Constitutional Law—The Big Picture: Applying Heightened Protection to Digital Cameras—*Commonwealth v. Mauricio*, 80 N.E.3d 318 (Mass. 2017).

The Fourth Amendment of the United States Constitution and article 14 of the Massachusetts Declaration of Rights (Article 14) both provide some measure of protection to an individual's private digital information by precluding law enforcement from conducting warrantless searches of personal electronic devices.[1] Article 14 accords private digital information stored on electronic devices greater constitutional protection from warrantless searches than the Fourth Amendment alone.[2] In *Commonwealth v. Mauricio*,[3] the Supreme Judicial Court of Massachusetts (SJC) considered whether a warrantless search of images stored on a digital camera fell within the search-incident-to-arrest exception to the warrant requirement and whether the search constituted a valid inventory search.[4] In *Mauricio*, the SJC held that the search

1. *See* U.S. CONST. amend. IV (prohibiting unreasonable searches and seizures); MASS. CONST. pt.1, art. XIV (granting protections against unreasonable searches and seizures similar to Fourth Amendment); Riley v. California, 134 S. Ct. 2473, 2488-91 (2014) (applying Fourth Amendment protections to smartphones); Commonwealth v. White, 59 N.E.3d 369, 373-74 (Mass. 2016) (noting cell phones protected by warrant requirement pursuant to Article 14); Commonwealth v. Dorelas, 43 N.E.3d 306, 311-12 (Mass. 2016) (illustrating application of Article 14 to searches in virtual world).

2. *See* Commonwealth v. Madera, 521 N.E.2d 738, 740 (Mass. 1998) (postulating Article 14 may provide greater protection than Fourth Amendment for searches and seizures); *see also* United States v. Edwards, 415 U.S. 800, 802-03 (1974) (discussing search-incident-to-arrest exception to warrant requirement under Fourth Amendment); Commonwealth v. Dorelas, 43 N.E.3d 306, 311-12 (Mass. 2016) (expounding warrant requirement for targeted electronics); Commonwealth v. Blevines, 782 N.E.2d 491, 494 n.4 (Mass. 2003) (acknowledging Article 14 more restrictive than Fourth Amendment). Generally, a warrant is required to search digital data because the search of a digital device does not fall under the search-incident-to-arrest exception. *See* Riley v. California, 134 S. Ct. 2473, 2488-89, 2495 (2014).

3. 80 N.E.3d 318 (Mass. 2017).

4. *See* MASS. GEN. LAWS ch. 276, § 1 (2016) (recognizing search-incident-to-arrest exception to warrant requirement); 80 N.E.3d at 321-22 (describing issue before court on appeal); *see also* Brief and Record Appendix of Appellant, Kevin A. Mauricio at 1, Commonwealth v. Mauricio, 80 N.E.3d 318 (Mass. 2017) (No. SJC-12254) (arguing search violated Mauricio's expectation of privacy in digital data). Mauricio argued that the right to privacy in one's stored digital information is protected from state intrusion under both the Fourth Amendment to the United States Constitution and Article 14. *See* Brief and Record Appendix of Appellant, Kevin A. Mauricio, *supra*, at 16-17. Ultimately, the SJC declined to address the constitutionality of expanding Fourth Amendment protections of cell phone data to data stored on digital cameras. *See* 80 N.E.3d at 323-24. In its opinion, the SJC also analyzed Mauricio's standing issues and whether the prosecution introduced sufficient evidence to sustain a conviction for receiving stolen property exceeding $250 in value; these issues are outside the scope of this Case Comment. *See id.* at 320, 324, 326; *see also* Commonwealth v. Seng, 766 N.E.2d 492, 503 (Mass. 2002) (describing standard for valid inventory search). In Massachusetts, a valid inventory search is "justified to safeguard the defendant's property, protect the police against later claims of theft or lost property, and keep weapons and contraband from the prison population." Commonwealth v. Seng, 766 N.E.2d 492, 503 (Mass. 2002). Searches incident to arrests are limited to "personal property . . . immediately associated with the person of the arrestee." United States v. Chadwich, 433 U.S. 1, 14-15 (1977),

of the digital camera's data was invalid because it exceeded the scope of the search-incident-to-arrest exception and was an invalid inventory search.[5]

