Saint Louis University Law Journal

Volume 61
Number 2 *(Winter 2017)*

Article 3

2017

Applying the Digital Search Incident to Arrest Doctrine to Predigital Content

Eugene R. Milhizer
Ave Maria School of Law, ermilhizer@avemarialaw.edu

APPLYING THE DIGITAL SEARCH INCIDENT TO ARREST DOCTRINE TO PREDIGITAL CONTENT

EUGENE R. MILHIZER*

"*Before you become too entranced with gorgeous gadgets and mesmerizing video displays, let me remind you that information is not knowledge, knowledge is not wisdom, and wisdom is not foresight. Each grows out of the other, and we need them all.*"[1]

"*A foolish consistency is the hobgoblin of little minds.*"[2]

INTRODUCTION

Stable law has many benefits. Stability can indicate that the law is morally grounded and socially useful. The law ought to be stable insofar as it reflects and implements transcendent and immutable values. Stable law can bind generations to enduring norms.[3] Stability can also lead to widespread knowledge and understanding of the law, which in turn affords people the capacity to conform their conduct to its precepts.[4] Moreover, stability suggests

* Dean Emeritus and Professor of Law, Ave Maria School of Law. Dean Emeritus Milhizer served as President/Acting President and Dean/Acting Dean of Ave Maria School of Law from 2008–2014. The author would like to thank his friend, John Willette, for his advice and counsel regarding technology. The author would also like to thank his research assistant, Andrea Phillips, for her outstanding work in the preparation of this article.

1. CHARLES E. LATHROP, THE LITERARY SPY: THE ULTIMATE SOURCE FOR QUOTATIONS ON ESPIONAGE & INTELLIGENCE 10 (2014) (quoting Sir Arthur C. Clarke).

2. RALPH WALDO EMERSON, *Self-Reliance* (1841), *reprinted in* OXFORD DICTIONARY OF QUOTATIONS § 5, at 307 (Elizabeth Knowles 6th ed., Oxford University Press 2004).

3. Of course, stability of the law is no guarantee that the law is moral. Slavery, for example, was legal in many American states for generations. Its ultimate abolition is in large part attributable to the immorality of the institution. *See* 1 OHIO ANTI-SLAVERY SOC'Y, NARRATIVE OF THE LATE RIOTOUS PROCEEDINGS AGAINST THE LIBERTY OF THE PRESS, IN CINCINNATI 3 (Cincinnati 1836); 1 R. GUY M'CLELLAN, REPUBLICANISM IN AMERICA: A HISTORY OF THE COLONIAL AND REPUBLICAN GOVERNMENTS OF THE UNITED STATES OF AMERICA FROM THE YEAR 1607 TO THE YEAR 1869 72 (R.J. Trumbull & Co. 1869); 2 CARL SCHURZ, HENRY CLAY: AMERICAN STATESMEN 70 (John T. Morse, Jr., ed., Boston, Mass. Houghton Mifflin 1897); 1 FRANCIS NEWTON THORPE, A SHORT CONSTITUTIONAL HISTORY THE UNITED STATES 190 (Boston, Little, Brown, and Co. 1904).

4. Vasquez v. Hillery, 474 U.S. 254, 265–66 (1986) ("[T]he important doctrine of stare decisis, the means by which we ensure that the law will not merely change erratically, but will

that the law is practical and perhaps wise. If it were otherwise, one might presume that the law would be revoked or modified, especially in a representative democracy. Sometimes, however, stable law is simply stagnant law, whose constancy can be attributed to nothing grander than inertia[5] or a lack of consensus for change.[6]

The law must also be dynamic. It does not exist in a vacuum but rather reacts and adapts to the changing social, economic and cultural circumstances. Technology is perhaps the most sweeping and pervasive agent of change. It is rapid, constant, and amoral. It can magnify good or evil. It can be unfathomably lethal or life-saving and medicinal. It relentlessly advances like an accelerating drumbeat, which leaves no aspect of human life untouched.[7] It can displace persons, occupations, and whole societies. Technological development is always destabilizing.

The tension between the stability of the law and the destabilizing impact of technology has been repeatedly played out in American courtrooms, particularly with regard to the Supreme Court's Fourth Amendment jurisprudence.[8] The results have been inconsistent and varied. For example, when listening devices became more sophisticated, the Court abandoned the trespass theory for searches in favor of an interest-based rationale.[9] Thermal

develop in a principled and intelligible fashion. That doctrine permits society to presume that bedrock principles are founded in the law rather than in the proclivities of individuals, and thereby contributes to the integrity of our constitutional system of government, both in appearance and in fact.").

5. *Law of Motion*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/law%20of%20motion [http://perma.cc/3ZFJ-XLYM] ("a statement in dynamics: a body at rest remains at rest and a body in motion remains in uniform motion in a straight line unless acted upon by an external force—called also Newton's first law of motion").

6. For example, most people think the current taxing policies should be fundamentally changed. *See* Rodney P. Mock & Nancy E. Shurtz, *The TurboTax Defense*, 15 FLA. TAX REV. 443, 443 (2014) ("[T]he current informal partnership between the software companies and the IRS should be critically assessed to address advances in software technology and increasing taxpayer reliance on commercial tax preparation software."). The failure to implement changes is largely the result of lack of consensus in support of any particular change. *See* Holly Doremus, *Takings and Transitions*, 19 J. LAND USE & ENVTL. LAW 1, 21–22 (2003) ("In the real world, policy inertia is likely to dominate policy impulsiveness, and adaptive plasticity is likely to prove elusive. Experience suggests that it is extraordinarily difficult to change the law. Law and policy choices often seem to hang on long after their original purpose has evaporated.").

7. *See, e.g.*, Bradley H. Leiber, *Applying Ethics Rules to Rapidly Changing Technology: The D.C. Bar's Approach to Metadata*, 21 GEO. J. LEGAL ETHICS 893 (2008).

8. U.S. CONST. amend. IV.

9. *Compare* Olmstead v. United States, 277 U.S. 438, 466 (1928) (applying a physical trespass rationale to determine whether the government's activity constitutes a search), *with* Katz v. United States, 389 U.S. 347, 353 (1967) (applying an expectation of privacy rationale to determine whether the government's activity constitutes a search); United States v. Jones, 132 S.

imaging devices caused the Court to further refine its approach for searches and introduced the term "not in general public use" to the Fourth Amendment lexicon.[10] Electronically transmitted conversations,[11] pen registers,[12] and overflights[13] were each considered and addressed. More recently, the Court took up the use of global positioning system (GPS) devices and beepers to track a suspect's movements.[14] On the horizon is the use of drones,[15] cell tower pinging,[16] metadata gathering,[17] through-the-wall technologies,[18] and other capabilities currently under development or not yet imagined.[19]

Ct. 945, 952 (2012) (discussing how the "reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test") (emphasis added).

10. Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."); *see* State v. Davis, 360 P.3d 1161, 1175 (N.M. 2015) (Chavez, J., specially concurring) (introducing the alternate phrasing "commercially available technology").

11. United States v. White, 401 U.S. 745, 751 (1971) ("If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations.").

12. Smith v. Maryland, 442 U.S. 735, 736, 739–46 (1979) ("The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

13. Florida v. Riley, 488 U.S. 445, 447–52 (1989) (allowing police to inspect a greenhouse from a helicopter without a warrant); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.").

14. *Jones*, 132 S. Ct. at 949–52 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'").

15. *See* United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *29 n.8 (E.D. Wash. Dec. 15, 2014); Y. Douglas Yang, *Big Brother's Grown Wings: The Domestic Proliferation of Drone Surveillance and the Law's Response*, 23 B.U. PUB. INT. L.J. 343, 344 (2014).

16. *See* United States v. Skinner, 690 F.3d 772, 776–81 (6th Cir. 2012); United States v. Wilford, 961 F. Supp. 2d 740, 772–73 (D. Md. 2013); Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under Fourth Amendment*, 92 A.L.R. Fed. 2d 1 (2015).

17. *See* United States v. Saboonchi, 990 F. Supp. 2d 536, 564–70 (D. Md. 2014); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532–33 (2005).

18. *See* United States v. Thompson, 811 F.3d 944, 949–50 (7th Cir. 2016); Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1410–11 (2004).

19. Suppose police obtained a new technology that allowed for the searching of a suspect's thoughts in the same manner as they can now remotely measure heat emanating from a distant source. The information thus gathered would be helpful, and in some cases even indispensable, for the prevention and investigation of crimes. The use of such a device would also have obvious Fourth Amendment implications. For example, would its use constitute a search? If so, would a

In *Riley v. California*, the Supreme Court addressed one of the most influential and ubiquitous technological devices of the early 21st century, the cell phone.[20] In *Riley*, the Court modified the long-standing search incident to lawful arrest (hereinafter "SILA") exception to the warrant requirement by providing heightened protection to the digital contents of a cell phone. This article explores whether *Riley*'s reasoning should lead to the same, enhanced protection for certain kinds of predigital information.[21] Part I of this article explains the development and rationale for the Court's SILA exception. Part II reviews the *Riley* decision and its reasoning. Part III considers whether the enhanced protection *Riley* affords to digital information stored in a cell phone should likewise be accorded to some types of predigital information encountered during a SILA. It concludes that some predigital information is deserving of the same enhanced protection that *Riley* grants to a cell phone's digital contents.

