1931)). The Supreme Court explicitly distinguished the exigency exception, which “naturally calls for a case-specific inquiry,” from the search-incident-to-arrest exception, which “appl[ies] categorically.” *Id.* at 1559 n. 3.
- 4 It is worth noting three things that the government is not arguing in this case. First, it does not challenge the district court’s finding that what occurred here was a Fourth Amendment search. See *Wurie*, 612 F.Supp.2d at 109 (“It seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone.”). Second, the government does not suggest that Wurie’s expectation of privacy was in any way reduced because his phone was apparently not password-protected. Third, it does not claim that this was an inventory search. See *Illinois v. Lafayette*, 462 U.S. 640, 103 S.Ct. 2605, 77 L.Ed.2d 65 (1983).
- 5 It is not clear from the record how much time passed between Wurie’s arrest and the search of his cell phone at the station house. Nonetheless, because Wurie has not raised the argument, we need not decide whether the government is correct that, under *Edwards*, the search here was “incident to” Wurie’s arrest, despite the delay. See 415 U.S. at 803 (“[S]earches and seizures that could be made on the spot at the time of arrest may legally be conducted later when the accused arrives at the place of detention.”).
- 6 The government has also suggested a more limited way for us to resolve this case: by holding that this particular search was lawful under *United States v. Sheehan*, 583 F.2d 30 (1st Cir.1978). But *Sheehan* was a seizure case, not a search case, and “[i]t is extremely important to distinguish a *search* of the person from a *seizure* of objects found in that search.” 3 Wayne R. LaFare, *Search & Seizure* § 5.2(j), at 185 (5th ed.2012). The defendant in *Sheehan* conceded that “the search of his wallet was legal”; he challenged only the seizure of a list of names and telephone numbers in the wallet. 583 F.2d at 31. Because the list was not “a fruit, instrumentality, or contraband, probative of a crime,” but rather “mere evidence,” we analyzed whether probable cause existed to support the seizure. *Id.* (citing *Warden v. Hayden*, 387 U.S. 294, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967)). The lawfulness of a search of the person incident to arrest, however, does not turn on the likelihood that evidence of the crime of arrest will be discovered. See *Robinson*, 414 U.S. at 234. The Supreme Court did articulate such a rule in *Gant* but limited it to the vehicle context. 556 U.S. at 343.
- 7 See, e.g., *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir.1996) (pager); *United States v. Uricoechea-Casallas*, 946 F.2d 162, 166 (1st Cir.1991) (wallet); *United States v. Holzman*, 871 F.2d 1496, 1504–05 (9th Cir.1989) (address book), *overruled on other grounds by Horton v. California*, 496 U.S. 128, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990); *United States v. Burnette*, 698 F.2d 1038, 1049 (9th Cir.1983) (purse); *United States v. Eatherton*, 519 F.2d 603, 610–11 (1st Cir.1975) (briefcase).
- 8 We are also cognizant of the fact that “[m]obile devices increasingly store personal user data in the cloud instead of on the device itself,” which “allows the data to be accessed from multiple devices and provides backups.” James E. Cabral et al., *Using Technology to Enhance Access to Justice*, 26 Harv. J.L. & Tech. 241, 268 (2012). Though the government insisted at oral argument that it was not seeking a rule that would permit access to information stored in the cloud, we believe that it may soon be impossible for an officer to avoid accessing such information during the search of a cell phone or other electronic device, which could have additional privacy implications. See *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir.2013) (en banc) (“With the ubiquity of cloud computing, the government’s reach into private data becomes even more problematic.”).
- 9 For cases demonstrating the potential for abuse of private information contained in a modern cell phone, see, for example, *Schlossberg v. Solesbee*, 844 F.Supp.2d 1165 (D.Or.2012), and *Newhard v. Borders*, 649 F.Supp.2d 440 (W.D.Va.2009).
- 10 The record here does not reveal the storage capacity of Wurie’s cell phone, but that is of no significance, for two reasons. First, “[e]ven the dumbest of modern cell phones gives the user access to large stores of information.” *Flores-Lopez*, 670 F.3d at 806. Second, neither party has suggested that our holding today should turn on the specific features of Wurie’s cell phone, and we find such a rule unworkable in any event. See *Thornton*, 541 U.S. at 623; *Murphy*, 552 F.3d at 411 (“[T]o require police officers to ascertain the storage capacity of a cell phone before conducting a search would simply be an unworkable and unreasonable rule.”).

- 11 The government and our dissenting colleague have also suggested that Wurie’s failure to answer calls or to return home after the drug deal might have alerted others to the fact of his arrest and caused *them* to destroy or conceal evidence (presumably the drug stash later discovered at his home). That is mere speculation, and it is also a possibility present in almost every instance of a custodial arrest; we do not think that such concerns should always justify the search of a cell phone or other electronic device. Furthermore, the risk of destruction, as we understand it, attaches to the evidence that the arrestee is actually carrying on his person—not to evidence being held or guarded elsewhere by a co-conspirator. See *Gant*, 556 U.S. at 339 (describing the need to safeguard “any evidence of the offense of arrest that an *arrestee* might conceal or destroy” (emphasis added)); *Chimel*, 395 U.S. at 763 (“In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence *on the arrestee’s person* in order to prevent its concealment or destruction.” (emphasis added)).