On May 28, 2014, police in Taunton, Massachusetts, responded to a report that two suspicious individuals were seen running out of the side door of a residence.[6] Shortly thereafter, Taunton police located and stopped two suspects matching the witness's description, one of whom was the defendant, Kevin Mauricio.[7] The police pat frisked Mauricio and conducted a search of his backpack, which resulted in the discovery of a digital camera, among other items.[8] The police ultimately arrested Mauricio and transported him to the local police station, where the police conducted an inventory search of Mauricio's backpack.[9]

During the inventory search, Taunton police Detective Dora Treacy discovered a digital camera and turned it on, hoping to find information related to the camera's true owner.[10] The digital images did not contain any evidence suggesting Mauricio stole the camera; however, Detective Treacy discovered a

abrogated by California v. Acevedo, 500 U.S. 565 (1991). Such searches are justified to protect the potential loss of evidence and law enforcement safety. *Id.* at 14.

5. *See* 80 N.E.3d at 321-22 (holding Massachusetts Constitution requires suppression of evidence from seized digital camera); *see also* George L. Blum, Annotation, *Validity of Search of Digital Camera and Associated Memory Cards*, 94 A.L.R. 6th 371, § 6 (Supp. 2018) (summarizing part of *Mauricio* holding pertaining to search-incident-to-arrest application). In reaching its conclusion, the SJC relied upon the reasoning employed by the United States Supreme Court in *Riley*—where the search of a cell phone incident to an arrest was held to be invalid—by similarly finding that the search of the digital camera was also excluded from the search-incident-to-arrest exception. *See* 80 N.E.3d at 322-24 (suggesting *Riley* reasoning excludes digital cameras from exception, but basing decision on Article 14). In *Riley*, the Supreme Court held that the warrantless search of a cell phone does not qualify for the search-incident-to-arrest exception because the search of a cell phone would neither prevent the destruction of evidence nor protect officers' safety. *See* Riley v. California, 134 S. Ct. 2473, 2484-85 (2014). Following suit, the SJC applied the same reasoning in finding that data on digital cameras likewise would not pose a significant threat to officer safety or lead to the destruction of evidence, and as such, the search-incident-to-arrest exception did not apply. *See* 80 N.E.3d at 322-23. Additionally, the SJC determined that Detective Dora Treacy's search of the data contained in the digital camera constituted an invalid inventory search because it was not carried out to inventory and retain custody of the item; instead the court found the search to be investigatory in nature. *See id.* at 325.

6. 80 N.E.3d at 320 (noting robbery took place on Downing Street); Commonwealth's Brief at 10, Commonwealth v. Mauricio, 80 N.E.3d 318 (Mass. 2017) (No. SJC-12254) (providing Commonwealth's detailed statement of facts).

7. *See* 80 N.E.3d at 320-21 (indicating law enforcement discovered potential suspects); *see also* Commonwealth's Brief, *supra* note 6, at 10-12 (describing circumstances justifying police search of Mauricio's backpack). Taunton Police Officer Collins stated: "[D]efendant [Mauricio] indicated that in fact the backpack did contain needles." Commonwealth's Brief, *supra* note 6, at 11.

8. *See* 80 N.E.3d at 320-21 (indicating police searched Mauricio at time of arrest). Mauricio's backpack contained numerous items, including digital cameras and electronic cords, a Bose sound docking station, jewelry, money, prescription pills, and needles. *See* Commonwealth's Brief, *supra* note 6, at 11.

9. *See* 80 N.E.3d at 320-21 (describing Taunton police encounter with Mauricio related to witnessed breaking and entering); Commonwealth's Brief, *supra* note 6, at 10-12 (identifying factor's giving rise to discovery of digital camera).