I. HISTORY OF THE SILA EXCEPTION

The Fourth Amendment is composed of two clauses: the reasonableness clause[22] and the warrant clause.[23] Whether the Framers intended the two clauses to operate independently (i.e., the reasonableness of a search can be

warrant be required? Would the use of such a device be deemed to be so intrusive as to be unreasonable regardless of the showing that the government might make in a particular case? What if this technology becomes commercially available? These and other issues would ultimately need to be addressed by the courts.

20. 134 S. Ct. 2473, 2491 (2014) ("Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."). According to the International Telecommunication Union's report in 2015, "[t]he proportion of the global population covered by mobile-cellular networks is now over 95 per cent," and "the number of mobile-cellular subscriptions has quintupled" since 2005. INTERNATIONAL TELECOMMUNICATION UNION, MEASURING THE INFORMATION SOCIETY REPORT 2015, at 2 (2015). "[T]he number of mobile-cellular subscriptions approaches 7.3 billion and mobile population coverage reaches close to 95 per cent globally." *Id.* at 100.

21. "Predigital" information, as used in this article, refers to information that could be created and stored by methods that predate the creation of "digital" information. Justice Alito used the term "predigital" in his separate opinion in *Riley*, 134 S. Ct. at 2496 (Alito, J., concurring in part, concurring in the judgment). The terms "digital" and "predigital" are discussed in more detail, *infra* notes 136–38 and accompanying text.

22. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

23. U.S. CONST. amend. IV ("[A]nd 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.").

evaluated without reference to a warrant)[24] or inter-dependently (i.e., for a search to be reasonable it must be based on a valid warrant)[25] has been the subject of a protracted debate,[26] with various Supreme Court justices over time acting as proponents for the opposing approaches.[27]

In the early years, the Court consistently held that a search had to be conducted "pursuant to a warrant or . . . fall within one of the exceptions to the warrant requirement."[28] This reasoning was forcefully reaffirmed by *Katz v. United States*[29] and its progeny, in which the Court shifted from a trespass theory to a privacy-interest approach for determining whether a government activity constituted a search.[30] Although recent Supreme Court cases may

24. TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION 46–47 (1969) (If you "have viewed the [F]ourth [A]mendment primarily as a requirement that searches be covered by warrants, [you] have stood the amendment on its head."); Akhil Redd Amar, *The Bill of Rights as a Constitution*, 100 YALE L.J. 1131, 1179 (1991) ("Searches without warrants are not presumptively illegitimate."); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 766–67 (1994) ("And this straightforward result is yet another signal that many of the most important searches and seizures can and must take place without warrants.").

25. United States v. Ventresca, 380 U.S. 102, 106–07 (1965) ("The fact that exceptions to the requirement that searches and seizures be undertaken only after obtaining a warrant are limited underscores the preference accorded police action taken under a warrant as against searches and seizures without one."); Phyllis T. Bookspan, *Reworking the Warrant Requirement: Resuscitating the Fourth Amendment*, 44 VAND. L. REV. 473, 514 (1991) ("The [F]ourth [A]mendment's warrant requirement is the only meaningful protection against unreasonable searches and seizures. The warrant requirement cannot be dispensed with; it must be revitalized."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 358 (1974) ("Under this theory, the Court has uniformly condemned searches and seizures made without a search warrant . . . .").

26. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 553 (1999).

27. *See* California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring in the judgment) (observing that the Court's Fourth Amendment "jurisprudence [has] lurched back and forth between imposing a categorical warrant requirement and looking to reasonableness alone.").

28. William W. Greenhalgh & Mark J. Yost, *In Defense of the "Per Se" Rule: Justice Stewart's Struggle to Preserve the Fourth Amendment's Warrant Clause*, 31 AM. CRIM. L. REV. 1013, 1041 (1994) ("A long line of cases from 1789–1958 recognized that for a search to be valid under the Fourth Amendment, that search must either be pursuant to a valid warrant or fall within one of the recognized exceptions to the warrant requirement.").

29. 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

30. Kyllo v. United States, 533 U.S. 27, 34 (2001) (following "[t]he *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable"); California v. Ciraolo, 476 U.S. 207, 211 (1986) ("*Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?"); Mancusi v. DeForte, 392 U.S. 364, 368 (1968) ("[T]he protection of the Amendment depends not upon a property right

portend a shift toward the primacy of the Reasonableness Clause,[31] the current status of the Court's decisional law can be fairly characterized as follows: for a search to be reasonable there is a presumptive requirement that it be conducted pursuant to a valid warrant,[32] which can be avoided only if the government's activity falls within the parameters of an explicitly delineated exception to the warrant requirement.[33] Put another way, the need for a warrant has become the "default position" when a warrant exception does not apply.[34]

---

in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion.").

31. *E.g.*, Wyoming v. Houghton, 526 U.S. 295, 299–300 (1999) (instructing that in evaluating the reasonableness of a search, the Court should look first to whether a particular action was regarded as unlawful under the common law and, second, whether it satisfies traditional standards of reasonableness); Florida v. Jimeno, 500 U.S. 248, 250 (1991) ("The touchstone of the Fourth Amendment is reasonableness."); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447, 455 (1990) (allowing a warrantless, suspicionless sobriety checkpoint on a highway based upon the special need of ending drunk driving); New Jersey v. T. L. O., 469 U.S. 325, 337, 340 (1985) (allowing the warrantless search of a student because "[a]lthough the underlying command of the Fourth Amendment is always that searches and seizures be reasonable, what is reasonable depends on the context within which a search takes place."); the Court famously upheld the *Terry* stop-and-frisk based upon reasonableness:

> [W]here a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous, where in the course of investigating this behavior he identifies himself as a policeman and makes reasonable inquiries, and where nothing in the initial stages of the encounter serves to dispel his reasonable fear for his own or others' safety, he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him. Such a search is a reasonable search under the Fourth Amendment, and any weapons seized may properly be introduced in evidence against the person from whom they were taken.

Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

32. Chimel v. California, 395 U.S. 752, 768 (1969) ("There was no constitutional justification, in the absence of a search warrant, for extending the search beyond that area. The scope of the search was, therefore, 'unreasonable' under the Fourth and Fourteenth Amendments, and the petitioner's conviction cannot stand."). Proponents of a presumptive warrant requirement commonly recite the following benefits of having police obtain a search warrant: (1) the judgment of a neutral and detached judicial officer regarding probable cause to search is often more accurate than the judgment of the police, who are motivated to investigate crime and catch criminals; (2) the risk of an unfounded intrusion upon privacy is reduced when a judicial officer makes the probable cause determination; and (3) even if the judicial officer rubber stamps the police request to search, a warrant ensures the police will not search without prior justification. *See* Johnson v. United States, 333 U.S. 10, 13, 14, 17 (1948).

33. Admittedly, this characterization of the Court's approach is a bit simplistic. *See, e.g.*, *Sitz*, 496 U.S. at 451–52, 455 (allowing a sobriety checkpoint, without individualized suspicion, in order to combat "the magnitude of the drunken driving problem" under a special needs exception); *Terry*, 392 U.S. at 10, 30 (allowing "stop and frisk[s]" when an officer has "reasonable grounds to believe that petitioner was armed and dangerous, and it was necessary for

One of the explicitly delineated exceptions to the warrant requirement involves searches incident to a lawful arrest. Under the SILA exception, a police officer who makes a lawful, custodial arrest[35] may conduct a contemporaneous,[36] warrantless search of the arrestee's person and the area within the arrestee's immediate control.[37] Search authority under the SILA exception extends to containers in the arrestee's possession and within his grabbing distance.[38] If the arrest occurs in a residence, the police may also conduct a warrantless search of "closets and other spaces immediately adjoining the place of arrest from which an attack could be immediately

the protection of himself and others to take swift measures to discover the true facts and neutralize the threat of harm if it materialized.").

34. JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE 198 (4th ed. 2006); *e.g.*, Arizona v. Gant, 556 U.S. 332, 343–44 (2009) (restraining the vehicle exception to the warrant requirement to circumstances when officer could have "reasonably have believed either that [the occupant] could have accessed his car at the time of the search or that evidence of the offense for which he was arrested might have been found therein"); New York v. Belton, 453 U.S. 454, 460 (1981) (vehicle exception to the warrant requirement involving marijuana odor; holding that "when a policeman has made a lawful custodial arrest of the occupant of an automobile, he may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile."); South Dakota v. Opperman, 428 U.S. 364, 372, 376 (1976) (holding that a warrantless, inventory search of a vehicle is constitutional if "following standard police procedures"); Schneckloth v. Bustamonte, 412 U.S. 218, 248–49 (1973) (allowing warrantless searches as long as the totality of the circumstances show that the consent was not coerced); Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 299 (1967) (allowing a warrantless search "as broad as may reasonably be necessary to prevent the dangers that the suspect at large in the house may resist or escape," an exigency exception).

35. United States v. Robinson, 414 U.S. 218, 234–35 (1973) (allowing law enforcement to thoroughly search—rather than just *Terry*-like frisk—a *custodial* arrestee because of the specific dangers associated with a *custodial* arrest, *e.g.*, the length of time an officer would have contact with the custodial arrestee during transport); the Court succinctly concluded that "it is the fact of custodial arrest which gives rise to the authority to search." *Id*. at 236.

36. Sibron v. New York, 392 U.S. 40, 63 (1968) (observing "[i]t is axiomatic that an incident search may not precede an arrest and serve as part of its justification").

37. *Chimel*, 395 U.S. at 763. The area under the arrestee's immediate control is sometimes referred to as the grabbing or lunging area. *See, e.g.*, *Belton*, 453 U.S. at 460 (grabbing); Thornton v. United States, 541 U.S. 615, 621 (2004) (lunging). It does not include penetration of bodily surfaces. *See* Schmerber v. California, 384 U.S. 757, 767–72 (1966); Winston v. Lee, 470 U.S. 753, 760–63 (1985). And it likely does not, at least in the ordinary case, include strip searches. *Cf.* United States v. Edwards, 415 U.S. 800, 808 n.9 (1974) (quoting Charles v. United States, 278 F.2d 386, 389 (9th Cir.), *cert. denied*, 364 U.S. 831 (1960)) ("We thus have no occasion to express a view concerning those circumstances surrounding custodial searches incident to incarceration which might 'violate the dictates of reason either because of their number or their manner of perpetration.'").

38. *Robinson*, 414 U.S. at 226 (allowing search of the arrestee and the surrounding area "'in order to remove any weapons'" or "'seize any evidence'") (quoting *Chimel*, 395 U.S. at 763).

launched."[39] The SILA exception does not confer authority to search beyond these parameters, such as to remote portions of a residence even if the arrest occurs within its walls.[40] Neither a search warrant nor probable cause to search is needed for the SILA exception. The requisite showing to conduct a warrantless SILA is simply that: (1) the arrest is lawful, i.e., based on probable cause; (2) the search is contemporaneous with the arrest; and (3) the scope of the search is confined to the arrestee and his grabbing distance and, in the case of an arrest in a residence, adjoining areas.[41] Further, the police may lawfully seize without a warrant any items discovered during a SILA, even if the item pertains to an unrelated crime,[42] provided the officer has probable cause to believe the item is contraband or an instrumentality, fruit, or evidence of a crime.[43]

The rationale for the SILA exception to the warrant requirement rests on enhancing police safety and preserving evidence. The Court has recognized that a custodial arrest provides the arrestee with an incentive to use a weapon to resist the police and escape, and to destroy or conceal evidence.[44] Moreover, an arrest in a residence creates the risk that an accomplice or friend of the arrestee might be close by and come to the arrestee's aid by attacking the police.[45] Because such risks are serious and ubiquitous, the Court fashioned a

39. Maryland v. Buie, 494 U.S. 325, 334 (1990) ("Beyond that, however, we hold that there must be articulable facts which, taken together with the rational inferences from those facts, would warrant a reasonably prudent officer in believing that the area to be swept harbors an individual posing a danger to those on the arrest scene.").

40. Early Supreme Court decisions authorized broader authority to search under SILA. United States v. Rabinowitz, 339 U.S. 56, 59–63 (1950); Harris v. United States, 331 U.S. 145, 151 (1947). Both these cases were overruled by *Chimel*. *Chimel*, 395 U.S. at 768. After *Chimel*, police may search beyond the grabbing distance (and adjoining areas, if applicable) only if the search is conducted pursuant to a warrant or falls within the scope of another exception to the warrant requirement.

41. Also required is that an arrest is authorized for the offense. Atwater v. City of Lago Vista, 532 U.S. 318, 347–55 (2001). There is not authority to conduct a warrantless search incident to a citation. Knowles v. Iowa, 525 U.S. 113, 116–19 (1998).

42. *E.g.*, *Robinson*, 414 U.S. at 235–36 (holding that the arresting officer properly seized heroin discovered during the search of a traffic offender).

43. *See* Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 307 (1967) (holding there must be "a nexus . . . between the item to be seized and criminal behavior"); Arizona v. Hicks, 480 U.S. 321, 326 (1987) (holding the police must have probable cause to seize items found in plain view).

44. *Chimel*, 395 U.S. at 763; *Robinson*, 414 U.S. at 234–35 ("It is scarcely open to doubt that the danger to an officer is far greater in the case of the extended exposure which follows the taking of a suspect into custody and transporting him to the police station than in the case of the relatively fleeting contact resulting from the typical *Terry*-type stop."); Riley v. California, 134 S. Ct. 2473, 2483 (2014).

45. Maryland v. Buie, 494 U.S. 325, 333–34 (1990) (Considering "[t]he risk of danger in the context of an arrest in the home," the "arresting officers are permitted in such circumstances to

bright-line SILA exception to address them categorically. Under the exception, the arresting officer is relieved of the burden of making an ad hoc judgment about whether a warrantless SILA is supported by probable cause or reasonable suspicion, just as the courts are spared the task of performing a case-by-case analysis of whether the officer's decision to search without a warrant was based on probable cause or reasonable suspicion.[46]

In the years following *Chimel v. California*,[47] much of the Court's attention with respect to SILA related to the outer boundaries of an arrestee's immediate control,[48] and whether the search was contemporaneous with the arrest.[49] This decisional authority often addressed the application of the SILA exception to vehicles and vehicle occupants.[50]

Far less developed by the Court was the question of whether there would be any restrictions on the police authority to search and seize items under SILA because of the particular privacy interests implicated by the item itself. Quite to the contrary, the Court expressed the view that a full and intrusive search of

take reasonable steps to ensure their safety after, and while making, the arrest. That interest is sufficient to outweigh the intrusion such procedures may entail.").

46. Further, the SILA exception also recognizes the impracticality of obtaining warrants to search incident to arrest given the fluidity and spontaneity of many arrests.

47. *Chimel*, 395 U.S. at 752.

48. *E.g.*, Preston v. United States, 376 U.S. 364, 365–66, 368 (1964) (finding officers' search of the vehicle of bank robbery suspects under search incident to arrest authority—after the vehicle was towed from the scene to a garage—was too remote to be a reasonable search).

49. *E.g.*, United States v. Edwards, 415 U.S. 800, 801–02, 805 (1974) (allowing a suspect's clothes to be admitted into evidence when they were seized after he spent the night in jail).

50. In 2009, the Court analyzed SILA with specific regard to the vehicle exception jurisprudence:

> Indeed, some courts have upheld searches under *Belton* "even when . . . the handcuffed arrestee has already left the scene."
>
> Under this broad reading of *Belton*, a vehicle search would be authorized incident to every arrest of a recent occupant notwithstanding that in most cases the vehicle's passenger compartment will not be within the arrestee's reach at the time of the search. To read *Belton* as authorizing a vehicle search incident to every recent occupant's arrest would thus untether the rule from the justifications underlying the *Chimel* exception—a result clearly incompatible with our statement in *Belton* that it "in no way alters the fundamental principles established in the *Chimel* case regarding the basic scope of searches incident to lawful custodial arrests." Accordingly, we reject this reading of *Belton* and hold that the *Chimel* rationale authorizes police to search a vehicle incident to a recent occupant's arrest only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search.
>
> Although it does not follow from *Chimel*, we also conclude 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."

Arizona v. Gant, 556 U.S. 332, 342–43 (2009) (alteration in original) (citations omitted) (quoting Thornton v. United States, 541 U.S. 615, 628 (2004); New York v. Belton, 453 U.S. 454, 460 n.3 (1981); *Thornton*, 541 U.S. at 632 (Scalia, J., concurring)).

an arrestee, including containers on the arrestee's person and within his reach, was reasonable if for no other reason than because the search was incident to a lawful arrest.[51] No additional showing, such as probable cause or an exigency to search, was needed.[52] Thus, containers on the arrestee's person and within the search zone could be searched and seized pursuant to the SILA exception even when there was no apparent threat to the safety of the police or the integrity of the evidence.