- 12 We acknowledge that we may have to revisit this issue in the years to come, if further changes in technology cause warrantless cell phone data searches to become necessary under one or both of the *Chimel* rationales.
- 13 The government invokes *United States v. Grupee*, 682 F.3d 143, 148 (1st Cir.2012), in which we addressed the good-faith exception despite the fact that the district court had not done so in its opinion. However, the record in that case reveals that the government had raised the good-faith exception below; the district court simply did not reach it.
- 14 The government does not claim a right to conduct warrantless searches of information in the cloud. This is an important concession, for it suggests that the government accepts that there are limits to searches of items found on custodial arrestees. I discuss my view of those limits later.
- 15 The insistence on a bright-line rule contrasts with the recent Supreme Court opinion in *Missouri v. McNeely*, — U.S. —, 133 S.Ct. 1552, — L.Ed.2d — (2013), which rejected a bright line rule and instead relied on a totality of the circumstances analysis for warrantless blood tests of drunk drivers, *id.* at 1564 (“[A] case-by-case approach is hardly unique within our Fourth Amendment jurisprudence. Numerous police actions are judged based on fact-intensive, totality of the circumstances analyses rather than according to categorical rules, including in situations that are [] likely to require police officers to make difficult split-second judgments.”). While it can be argued that a bright-line rule is preferable, it cannot be claimed that such a rule is necessary.
- 16 The term “destructible” evidence is perhaps intended to mean “physical” or “tangible” evidence. That distinction does not fly, for two reasons. First, just because evidence is intangible does not make it indestructible. As noted, an arrestee can delete data just as easily as he can discard drugs. Second, any distinction based on the difference between tangible and intangible evidence ignores the fact that we have upheld the warrantless search of intangible information during a custodial arrest. *United States v. Sheehan*, 583 F.2d 30, 31 (1st Cir.1978).
- 17 It is also half-heartedly suggested that containers that hold physical objects, unlike cell phones, pose a risk to officer safety. “[T]he officer who conducted the search in *Robinson* had no idea what he might find in the cigarette pack, which therefore posed a safety risk.” *Supra* at 23. I find it hard to believe that a reasonable police officer is more justified in remaining on guard against booby-trapped cigarette packs and wallets in the line of duty, than she is against sophisticated electronic devices.
- 18 For instance, in *Robinson*, the police conducted their search pursuant to a standard operating procedure of the police department, which trained officers to carry out a full field search after any arrest. *United States v. Robinson*, 414 U.S. 218, 221 n. 2 (1973). That entailed “completely search[ing] the individual and inspect[ing] areas such as behind the collar, underneath the collar [sic], the waistband of the trousers, the cuffs, the socks and shoes ... [as well as] examin[ing] the contents of all the pockets’ [sic] of the arrestee....” *Id.* (internal quotation marks omitted). Given that Robinson was arrested for a traffic violation, and that the arresting officer conceded that he felt no personal risk during the arrest, the only conceivable purpose for this search was to gather general evidence.
- 19 If there had been a constitutional violation here, the application of the good faith exception would present an interesting question. Because I would find no constitutional violation, however, I do not address the government’s good faith exception argument. But I disagree with the majority’s decision not to consider the good faith exception to the extent that it based that decision on the government’s failure to invoke the exception before the district court. We may affirm on any basis apparent from the record. See *United States v. Sanchez*, 612 F.3d 1, 4 (1st Cir.2010). Of course, if the record is underdeveloped because the appellee did not present the issue to the district court, the appellee must suffer the consequences. See *Giordenello v. United States*, 357 U.S. 480, 488, 78 S.Ct. 1245, 2 L.Ed.2d 1503 (1958) (“To permit the Government to inject its new theory into the case at this stage would unfairly deprive petitioner of an adequate opportunity to respond. This is so because in the District Court petitioner, being entitled to assume that the warrant constituted the only purported justification for the arrest, had no reason to ... adduce evidence of his own to rebut the contentions that the Government makes here for the first time.”).
- Such is not the case here. The good faith exception is merely an extension of the government’s main argument that this search complied with existing law. The factual record appears sufficiently developed to allow our consideration of this argument, and the government, by raising it in its brief on appeal, gave Wurie the opportunity to respond in his reply brief. Thus, I would not bypass this argument merely because the government first raised it on appeal. See *Jordan v. U.S. Dep’t of Justice*, 668 F.3d 1188, 1200 (10th Cir.2011) (holding that an appellate court may affirm on an alternate ground “provided that the alternate ground is within our power to formulate and the opposing party has had a fair chance to address it”) (citations omitted) (internal quotation marks and alterations omitted).