10. *See* 80 N.E.3d at 321 (describing Detective Treacy's inventory search and procedure).

photograph depicting Mauricio posing with firearms.[11] Subsequently, Taunton police attempted to identify the firearms in the image by comparing them to firearms stolen during a prior residential break-in.[12]

After comparing the two sets of firearms, the police determined that the firearms in the photograph matched the ones stolen from the earlier break-in.[13] Consequently, the police charged Mauricio with carrying a firearm without a license and receiving stolen property.[14] Mauricio filed a motion to suppress the images from the digital camera, alleging that the police viewed the images only as a result of an improper warrantless inventory search of his digital camera, and as an invalid search incident to the arrest.[15] The trial court denied the motion, and the jury convicted Mauricio on both counts.[16] On appeal, the SJC vacated Mauricio's conviction for carrying a firearm without a license.[17] In so doing, the SJC determined that the search of the digital camera could not be justified as an inventory search, and did not fall within the search-incident-to-arrest exception to the warrant requirement.[18]

11. *See id.* (noting Detective Treacy came across photo of man with firearms); *see also* Commonwealth's Brief, *supra* note 6, at 12-13 (summarizing search of digital camera and describing incriminating photograph). *But see* Brief and Record Appendix of Appellant, Kevin A. Mauricio, *supra* note 4, at 4-5 (presenting testimony regarding search of digital camera). Counsel for Mauricio stated that Detective Treacy knew the camera contained a number of images, and yet, she continued to look through the images without any proof the camera was stolen. *See id.*

12. *See* 80 N.E.3d at 321 (summarizing police department's efforts to identify owner of firearms); Brief and Record Appendix of Appellant, Kevin A. Mauricio, *supra* note 4, at 5-6 (summarizing Taunton police's open investigation relating to recent "housebreak"). The earlier break-in occurred on May 12, 2014, over two weeks before Mauricio's arrest in connection to the Downing Street break-in. *See* Brief and Record Appendix of Appellant, Kevin A. Mauricio, *supra* note 4, at 5-6.

13. *See* 80 N.E.3d at 321 (describing investigatory steps taken to identify firearms).

14. *See id.* at 320 (summarizing charges brought against Mauricio). The government charged Mauricio with two offenses: for possession of a firearm without a license in violation of chapter 269, section 10(a) of the Massachusetts General Laws, and for receiving stolen property in excess value of $250 in violation of chapter 266, section 60 of the Massachusetts General Laws. *Id.*

15. *See id.* at 321-22 (identifying progression of trial motions). Mauricio filed two motions to suppress, the first sought to suppress "all physical evidence and any alleged statements obtained by law enforcement authorities as a result of the search and seizure by the Taunton police department." *Id.* at 321. The trial court originally granted the first motion before reconsidering the issue and denying the motion after the Commonwealth filed a motion for reconsideration. *Id.* Mauricio then filed a second motion that specifically addressed the search of the digital camera; but the court denied this motion, concluding that the police searched the digital camera pursuant to a valid inventory search. *Id.*

16. *See id.* at 320-21 (noting motion denied and Mauricio convicted of both charges).

17. *See* 80 N.E.3d at 327 (reversing Mauricio's motion to suppress images which ultimately resulted in one vacated conviction). The SJC held "that the search of data contained in digital cameras falls outside the scope of the search-incident-to-arrest exception to the warrant requirement." *Id.* at 324. Furthermore, the SJC found the inventory search of the digital camera to be investigatory in nature and therefore invalid. *Id.* at 325.

18. *See id.* at 324-27 (outlining SJC's reasoning in reversing motion to suppress). The SJC held the inventory search to be invalid because Detective Treacy searched for information regarding the camera's true owner, making the search investigatory in nature. *See id.* at 325. Further, the search of images on the digital camera was not justified as a search incident to the arrest because the data did not pose a threat to officer safety, and the police had secured the device, thereby mitigating the threat of evidence destruction. *See id*. at 323.