In *United States v. Robinson*, for example, the suspect was arrested for suspicion of driving on a revoked license.[53] During the ensuing SILA, the arresting officer felt an object in the arrestee's breast pocket that he could not identify.[54] The officer pulled it out and saw that it was a crumpled cigarette packet.[55] The officer could feel objects inside the packet that did not seem to be cigarettes.[56] The officer was confident, however, that the packet did not contain a weapon that could threaten his safety.[57] Further, the officer did not claim that a contemporaneous search of the packet was needed to preserve evidence[58] as he could have seized and secured the packet, and later sought a warrant to search its contents.[59] The officer nevertheless immediately opened the packet and found inside several gelatin capsules containing heroin.[60] The officer seized the capsules, which served as the basis for the arrestee's prosecution on drug possession charges.[61]

The Supreme Court held in *Robinson* that the authority to conduct a warrantless SILA "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."[62] The Court explained 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."[63] The Court instructed that this

51. United States v. Robinson, 414 U.S. 218, 235 (1973).

52. *Id.*

53. *Id.* at 220.

54. *Id.* at 221–23.

55. *Id.* at 223.

56. *Robinson*, 414 U.S at 223.

57. *Id.* at 251, 253, 256 (Marshall, J., dissenting).

58. *Id.* at 252.

59. Probable cause for an arrest allows an officer to search the arrestee's person and immediately surrounding area—permitting the officer to seize containers found therein—but it does not allow a search of seized containers without a subsequent search warrant or pertinent exigent circumstance. United States v. Chadwick, 433 U.S. 1, 14–15 (1977) (quoting Chimel v. California, 395 U.S. 752, 763 (1969)); Preston v. United States, 376 U.S. 364, 367 (1964).

60. *Robinson*, 414 U.S. at 223.

61. *Id.*

62. *Id.* at 235.

63. *Id.*

is a bright-line rule, which obviates the need to "litigate[] 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."[64] The Court concluded that "in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement . . . but is also a "reasonable" search under [the Fourth] Amendment."[65]

But what if the container in *Robinson* had been a purse or a briefcase rather than a crumpled cigarette packet? Could the police then search its contents without a warrant? What if the officer had removed a diary or sealed envelope from the arrestee's person and opened it to check for weapons? Could the officer then read its contents? Should a categorical approach to the SILA exception be applied to these items, thereby permitting their private content to be thoroughly searched absent a warrant or even probable cause? A recent Supreme Court decision addressing digital technology and data may be instructive in responding to these types of issues.

II. SILA APPLIED TO THE DIGITAL CONTENTS OF CELL PHONES

In *Riley v. California*, decided in 2014, the Supreme Court unanimously held that the warrantless search of a cell phone seized during an arrest is unconstitutional.[66] The case arose from a split among federal and state courts over whether the Fourth Amendment permitted the warrantless search of the digital contents of a cell phone under SILA authority.[67]

64. *Id.*

65. *Robinson*, 414 U.S. at 235.

66. 134 S. Ct. 2473, 2495 (2014).

67. Circuit courts were split on the issue of whether or not the contents of a cell phone could be searched without a warrant after a lawful arrest. *See* United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013) ("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."); United States v. Flores-Lopez, 670 F.3d 803, 804–10 (7th Cir. 2012) (allowing the search of the cell phone in order to get its phone number, but noting that it may be problematic if other personal information were sought); United States v. Arellano, 410 F. App'x 603, 606–07 (4th Cir. 2011) (allowing the officers to seize the cell phone under SILA, but not to power on the cell phone and field incoming calls); United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007) (allowing the SILA exception to validate the cell phone search of the custodial arrestee because a cell phone is like a container, which could hold evidence of a crime). State supreme courts also had differing opinions as to whether or not a custodial arrest allowed the warrantless search of cell phones. *See* Smallwood v. State, 113 So. 3d 724, 738, 740 (Fla. 2013) (not allowing warrantless searches of cell phone data without a further exigency or safety concern: "In our view, allowing law enforcement to search an arrestee's cell phone without a warrant is akin to providing law enforcement with a key to access the home of the arrestee."); Commonwealth v. Phifer, 979 N.E.2d 210, 215–16 (Mass. 2012) ("[T]he limited search of the defendant's cellular telephone to examine the recent call list was a permissible search incident to the defendant's lawful arrest," because the search was limited and the officer had probable cause

Riley was a consolidated opinion involving two cases.[68] In the first case, David Riley was pulled over for expired registrations tags.[69] During the stop, the officer learned that Riley was driving with a suspended driver's license.[70] Police department policy, at the time, required the vehicle be towed and impounded to prevent someone, like Riley, from driving again with a suspended license.[71] Department policy also required officers to perform an inventory search of the vehicle, which led the police to find two loaded handguns under its hood.[72] Because of the discovery of the concealed weapons and gang paraphernalia during the vehicle search, police placed Riley under arrest and searched his cell phone's digital contents without a warrant.[73] The cell phone search yielded information indicating that Riley was a member of a local gang.[74] Evidence found in the cell phone included pictures, cell phone contacts, text messages, and video clips.[75] Among the photos was a picture of another vehicle that Riley owned that was involved in an earlier gang shooting.[76] Based in part on the pictures and videos recovered from the cell phone, Riley was charged in connection with the gang shooting and the prosecution sought a sentence enhancement based on Riley's gang membership.[77] Riley moved to suppress the cell phone evidence, but the judge

that the call log would contain evidence of the crime.); Hawkins v. State, 723 S.E.2d 924, 925–26 (Ga. 2012) (allowing the warrantless search of cell phones under the closed-container SILA exception); People v. Diaz, 244 P.3d 501, 509–11 (Cal. 2011) (allowing even a delayed search of the cell phone's text messages because the cell phone was on the custodial arrestee's person at the time of arrest); State v. Smith, 920 N.E.2d 949, 954–56 (Ohio 2009) (not allowing the search of a cell phone without a warrant because cell phones hold highly private information and are therefore not equivalent to closed containers).

68. People v. Riley, No. D059840, 2013 Cal. App. Unpub. LEXIS 1033 (Cal. Ct. App. Feb. 8, 2013), *rev'd sub nom.* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Wurie, 612 F. Supp. 2d 104 (D. Mass. 2009), *rev'd and remanded*, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 134 S. Ct. 2473 (2014).

69. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *5–6; *Riley*, 134 S. Ct. at 2480.

70. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *6; *Riley*, 134 S. Ct. at 2480.

71. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *6; *Riley*, 134 S. Ct. at 2480.

72. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *6–7; *Riley*, 134 S. Ct. at 2480 (citing CAL. PENAL CODE §§ 12025(a)(1), 12031(a)(1) (West 2009)). Later ballistic testing would confirm that the handguns were used in an earlier gang-related murder, for which Riley had been a suspect. Eyewitnesses to the shooting claimed Riley could have been one of the shooters, but they did not positively identify Riley. None of this information was known to the arresting officer at the time of the traffic stop. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *2–3.

73. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *7–8; *Riley*, 134 S. Ct. at 2480–81.

74. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *4, *8; *Riley*, 134 S. Ct. at 2480–81.

75. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *7–8; *Riley*, 134 S. Ct. at 2480–81.

76. *Riley*, 134 S. Ct. at 2481.

77. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *1, *1 n.2; *Riley*, 134 S. Ct. at 2481.

permitted it to be introduced at both the first trial and on retrial.[78] Ultimately, Riley was found guilty, and the California Court of Appeal affirmed his conviction.[79]

In the second case, Brima Wurie was arrested after police saw him participate in an apparent drug sale.[80] At the police station, officers seized two cell phones from Wurie's person, including a "flip phone."[81] Shortly thereafter, police observed the "flip phone" receive multiple calls from a source identified as "my house" on the phone's external screen.[82] The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they believed was Wurie's apartment.[83] Police obtained a search warrant for Wurie's residence and, during the ensuing search, found crack cocaine, marijuana, drug paraphernalia, a firearm, ammunition, and cash.[84] Wurie was later charged with drug and firearm offenses, and he moved to suppress the evidence obtained from the search of the apartment.[85] The district court denied the motion and Wurie was convicted.[86] A divided panel of the First Circuit Court of Appeals reversed the denial of the motion to suppress and vacated the related convictions.[87] The court held that cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant because of the vast amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests.[88]

Chief Justice Roberts delivered the opinion of the Supreme Court on the consolidated cases, holding that a warrant is required to search a cell phone seized incident to a lawful arrest.[89] Roberts wrote that the digital contents of cell phones do not fall within the warrantless search authority of the SILA exception to the warrant requirement established by *Chimel*:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade

78. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *1–2, *5, *8–10, *20; *Riley*, 134 S. Ct. at 2481.
79. *Riley*, 2013 Cal. App. Unpub. LEXIS 1033, at *1, *30; *Riley*, 134 S. Ct. at 2481.
80. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2481.
81. *Wurie*, 728 F.3d at 2, 15; *Riley*, 134 S. Ct. at 2481.
82. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2481.
83. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2481.
84. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2481.
85. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2482.
86. *Wurie*, 728 F.3d at 2; *Riley*, 134 S. Ct. at 2482.
87. *Wurie*, 728 F.3d at 1, 14.
88. *Id.* at 13–14.
89. *Riley*, 134 S. Ct. at 2495.

> hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.[90]

Roberts recognized that evidence stored on a cell phone may possibly be destroyed by either remote wiping or data encryption, but he explained that this is "the ordinary operation of a phone's security features, apart from *any* active attempt by a defendant or his associates to conceal or destroy evidence upon arrest."[91] Accordingly, the warrantless search of the phone's digital contents would likely make little difference regarding the preservation of data.

> Cell phone data would be vulnerable to remote wiping from the time an individual anticipates arrest to the time any eventual search of the phone is completed. . . . Likewise, an officer who seizes a phone in an unlocked state might not be able to begin his search in the short time remaining before the phone locks and data becomes encrypted.[92]

Finally, Roberts argued that cell phones differ in both a quantitative and a qualitative sense from other objects that might be found in an arrestee's pocket.

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[93]

Justice Alito wrote a separate opinion concurring in part and concurring in the judgment, citing his dissent in *Arizona v. Gant*[94] that questioned *Chimel*'s categorical approach to the SILA exception.[95] Alito nonetheless agreed with the majority:

> [W]e should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.[96]

90. *Id.* at 2485.

91. *Id.* at 2486 (emphasis in original).

92. *Id.* at 2487. Roberts cites several common methods for either turning off or preventing the phone's security features. Roberts then cites several common examples to either turn off or prevent the phone's security features. *Id.*

93. *Id.* at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

94. *Riley*, 134 S. Ct. at 2495–96 (Alito, J., concurring in part, concurring in judgment) (citing Arizona v. Gant, 556 U.S. 332, 361–363 (2009) (Alito, J., dissenting)).

95. *Gant*, 556 U.S. at 361–63 (Alito, J., dissenting) (questioning Chimel v. California, 395 U.S. 752, 762–63 (1969)).

96. *Riley*, 134 S. Ct. at 2496 (Alito, J., concurring in part, concurring in judgment).

Alito expressed concern, however, that the majority opinion creates certain anomalies. He observed that "[u]nder established law, the police may seize and examine [hard copies of information] in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out."[97] Alito suggested that Congress and state legislatures may need to consider new laws that draw "reasonable distinctions based on categories of information or perhaps other variables."[98] In the absence of proactive legislation, Alito cautioned that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[99]

Few would disagree with Alito's admonition that the elected branches of government should enact laws in response to emerging technologies that safeguard privacy interests beyond the Fourth Amendment's basic parameters.[100] There are many examples of effective legislation that provide enhanced privacy consistent with fundamental values and public sentiment.[101] Regardless of the presence or absence of such statutes, however, the Fourth Amendment affords an irreducible core of privacy protection that must be judicially recognized and applied, especially in circumstances when the elected

97. *Id.* at 2497.

98. *Id.*

99. *Id.*

100. Laws are subordinate to the Constitution. Thus, legislation can provide greater protection for privacy than required by the Fourth Amendment but it may not lessen or diminish its protection. *See* Missouri v. McNeely, 133 S. Ct. 1552, 1567 (2013) (quoting Virginia v. Moore, 553 U.S. 164, 171 (2008)) (alteration in original) ("States [may] choos[e] to protect privacy beyond the level that the Fourth Amendment requires."); Nitro-Lift Techs., L.L.C. v. Howard, 133 S. Ct. 500, 504 (2012) ("Where a specific statute, for example, conflicts with a general constitutional provision, the latter governs. And the same is true where a specific state statute conflicts with a general federal statute."); State v. Boggs, 741 N.W.2d 492, 499 (Iowa 2007) ("States are not only permitted to enact statutes that are consistent with constitutional principles, they may also define greater rights than provided by the federal and state constitution."); State v. Lynch, 74 P.3d 73, 79 (N.M. 2003) ("As a general proposition, statutes may provide greater, but not less, protection to individual rights than the constitution.").

101. *See, e.g.*, Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2012) (protecting electronic communications unless heightened circumstances allow disclosure, such as the information "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities"); Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2511 (2012) (protecting against recording oral communications, unless falling under limited exceptions); Bank Secrecy Act, 12 U.S.C. § 1829b (1994) (requiring banks to make copies of checks and deposits but not allowing the information to be automatically seized by the government); Privacy Protection Act, 42 U.S.C. § 2000aa-11(a) (1982) (protecting information that "would intrude upon a known confidential relationship such as that which may exist between clergyman and parishioner; lawyer and client; or doctor and patient" because of "a recognition of special concern for [those] privacy interests"); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1982) (protecting dissemination of education records).

branches of government are slow or unwilling to act. It is in this spirit that *Riley*'s potential application to predigital privacy will next be considered.

III. EXTENDING *RILEY* DIGITAL PROTECTION TO SOME TYPES OF PREDIGITAL INFORMATION

Riley modified the prior categorical rule that all items taken from an arrestee's person may be fully searched absent a warrant and probable cause pursuant to the SILA exception.[102] It holds that the SILA authority does not extend to the digital contents of a cell phone seized during a SILA.[103] Instead, police may seize the item based on probable cause and apply for a warrant to search it.[104] The fundamental question presented by *Riley* with regard to its possible broader application to predigital information is this: is the digital information stored on cell phones afforded the enhanced protection of a warrant during a SILA because of peculiar privacy considerations related to the quantity and quality of the information contained in such devices, or instead is the data typically stored in a cell phone part of a larger class of information that is entitled to the enhanced protection of a warrant during a SILA? Put simply, are the digital contents of a cell phone uniquely deserving of the protection of a warrant when the phone's contents could otherwise be searched without a warrant during a SILA?

To answer this question, it is initially useful to consider the Court's rationale for the SILA exception as it was originally applied to predigital information. The SILA exception and its bright-line application are predicated on a balancing of competing interests. On the one hand, the government has a powerful and undeniable interest in protecting the safety of police officers while making arrests and preserving evidence that is obtained from arrestees.[105] Besides being weighty—and the interest in police safety is especially weighty[106]—these law enforcement interests are almost always

102. *Riley*, 134 S. Ct. at 2484.

103. *Id.* at 2485.

104. If the arrestee was to be confined immediately following his arrest, then the cell phone could be impounded (seized) and inventoried. *See* Illinois v. Lafayette, 462 U.S. 640, 644, 647 (1983) ("A so-called inventory search is not an independent legal concept but rather an incidental administrative step following arrest and preceding incarceration. . . . The reasonableness of any particular governmental activity does not necessarily or invariably turn on the existence of alternative 'less intrusive' means."). Whether the digital contents of the cell phone could be obtained pursuant to an inventory search based on prospective confinement is beyond the scope of this article.

105. *Riley*, 134 S. Ct. at 2483.

106. *See* Arizona v. Johnson, 555 U.S. 323, 331 (2009) ("The government's 'legitimate and weighty' interest in officer safety, the Court said, outweighs the '*de minimis*' additional intrusion.") (quoting Pennsylvania v. Mimms, 434 U.S. 106, 110–11 (1977)); Maryland v. Buie, 494 U.S. 325, 332 (1990) ("[A]lthough a frisk for weapons 'constitutes a severe, though brief,

implicated anytime someone is arrested.[107] Further, the arrest and circumstances surrounding it are often unforeseeable, and thus not subject to prior judicial review.[108] On the other hand, the countervailing privacy interests implicated during a SILA are comparatively weak. A search incident to an arrest generally involves only marginal additional intrusiveness beyond that already experienced by the arrestee by virtue of his arrest.[109] Given the strength and virtual certainty of the government's interest to search, as contrasted to the minimal intrusiveness of the search experienced by the

intrusion upon cherished personal security,' such a frisk is reasonable when weighed against the 'need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest.'") (quoting Terry v. Ohio, 392 U.S. 1, 24–25 (1968) (citation omitted)). A stop and frisk is allowed when "a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger." *Terry*, 392 U.S. at 27. "There is no reason why an officer, rightfully but forcibly confronting a person suspected of a serious crime, should have to ask one question and take the risk that the answer might be a bullet." *Id.* at 33 (Harlan, J., concurring).

107. Chimel v. California, 395 U.S. 752, 762–63 (1969) ("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 in order to resist arrest or effect his escape.").

108. *Id.* at 778–79 (White, J., dissenting).

109. In *Chimel*, Justice White's dissenting opinion paves the way for the concept of SILA's slight privacy interest infringement when the suspect is already under arrest:

> [I]f circumstances can justify the warrantless arrest, it would be strange to say that the Fourth Amendment bars the warrantless search, regardless of the circumstances, since the invasion and disruption of a man's life and privacy which stem from his arrest are ordinarily far greater than the relatively minor intrusions attending a search of his premises.

Id. at 776.

Less than four years later, the Court in *Robinson* explained:

> 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. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment.

United States v. Robinson, 414 U.S. 218, 235 (1973). *See* United States v. Edwards, 415 U.S. 800, 801–02, 805 (1974) (upholding the reasonable search and seizure of clothing literally taken off a custodial arrestee's back the morning after his arrest, ten hours post-arrest, because it was a "normal incident of a custodial arrest, and reasonable delay," and the custodial arrestee "was no more imposed upon than he could have been at the time and place of the arrest or immediately upon arrival at the place of detention"); Weeks v. United States, 232 U.S. 383, 386–88, 392, 398 (1914) (holding, after the arrest of a man at his place of work, the warrantless search and seizure of the arrestee's lottery papers—found in his bedroom after a neighbor showed police where to find the key to the home—unreasonable, because the police needed a warrant to enter the sanctity of the home and the papers were not found within arrestee's control at the time of the arrest).

arrestee, the Court fashioned a categorical bright-line exception to the warrant requirement for SILA.[110]

In *Riley*, the competing values implicated by searching the digital contents of cell phones caused the Court to recalibrate its earlier SILA balancing. The Court observed that police safety is not jeopardized by the digital contents of a cell phone, and it is unlikely that the contemporaneous searching of a cell phone's digital contents will assist in the preservation of evidence.[111] In any event, a cell phone can always be seized during a SILA and a warrant can be sought to search its digital contents.[112] Balanced against these negligible government interests in support of a contemporaneous search of a cell phone's digital contents is the especially weighty intrusion upon individual privacy interests caused by such an action. The digital information contained in a cell phone is often both intimate and wide-ranging. The intrusion upon privacy interests resulting from such a search would likely exceed the relative intrusiveness upon the arrestee's liberty interests by virtue of his arrest. Because the government's interest in conducting a contemporaneous search is weak and the individual privacy interests implicated are far more compelling, the SILA exception is not allowed for the digital contents of cell phones.[113]

Note that *Riley* did not replace the bright-line SILA rule with a case-by-case exception for cell phones. Rather, it established a categorical, bright-line exemption for these devices.[114] Accordingly, no cell phone can have its digital contents derivatively searched based on a lawful arrest.[115] A warrant is presumptively required.[116] For a warrantless search to be reasonable in connection with an arrest, it must fall within the parameters of another exception to the warrant requirement, such as an exigency exception, based on the particular circumstances of the case.[117]

110. *Riley*, 134 S. Ct. at 2493, 2495.

111. *Id.* at 2485–87.

112. It does not necessarily follow that a search warrant will inevitably be granted to search a cell phone's digital contents. A warrant would be denied in those cases in which the government lacks probable cause to search, a result that is consistent with broader Fourth Amendment jurisprudence. Further, regardless of whether the government has authority to search a cell phone under a warrant or SILA, it may lack the capacity to access encrypted content. *See* Lev Grossman, *Inside Apple CEO Tim Cook's Fight With the FBI*, TIME (Mar. 17, 2016), http://time.com/4262480/tim-cook-apple-fbi-2/ [http://perma.cc/2P4B-E5tv].

113. *Riley*, 134 S. Ct. at 2492, 2495.

114. *Id.* at 2493, 2495.

115. *Id.* at 2493.

116. *Id.*

117. "To the extent that a search of cell phone data might warn officers of an impending danger, *e.g.*, that the arrestee's confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances." *Id.* at 2478. "The exceptions are 'jealously and carefully drawn,' Jones v. United States, 357 U.S. 493, 499 (1958), and there must be 'a showing by those who seek

The specific facts of *Robinson*, albeit superficially, support drawing a sharp distinction between the digital contents of a cell phone and the predigital contents of other containers. The container in *Robinson* was a crumpled cigarette package.[118] It has none of the obvious attributes of a container containing highly personal or private information, such as a cell phone. The cigarette package could be accurately described as a container that is unworthy of the protection of a warrant in SILA situations.[119] This is an easy case.

But what about other types of predigital containers? Surely a handwritten diary will predictably contain highly personal and private information, perhaps information that is even more personal and private than much of the information that could routinely be obtained from a cell phone.[120] In such

exemption . . . that the exigencies of the situation made that course imperative,' McDonald v. United States, 335 U.S. 451, 456 (1948)." Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971) (alteration in original) (citations added). For example, in *Warden*, the police were looking for an armed robber who, through an informant tip, was thought to be in the home searched. Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 297–98 (1967). The Court not only found that the exigent circumstances allowed the warrantless entry of the home and search for the suspect, but allowed the search for weapons and accomplices even after the suspect was caught.

> The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others. Speed here was essential, and only a thorough search of the house for persons and weapons could have insured that Hayden was the only man present and that the police had control of all weapons which could be used against them or to effect an escape.

Warden, 387 U.S. at 298–99. However, the Court did not allow a per se exigency exception to apply to blood tests in DUI cases even though alcohol dissipates in the blood. Missouri v. McNeely, 133 S. Ct. 1552, 1560–61 (2013).

118. United States v. Robinson, 414 U.S. 218, 223 (1973).

119. Robbins v. California, 453 U.S. 420, 429–32 (1981) (Powell, J., concurring) (explaining that "officers needed a warrant to open a sealed, opaquely wrapped container in the rear compartment of a station wagon," containing two bricks of marijuana, because there is a "reasonable expectation of privacy" in a package thus wrapped), *overruled by* United States v. Ross, 456 U.S. 798 (1982). The *Robbins* majority disagreed with Powell, observing that "[w]hat one person may put into a suitcase, another may put into a paper bag." *Robbins*, 453 U.S. at 426, *overruled by Ross*, 456 U.S. 798.

120. Ironically, there may be a diminished expectation of privacy with regard to some digital information. For example, digital information that is published on social media would have a diminished expectation of privacy. United States v. Meregildo, 883 F. Supp. 2d 523, 525–26 (S.D.N.Y. 2012) (citing Katz v. United States, 389 U.S. 347, 351–52 (1967); United States v. Barone, 913 F.2d 46, 49 (2d Cir. 1990)) (holding that law enforcement officers, building a case against a gang member, could use information obtained through a cooperating witness' social media profile access—a Facebook friend's access); *In re* Application of the United States, 830 F. Supp. 2d 114, 139 (E.D. Va. 2011) (emphasis added) (citing Wyoming v. Houghton, 526 U.S. 295, 303–06 (1999)) (holding that "[p]etitioners knew or should have known that their IP address information was subject to examination by Twitter, so they had a *lessened* expectation of privacy in that information, particularly in light of their apparent consent to the Twitter Terms of Service and Privacy Policy."). Similarly, information that has been communicated via e-mail or a text would seemingly have a diminished expectation of privacy. State v. Patino, 93 A.3d 40, 55–56

circumstances, upon what principled basis could the Court require the protection of a warrant for a digital diary accessed via a cell phone but not require a warrant for a handwritten diary accessed by opening a book and reading it? Four possible arguments might be reasonably raised in support of such a distinction. For the reasons set forth below, none of these contentions are ultimately persuasive.

First, one might argue that cell phones presumptively contain private information while predigital items do not. While this assertion may generally be correct, it would not be accurate in all circumstances. It would certainly not be true, for example, in the case of purses, wallets, briefcases, and backpacks. It would not be true for paper books that are clearly recognizable as diaries and notebooks. It would not be true for containers marked as medical or financial records. It would not be true for scrapbooks, photo albums, and sealed correspondence. In all such circumstances, it seems doubtful that a fact-based distinction predicated on degrees of privacy could be reasonably drawn between digital information in cell phone containers and these types of predigital information in traditional containers. Given all of the situations in which this presumption would be in contradiction with the actual facts, it would seem unjustified to predicate a bright-line rule on its presumed accuracy.

A second possible argument in favor of categorically distinguishing between digital and predigital information is that such line drawing is supported by the rationale underlying the SILA exception. This argument likewise fails. The basis for the SILA exception is police safety and preservation of evidence. There is no reason for believing the contents of a handwritten diary or a sealed envelope, for example, would pose any greater threat to these law enforcement interests than would the digital contents of a cellphone. Of course, a diary or envelope—indeed, any container including a cell phone in a carrying case—could conceivably conceal a weapon or evidence that might be destroyed. *Riley* responds to these concerns by allowing a limited warrantless search of cell phones to address these risks.[121] Similar allowances could easily be permitted for the physical contents of books, envelopes, briefcases, purses, wallets and so forth. Put simply, the risk-

(R.I. 2014) (citing Rakas v. Illinois, 439 U.S. 128, 154 (1978); United States v. Jacobsen, 466 U.S. 109, 117 (1984)) ("In determining whether a person has an expectation of privacy in his text messages, the most important factor . . . is from whose phone the messages are accessed" because it indicates less control of the information and the corresponding assumption of risk when speaking with another person).