In 1967, the United States Supreme Court expanded the scope of the Fourth Amendment protection against unreasonable searches and seizures to include electronic wiretaps of telephone communications in *Katz v. United States*.[19] That same year, in *Berger v. New York*[20]—a case involving an electronic recording device—the Supreme Court attempted to achieve a balance between traditional searches of tangible objects and the evolving technology of electronic surveillance by declaring the unconstitutionality of indiscriminate electronic eavesdropping.[21] Since *Katz* and *Berger*, the Supreme Court has continued to apply the Fourth Amendment to digital communications.[22]

Around the same time the Supreme Court decided *Katz* and *Berger*, the Court affirmed the bright-line rule for police searches incident to a lawful arrest as an exception to the Fourth Amendment warrant requirement: Police may conduct a warrantless search of both the arrestee and the area within the arrestee's control to identify physical objects that may pose a risk to officer safety.[23] In *United States v. Robinson*,[24] during a pat frisk of the defendant, the officer felt an object in the defendant's jacket pocket that turned out to be a cigarette pack containing heroin capsules.[25] Whether this exception applies to digital devices has become a question courts are struggling to answer and application of this bright-line rule to digital devices, such as cell phones, has become problematic given their potentially unlimited storage capacity.[26]

19. 389 U.S. 347, 353, 359 (1967) (holding warrantless wiretapping of telephone communications violated Fourth Amendment). The Supreme Court was careful to point out that the Fourth Amendment protection against unreasonable searches and seizures does not only cover tangible items, and extends beyond technical trespass. *See id.* at 353. Furthermore, the Supreme Court explained that the determination of a Fourth Amendment violation is not contingent upon "presence or absence" of physical invasions of privacy because the Fourth Amendment protects people, not simply places or things. *See id.*

20. 388 U.S. 41 (1967).

21. *See* Berger v. New York, 388 U.S. 41, 44, 58-60 (1967) (declaring warrantless electronic eavesdropping unconstitutional). Particularly troubled by the indiscriminate nature of the electronic eavesdropping statute at-issue, the *Berger* Court emphasized its concern with "the statute's failure to describe with particularity the conversations sought," because this gave law enforcement free rein to "'seize' any and all conversations." *Id.* at 59.

22. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 522 (2001) (summarizing decades-long protection of oral and electronic communications); *see also* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 552-53 (2017) (describing recent evolution of Fourth Amendment protection of electronic devices).

23. *See* United States v. Robinson, 414 U.S. 218, 224 (1973) (promulgating warrant exception for searches incident to arrest). In *Robinson*, the Supreme Court upheld the constitutionality of the search of a container on the arrestee's person, stating that law enforcement personnel are entitled to inspect objects they come across during a search incident to arrest. *See id.* at 236. The longstanding search-incident-to-arrest exception allows officers to search both the person and the area within the arrestee's control. *See id.* at 224. This exception is justified by law enforcement's need to search for weapons and to prevent the destruction of evidence. *See* United States v. Edwards, 415 U.S. 800, 802-03 (1974).

24. 414 U.S. 218 (1973).

25. *See* United States v. Robinson, 414 U.S. 218, 221-23 (1973) (describing factual scenario of search in *Robinson*).

26. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 292-93 (2005) (discussing incompatibility between existing search doctrine and application to modern digital

In *Riley v. California*,[27] the Supreme Court considered whether law enforcement officials may conduct warrantless searches of digital information on cell phones seized from lawfully arrested individuals.[28] The Supreme Court balanced law enforcement concerns against personal privacy interests in digital data stored on cell phones and refused to extend the *Robinson* search-incident-to-arrest rule; instead the Court held that generally, the police may not search digital information on a cell phone seized incident to a lawful arrest without a warrant.[29] The Supreme Court distinguished searching cell phones—which contain vast amounts of personal information that implicates significantly greater personal privacy interests—from the limited physical search at issue in *Robinson*.[30] In discussing these privacy interests, the Supreme Court noted how "a cell phone collects in one place many distinct types of information" that could amount to "the sum of an individual's private life [being] reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[31] Given the substantial privacy interests at stake when digital data is involved, the Supreme Court declined to permit warrantless searches of cell phones seized during an arrest.[32] Since *Riley*, state and federal courts have