121. The Court allows SILA limited searches of the physical contents of a cell phone, and still allows the exigency exception to allow a search of the phone's digital contents. Riley v. California, 134 S. Ct. 2473, 2494 (2014) ("Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury.").

avoidance rationale for the SILA exception does not support treating facially private predigital information in cell phones any differently than facially private digital information in traditional containers.

A third argument for distinguishing between the digital contents of a cell phone and predigital information in traditional containers relates to the sheer quantity of the information that can be stored on the former. A quantitative approach for assessing privacy, however, is inconsistent with the Court's predigital case authority. For decades, the Court repeatedly held that the need for a warrant is to be determined by the quality of the privacy interest intruded upon and not the quantity of the information to be searched. For example, in *Smith v. Maryland*, the Court held that the warrantless use of a pen register to obtain certain information (the phone numbers dialed by the suspect) was reasonable because the information gathered was not private.[122] A warrant was not needed regardless of the amount of such data collected because of the public nature of the data.[123] On the other hand, if the pen register had obtained a single bit of information regarding the contents of a telephone conversation, this would have constituted a warrantless search in violation of the Fourth Amendment because of the private nature of this information.[124] *Smith* teaches that it is the quality and not the quantity of the information obtained via the pen register that determines whether the government's warrantless use of this device constitutes an unreasonable search.

The same distinction between the quality and quantity of information has been recognized even when the information to be searched is far more extensive and diverse. For instance, police may conduct a warrantless search of the entire contents of a mobile home residence, in large part because of the diminished expectation of privacy afforded to vehicles in general.[125] In contrast, police would presumptively need a warrant to search a non-mobile residence or a personal computer kept inside of it.[126] A search warrant would be required for a fixed residence even if the police knew the precise location of

122. 442 U.S. 735, 745–46 (1979) ("[P]etitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required.").

123. *Id.*

124. *Id.* at 741 ("Yet a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.").

125. California v. Carney, 471 U.S. 386, 392 (1985) ("In short, the pervasive schemes of regulation, which necessarily lead to reduced expectations of privacy, and the exigencies attendant to ready mobility justify searches without prior recourse to the authority of a magistrate so long as the overriding standard of probable cause is met.").

126. It has long been held that entering a home without a warrant is per se unreasonable. *See* Payton v. New York, 445 U.S. 573, 586 (1980). "That the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose . . . " *Id.* at 596 n.44 (quoting Semayne's Case, 77 Eng. Rep. 194, 195 (K.B. 1603)).

the information in the residence or stored in the computer inside of it and thus could avoid any collateral privacy intrusions during their search. Under the Court's traditional decisional authority, the Fourth Amendment presumptively requires a warrant for in-home searches because it protects against unreasonable intrusions upon privacy regardless of how wide-ranging or cabined the intrusion may be.[127] In contrast, the Fourth Amendment is generally not concerned with activities that do not intrude upon cognizable privacy interests regardless of the volume of information these activities may gather.[128] It follows from these principles that the requirement for a search warrant based on a cell phone's capacity to store a vast quantity of data, even if defensible on the merits in such cases, is irrelevant when evaluating whether a warrant is needed to protect the privacy interests implicated by a single bit of information residing in a traditional container having a much smaller storage capacity.

Recently, the Court considered whether the quantity of information obtained by a GPS or beeper device was a factor in determining whether a search warrant was required for its use in *United States v. Jones*.[129] *Jones*, taken together with *Riley*, may portend that a quantitative analysis—in addition to a qualitative analysis—is sometimes necessary in evaluating privacy interests, given the capacity of new technologies to gather and store voluminous information. But the conclusion that a search warrant should be required in some circumstances because of the vast quantity or diversity of information that can be obtained by or stored in a digital device does not mean that clearly private information should be accorded less protection because it is gathered or stored in a narrow or discreet manner.

A fourth argument in support of drawing a distinction between digital and predigital information is that doing so preserves the benefits of a simple and clear bright-line SILA rule. The premise of this argument is correct, insofar as categorical rules are undeniably easier for police to apply in the field and for courts to review at trial and on appeal. While simplicity and ease of application are desirable, these benefits should not be decisive in assessing the wisdom of a bright-line rule. Rather, a rule's other benefits and burdens should be

127. *See* Arizona v. Hicks, 480 U.S. 321, 324–25 (1987) (holding that moving a few stereo components to read serial numbers on the bottom of them based on a reasonable suspicion they were stolen constituted an unreasonable search of these items as this exceeded the scope of a legitimate exigency-based search of an entire residence for a shooter, victim, and weapons).

128. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

129. 132 S. Ct. 945 (2012). Justices Alito, Ginsburg, Breyer, Kagan, and Sotomayor concurred, adding further analysis into the increased privacy interest that occurs with "longer term GPS monitoring in investigations." *Id.* at 964 (Alito, J., concurring). The longer the GPS monitoring, the greater "the sum of one's public movements" the government could retain. *Id.* at 956 (Sotomayor, J., concurring).

evaluated before reaching a comprehensive judgment about its wisdom.[130] The Court's *Chimel-Riley* approach to the SILA warrant exception should be subjected to the same scrutiny.

The most important benefit of a categorical SILA rule (with a categorical cell phone exception) is that it relieves the arresting officer from making a case-by-case determination of whether it is reasonable to search containers on the arrestee's person or within his reach. Preempting this decision from the officer during an arrest protects police from the possibly dire consequences of misjudging circumstances and incorrectly deciding that a search was not warranted. This reasoning, however, posits a false choice for the arresting officer: between either conducting a thorough, contemporaneous search or foregoing a search all together. There is a third option that is readily available and easily implemented, i.e., the arresting officer may seize an item having facial indicia of enhanced privacy without a warrant, perform a cursory search of it—if reasonable to ensure it is not dangerous—and then later seek a warrant to authorize a more extensive search of it based on probable cause. This third approach would fully serve all of the objectives of the SILA exception while simultaneously providing the enhanced protection of a warrant to predictably private information. While such a revised SILA rule would be somewhat more nuanced and less categorical than a bright-line *Chimel-Riley* distinction, any concerns about the complexity of its application could be mitigated by limiting judicial review of the arresting officer's decision to a simple objective reasonableness standard.[131] The concept of "objective reasonableness" is both

130. Every bright-line rule necessarily has some lack of conformity (the delta) between the results obtained via the application of the rule versus the results obtained through a case-by-case approach. This delta is a cost or burden of a bright-line rule that should be assessed when evaluating the rule's wisdom. Where the delta is wide or the interests compromised via application of a bright-line rule are weighty, the rule seems unwarranted. *See* Tennessee v. Garner, 471 U.S. 1, 9–11, 21–22 (1985) (invalidating a Tennessee bright-line rule that allowed deadly force without probable cause to believe the criminal suspect was dangerous and had recently committed a felony, since life is an especially weighty factor). A bright-line rule can more readily be justified where the delta is small and the interests harmed are comparatively minor. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 351–54 (2001) ("If an officer has probable cause to believe that an individual has committed even a very minor criminal offense in his presence, he may, without violating the Fourth Amendment, arrest the offender" provided the officer has the statutory authority to make a custodial arrest).

131. The Court notes that the objective reasonableness standard lessens "second-guessing" by the hindsight of judicial review:

> Often enough, the Fourth Amendment has to be applied on the spur (and in the heat) of the moment, and the object in implementing its command of reasonableness is to draw standards sufficiently clear and simple to be applied with a fair prospect of surviving judicial second-guessing months and years after an arrest or search is made. Courts attempting to strike a reasonable Fourth Amendment balance thus credit the government's side with an essential interest in readily administrable rules.

familiar to police officers and consistent with broader Fourth Amendment requirements, and thus it should present few difficulties in its application or review.[132]

The guideposts for the reasonableness standard could be simple and easily applied. Officers may always search arrestees for weapons and to preserve evidence. Accordingly, physical evidence on the arrestee's person and within his grabbing distance can be thoroughly inspected for these limited purposes. A more intrusive search of items having indicia of enhanced privacy interests—such as by reading text, listening to recordings, accessing video, etc.—is generally not permitted without a warrant.[133] The arresting officer, in any case, may seize such items and apply for a warrant to search their private contents.[134] Under this approach, the same protection accorded to cell phones

Atwater, 532 U.S. at 347; Whren v. United States, 517 U.S. 806, 812–13 (1996) (following the Court precedent that the Fourth Amendment reasonableness requirement does not hinge upon an officer's subjective intent but upon "objectively justifiable behavior," aside from the limited "context of inventory search or administrative inspection") (citing United States v. Villamonte-Marquez, 462 U.S. 579, 584, n.3 (1983)) (citing United States v. Robinson, 414 U.S. 218, 218 (1973)); Hunter v. Bryant, 502 U.S. 224, 228 (1991) ("[T]he court should ask whether the agents acted reasonably under settled law in the circumstances, not whether another reasonable, or more reasonable, interpretation of the events can be constructed five years after the fact.").