searches); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 403, 403 n.1, 404-05 (2013) (summarizing how cell phone searches have challenged courts and illustrating circuit split on this issue); *see also* Elizabeth S. Myers, Note, *Containing Cell Phones? Restoring the Balance Between Privacy and Government Interests in Fourth Amendment Cell Phone Searches and Seizures*, 48 SUFFOLK U. L. REV. 203, 204-05 (2015) (overviewing several approaches to warrantless searches of cell phones). Prior to *Riley*, there was a jurisdictional split as to whether a warrant should be required to conduct a search of digital data on a cell phone. *See* Myers, *supra*, at 215-17 (detailing circuit split).

27. 134 S. Ct. 2473 (2014).

28. *See* Riley v. California, 134 S. Ct. 2473, 2480 (2014) (stating issue before Supreme Court).

29. *See* Riley v. California, 134 S. Ct. 2473, 2485, 2495 (2014) (announcing Supreme Court's holding). In declining to adopt the *Robinson* test, the Supreme Court explicitly stated that the rationale from *Robinson*—that an individual's privacy interests in property are diminished when in custody—is not appropriate with respect to digital evidence. *See id.* at 2484-85.

30. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (distinguishing digital data searches from physical searches and highlighting impracticality of applying existing doctrines); *see also* Marjorie A. Shields, Annotation, *Validity of Search of Wireless Communication Devices*, 62 A.L.R. 6th 161, §§ 6-7 (2018) (summarizing pre- and post-*Riley* case law determining validity of electronic device searches incident to arrest).

31. *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (discussing cell phone storage and impact on personal privacy).

32. *See* Riley v. California, 134 S. Ct. 2473, 2485, 2491 (2014) (discussing individuals' privacy interests in digital data). The Supreme Court declined to extend the *Robinson* rule to searches of cell phones because digital information does not present a safety risk to officers and does not create a serious and unavoidable risk of evidence being destroyed. *See id.* at 2484-87; *see also* 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, 48-49 (2012) (noting risks of evidence preservation and officer safety insufficient to support warrantless cell phone searches); Alexandra Gioseffi, Comment, Lichtenberger, Sparks, *and* Wicks*: The Future of the Private Search Doctrine*, 66 EMORY L.J. 395, 429 (2017) (asserting electronic devices differ from physical containers).

addressed arguments analogizing digital cameras to cell phones because of their ability to store substantial amounts of information.[33]

Federal and state courts continue to grapple with expanding the holding in *Riley* to other items, including digital cameras, because the Supreme Court has yet to decide whether the Fourth Amendment protections applicable to cell phones also extend to other electronic devices.[34] Similalr to the Fourth Amendment, Article 14 of the Massachusetts Constitution governs inventory searches, searches incident to arrest, and searches of seized items and digital data.[35] Pursuant to Article 14, the SJC has the authority to decide a case on state grounds instead of federal grounds "[b]ecause the Massachusetts Declaration of Rights is a sovereign document."[36] The SJC has interpreted Article 14 to require law enforcement to obtain a warrant prior to searching digital data contained on seized devices, such as cell phones.[37] Due to the

33. *See* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (extending *Riley*'s protection over cell phones to digital cameras). In *Whiteside*, the District Court for the Southern District of New York analogized digital cameras that possess immense amounts of information to cell phones. *See id.* at *4-5; *see also* United States v. Miller, 34 F. Supp. 3d 695, 699-700 (E.D. Mich. 2014) (citing differences between digital cameras and cell phones in declining to extend *Riley*); Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1171 (D. Or. 2012) (concluding warrantless search of digital camera violated Fourth Amendment prior to *Riley*).

34. *Compare* Riley v. California, 134 S. Ct. 2473, 2487-89 (2014) (concluding cell phone data implicates privacy concerns), *and* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4-5 (S.D.N.Y. June 29, 2015) (analogizing data storage capacity in digital cameras to cell phones), *with* United States v. Miller, 34 F. Supp. 3d 695, 699-700 (E.D. Mich. 2014) (distinguishing cameras with limited storage from cell phones and declining to extend *Riley*), *and* Am. News & Info. Servs., Inc. v. Gore, No. 12-CV-2186 BEN (KSC), 2014 WL 4681936, at *9-10, *15 (S.D. Cal. Sept. 18, 2014) (analyzing Fourth Amendment dicta in context of camera search, but deciding on other grounds). The District Court for the Southern District of California discussed how a video camera falls somewhere between searching a cigarette pack and a cell phone. Am. News & Info. Servs., Inc. v. Gore, No. 12-CV-2186 BEN (KSC), 2014 WL 4681936, at *10 (S.D. Cal. Sept. 18, 2014).

35. *See* MASS. CONST. pt.1, art. XIV (establishing warrant requirement in Massachusetts to protect against unreasonable searches and seizures); Commonwealth v. White, 12 N.E.3d 348, 351-53 (Mass. 2014) (describing search-incident-to-arrest and inventory search exceptions to warrant requirement); Commonwealth v. Seng, 766 N.E.2d 492, 503 (Mass. 2002) (emphasizing need to conduct inventory searches in noninvestigatory manner); *see also* Commonwealth v. Dyette, 32 N.E.3d 906, 916-17 (Mass. App. Ct. 2015) (holding warrantless search of smartphone violated Fourth Amendment where no exigent circumstances present).

36. *See* Joseph A. Grasso, Jr., *"John Adams Made Me Do It": Judicial Federalism, Judicial Chauvinism, and Article 14 of Massachusetts Declaration of Rights*, 77 MISS. L.J. 315, 317-18 (2007) (stating Massachusetts need not "walk in lockstep with . . . Supreme Court[]"); Roderick L. Ireland, *How We Do It in Massachusetts: An Overview of How the Massachusetts Supreme Judicial Court Has Interpreted Its State Constitution to Address Contemporary Legal Issues*, 38 VAL. U. L. REV. 405, 407 (2004) (discussing SJC's obligation to uphold Massachusetts law); *see also* Commonwealth v. Blood, 507 N.E.2d 1029, 1033 n.9 (Mass. 1987) (indicating Article 14's enhanced substantive protection); Commonwealth v. Upton, 476 N.E.2d 548, 556 (Mass. 1985) (concluding Article 14 provides greater protection than Fourth Amendment in probable cause determinations).

37. *See* MASS. CONST. pt.1, art. XIV (certifying warrant requirement); Commonwealth v. White, 59 N.E.3d 369, 371-72, 374-76 (Mass. 2016) (applying Article 14's warrant requirement to cell phone searches); *see also* Commonwealth v. Dorelas, 43 N.E.3d 306, 312 (Mass. 2016) (acknowledging warrant requirement and need for probable cause in electronic data searches). In *Dorelas*, the SJC affirmed the warrant requirement

evolving development of technology, digital cameras and memory cards now possess increased storage capacity, likening them to cell phones that are afforded heightened protection.[38]

In *Mauricio*, the SJC reversed an order denying a motion to suppress images from a digital camera, determining that the search of the digital camera was invalid for two reasons: First, the inventory search exceeded the scope of a valid inventory search, and second, the search of the digital camera following the arrest fell outside the permissible scope of the search-incident-to-arrest exception to the warrant requirement.[39] The SJC had no trouble declaring the search invalid once it determined that Detective Treacy conducted a search that was investigatory in nature by actively turning on the camera to view its digital contents.[40] This type of search is at odds with the purpose of the inventory search exception to the warrant requirement—to account for all items and safeguard the arrested party's property—and thus exceeded the boundaries of the exception.[41]