132. United States v. Leon, 468 U.S. 897, 924 (1984) ("[T]he good-faith exception [to the warrant requirement], turning as it does on *objective reasonableness*, should not be difficult to apply in practice. When officers have acted pursuant to a warrant, the prosecution should ordinarily be able to establish objective good faith without a substantial expenditure of judicial time.") (emphasis added); *Whren*, 517 U.S. at 812 (The Court "flatly dismissed the idea that an ulterior motive might serve to strip the agents of their legal justification," because the subjective intent of the officer does not negate the legally objective justification for the officer's actions.); Terry v. Ohio, 392 U.S. 1, 21–22 (1968) ("And in making that assessment it is imperative that the facts be judged against an objective standard: would the facts available to the officer at the moment of the seizure or the search 'warrant a man of reasonable caution in the belief' that the action taken was appropriate?").

133. This idea of limiting a SILA of some items having indicia of privacy to a cursory inspection to protect police is similar to the function of a protective sweep, which permits a cursory inspection of a residence to determine if others are present who may present a danger to police. Maryland v. Buie, 494 U.S. 325, 327 (1990). *Buie* upheld the admittance of a running suit found during a protective sweep of the basement—even though the suspect was already arrested and the basement was beyond the immediately adjoining area of the arrest—because the officers could provide "specific and articulable facts" that a dangerous individual was in the basement. *Id.* at 327–28, 332 (quoting *Terry*, 392 U.S. at 21). Of course, a more intrusive search would be reasonable without a warrant if it is prompted by a concern for police safety or the destruction of evidence.

134. This is analogous to an officer's authority to seize a container based on probable cause but to need a warrant to search its contents. United States v. Chadwick, 433 U.S. 1, 15 (1977) (quoting Preston v. United States, 376 U.S. 367 (1964)) ("Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain

because of the presumptively private nature of their contents would be accorded to predigital information presenting presumptively similar privacy expectations.

More broadly and apart from the above-discussed considerations, the Court must be careful to avoid drawing an artificial dichotomy between digital and predigital information for SILA purposes. "Digital data" can be defined as "[i]nformation represented and processed in the form of combinations of digits (0 and 1, in the binary system)."[135] Computers and cell phones, among other devices, store and access digital information. Predigital information includes "analog data," which is defined as "[d]ata represented in a quantitatively analogous way."[136] "Examples are the deflection of a movable-coil meter, the positioning of a slider on a slide rule, and the setting of a variable resistor to represent the value of a nonelectrical quantity."[137] Analog information can be accessed and stored, for example, on traditional telephone answering machines, record players and magnetic tape recorders. Predigital information also encompasses what might be termed pre-analog information such as handwriting, printings, drawings and film photography. Pre-analog information extends back in time for centuries. Notable and venerable examples of pre-analog information include the Dead Sea Scrolls, hieroglyphics and cave paintings.[138]

While the technological differences between digital information and some types of predigital information is obvious, some distinctions are not so clear. For example, would a magnetic tape recording be considered digital or predigital information for SILA purposes? What if the recording was stored on a floppy disk? What about information stored in a photocopier or a telephone answering machine? Applying a digital/predigital distinction, would the actual writing made by a smartpen be subject to a warrantless SILA while a search of

access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest," thus requiring a warrant to search the personal property).

135. THE ILLUSTRATED DICTIONARY OF ELECTRONICS 189 (Stan Gibilisco ed., 8th ed. 2001). "[D]igital," in general, means "[p]ertaining to components, circuits, or systems that use signals having an integral number of discrete levels or values, rather than signals, whose levels or values vary over a continuous range." *Id.* at 188. *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 375 (Steve Schoen ed., 26th ed. 2011).

136. THE ILLUSTRATED DICTIONARY OF ELECTRONICS, *supra* note 135, at 27.

137. *Id.* "[A]nalog," in general, means "[a] quantity that corresponds, point for point or value for value, to an otherwise unrelated quantity. Thus, voltage is the analog of water pressure, and current is the analog of water flow." *Id. See* NEWTON, *supra* note 135, at 125–26.

138. Also known as parietal art, cave paintings date back some 40,000 years. K. Kris Hirst, *Cave Art—What Archaeologists Have Learned: Parietal Art of the Ancient World*, ABOUT.COM, http://archaeology.about.com/od/cterms/g/caveart.htm [http://perma.cc/EZ8C-JDG5].

the data stored in the pen requires a warrant?[139] If so, does this distinction make sense?

Consider the range of issues raised in the following two situations if a strict digital/predigital distinction for the SILA exception is recognized and applied. In the first case, police arrest a suspect within arm's reach of a file cabinet. They perform a cursory search of the cabinet's interior and determine there are no weapons inside. While conducting the weapons search, police see paper files, analog tape recordings and a digital flash drive inside the cabinet. Which of these items, if any, should be subject to an intrusive warrantless SILA? Is there any principled basis for distinguishing between these items for SILA purposes? Suppose the file cabinet has a digital locking mechanism. Does this matter? What if the cabinet, instead, had a mechanical lock and key mechanism? Would the result be different?[140]

In the second case, assume a fax machine is within the grabbing distance of an arrestee when he is lawfully arrested. Is a warrant needed to perform a SILA of the information contained in the machine's memory? May printed pages stacked in the machine's tray be searched without a warrant? May the pages awaiting transmission on top of the machine be searched without a warrant? If the machine is in the midst of printing a transmission when the arrest is made, may the police read what is already printed as part of a SILA? May police instead wait for the printing to be completed and then read the entire document pursuant to the SILA exception? May police wait for pending transmissions to be received and printed, and then read those transmissions pursuant to SILA authority?

139. "A smartpen is a computer in a pen that captures everything a person hears and writes and synchronizes the written notes with the audio. Smartpen users can simply tap on their handwritten notes with their smartpen to hear the conversation play back from that exact moment in time." *AT Quick Guide: Taking Notes with the LiveScribe Smartpen*, HIGH INCIDENCE ACCESSIBLE TECH. (May 9, 2011), http://www.montgomeryschoolsmd.org/departments/hiat/tech_quick_guides/LiveScribe_taking_notes.pdf [http://perma.cc/J7U4-EBHU].

140. One could of course argue that regardless of the type of locking mechanism present, if the cabinet was locked its contents would not be readily accessible to the arrestee and thus not subject to being searched under the SILA exception. But what if the cabinet was unlocked? Would it then matter if the locking mechanism is digital or predigital? Consider that *Riley* does not suggest that the reasonableness of searching a cell phone's digital contents turns on whether the contents are password protected, i.e., whether a digital lock has been engaged. Riley v. California, 134 S. Ct. 2473, 2487 (2014) ("Similarly, the opportunities for officers to search a password-protected phone before data becomes encrypted are quite limited."). Even if the digital lock, *e.g.*, password protection, was not engaged, the digital contents could not be searched pursuant to the SILA exception. On the other hand, the contents of a filing cabinet with an unlocked mechanical locking mechanism would be subject to a warrantless SILA under *Chimel* and its progeny if the interior of the cabinet was within the arrestee's grabbing distance. *See* Chimel v. California, 395 U.S. 752, 763 (1969).

As these hypothetical situations demonstrate, in many cases any supposed practical or interest-based differences between digital and predigital information for Fourth Amendment purposes is illusory and meaningless. Applying differing Fourth Amendment standards on a digital versus predigital distinction alone would literally elevate format over substance and may have no correlation to the actual privacy interests at stake. It would be unprincipled and unwise to decide mechanically whether to afford the enhanced privacy protections recognized by *Riley*, depending on whether the information in question could be better characterized as digital or predigital.

CONCLUSION

Riley is not the first time that the Court has had to reevaluate its decisional law in light of technological advancements. It certainly will not be the last. The Court's engagement of emerging technologies offers it an opportunity to reconsider and correct past decisions addressing traditional situations. In doing so, the Court would be wise to focus on underlying Fourth Amendment values rather than on technical gadgetry. Private content is private, whether it is handwritten in a diary, entered and stored digitally on a cell phone, or created and retained by some modality that has yet to be invented. Technology advances. The Court must respond. In doing so, it should be guided by enduring constitutional principles rather than the particular attributes of a transient device, however remarkable and pervasive it may be.