The reasoning that led the SJC to conclude that the search of the digital camera's data fell outside of the search-incident-to-arrest exception was somewhat less straightforward.[42] The SJC heavily relied on the reasoning employed by the Supreme Court in *Riley* to exclude digital cameras from the search-incident-to-arrest exception without directly extending the *Riley* holding to digital cameras altogether.[43] The SJC found the *Riley* Court's focus on the

for searches of electronic devices, and emphasized that such warrants must be particularized in scope, clearly state what the officer is seeking, and specify where in the device he or she will search. *See* Commonwealth v. Dorelas, 43 N.E.3d 306, 312 (Mass. 2016). To illustrate the need for such a narrow standard, the court drew a comparison between the physical and virtual worlds: In the physical world, law enforcement is limited in its search to the physical boundary of a building or container itself; in contrast, no such boundaries exist in the virtual world and thus, a search could extend infinitely into however much data is accessible through the device. *See id.*

38. *See* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (pointing out similarity of digital camera storage capacity to cell phone storage capacity); RICK AYERS ET AL., NAT'L INST. OF STANDARDS AND TECH., U.S. DEP'T OF COMMERCE, SPECIAL PUB. NO. 800-101, GUIDELINES ON MOBILE DEVICE FORENSICS 3 (2014), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf [https://perma.cc/9WEE-2PV8] (summarizing storage capabilities of mobile devices). The National Institute of Standards and Technology's report suggests digital cameras with memory cards function similarly to cell phones and other mobile devices due to their multimedia storage capabilities. *See* AYERS ET AL., *supra*, at 3-4.

39. *See* 80 N.E.3d at 324-25, 327 (stating SJC's conclusion).

40. *See id.* at 325 (summarizing Detective Treacy's actions).

41. *See id.* at 325 (identifying inconsistencies with Detective Treacy's search and purposes of inventory searches); Commonwealth v. White, 12 N.E.3d 348, 353 (Mass. 2014) (stressing inventory searches procedurally regulated); Commonwealth v. Seng, 766 N.E.2d 492, 504-05 (Mass. 2002) (outlining principles distinguishing inventory searches from investigatory searches); *see also* MASS. CONST. pt. 1, art. XIV.

42. *See* 80 N.E.3d at 322 (noting Supreme Court has grappled with defining search-incident-to-arrest exception).

43. *See id.* at 322-24 (deciding case on Article 14, not Fourth Amendment grounds); Commonwealth v. Madera, 521 N.E.2d 738, 740 (Mass. 1988) (explaining Article 14 potentially more protective than Fourth Amendment); *see also* Riley v. California, 134 S. Ct. 2473, 2488-89 (2014) (reasoning cell phones implicate significant privacy concerns).

tremendous amount of personal information storable on a digital device particularly important.[44] While acknowledging that digital cameras do not allow for the same type or extent of data storage as cell phones, the SJC nonetheless felt that the similarities between the two types of devices were compelling enough to merit a similar holding in *Mauricio* as in *Riley*.[45] The SJC declined to address the constitutionality of warrantless searches of digital cameras on Fourth Amendment grounds—because the Supreme Court has not yet addressed the issue—and instead based its determination on Article 14.[46]

Pursuant to Article 14, the SJC concluded that the Commonwealth failed to show that the facts surrounding the search of the digital camera excluded it from the search warrant requirement.[47] Specifically, the SJC noted that the situation involved neither a threat to officer safety nor the destruction of evidence, and there was sufficient time for law enforcement to obtain a warrant.[48] Therefore, because the search was not conducted incident to arrest, the SJC held that the photographic evidence gathered as a result of the improper search must be suppressed as a matter of law, and accordingly, vacated Mauricio's conviction for carrying a firearm without a license.[49]

Because the SJC concluded that Detective Treacy impermissibly searched the data contained in the digital camera, the SJC properly rendered the photographic evidence discovered from the memory card of the digital camera inadmissible.[50] Furthermore, the SJC's decision to apply the Supreme Court's reasoning in *Riley* to illustrate that digital cameras and cell phones implicate similar privacy concerns, without expanding *Riley* to digital camera searches, was an effective method to determine the search's validity under Article 14.[51]

44. *See* 80 N.E.3d at 323 (discussing quantity of information digital camera can store); *see also* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) (noting storage capacity of digital cameras compared to smartphones); *cf.* United States v. Miller, 34 F. Supp. 3d 695, 700 (E.D. Mich. 2014) (postulating digital cameras do not store same amount of information present in cell phones).

45. *See* 80 N.E.3d at 322-24 (articulating *Riley*'s reasoning pursuant to Article 14 jurisprudence); *see also* Riley v. California, 134 S. Ct. 2473, 2489-90 (2014) (identifying reasons to distinguish cell phone data from physical records).

46. *See* 80 N.E.3d at 324 (basing decision on Article 14 grounds); *see also* Commonwealth v. Madera, 521 N.E.2d 738, 740-41 (Mass. 1988) (ruling on Article 14 grounds without regard to Fourth Amendment); Commonwealth v. Blood, 507 N.E.2d 1029, 1033 n.9 (Mass. 1987) (recognizing increased substantive protections under Article 14); Commonwealth v. Upton, 476 N.E.2d 548, 556 (Mass. 1985) (suggesting Article 14 may be more protective than Fourth Amendment).

47. *See* 80 N.E.3d at 322-24 (discussing facts of search incident to arrest).

48. *See id.* at 323-24 (stating "twin threats" mitigated). Importantly, the SJC discussed how the digital camera in police custody nearly eliminated the threats of officer safety and destruction of evidence. *See id.* at 324.

49. *See id.* at 327 (reiterating holding).

50. *See id*. at 325-26 (noting Article 14 required exclusion of evidence due to warrantless search without permissible exception).

51. *See* 80 N.E.3d at 323-24 (refusing to extend *Riley* to digital cameras); Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012) (observing vast personal information storage capacity of digital cameras); AYERS ET AL., *supra* note 38, at 3-4 (comparing functionality of multiple mobile devices). *But see* United States v. Miller, 34 F. Supp. 3d 695, 699-700 (E.D. Mich. 2014) (suggesting digital cameras store less personal

Although Article 14 may afford substantive protection to individuals and their digital privacy, federal Fourth Amendment jurisprudence on the issue is relatively uncertain without a Supreme Court ruling.[52] The SJC also correctly dismissed the Commonwealth's argument that the lack of a computerized function differentiates digital cameras from cell phones under a *Riley* analysis, because relying upon such a small distinguishing factor would result in muddled jurisprudence.[53] By applying *Riley*'s reasoning in the context of Article 14—and not *Robinson*'s bright-line, search-incident-to-arrest rule—the SJC expanded the types of digital devices that Massachusetts law enforcement officers cannot search without a warrant.[54]

In *Riley*, the Supreme Court reviewed the *Robinson* exception to the search warrant requirement which allows officers to search a person and their belongings during an arrest to promote the safety of the officers and to prevent the destruction of evidence.[55] In *Robinson*, the Court reasoned that unknown physical objects could pose threats to officer safety during searches conducted

information than cell phones). The SJC will often decide cases under Article 14 in providing protections which have not yet been decided on or granted by the Supreme Court. *See* Grasso, *supra* note 36, 317-18 (examining SJC's independent interpretation of Massachusetts Constitution); Ireland, *supra* note 36, at 407-10 (reviewing SJC's tendency to rely on Massachusetts Constitution to grant protections not federally recognized).

52. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014) (describing Fourth Amendment privacy protection for information on cell phones); 80 N.E.3d at 323-24 (characterizing Article 14's substantive protection and Supreme Court's lack of determination on digital cameras). When analyzing a warrantless search of a digital camera, a federal court's outcome is uncertain because the Supreme Court has yet to determine if *Riley* is applicable to digital cameras. *See* 80 N.E.3d at 323; *see also* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (providing insight into how courts will balance competing interests through discussion of camera search cases); Commonwealth v. Upton, 476 N.E.2d 548, 556 (Mass. 1985) (providing support for Article 14's tendency to provide greater protection than Fourth Amendment). The SJC has concluded that rulings based on Article 14, as opposed to those based on the Fourth Amendment, require more precision and definitiveness. *See* Commonwealth v. Upton, 476 N.E.2d 548, 556 (Mass. 1985).

53. *See* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170-71 (D. Or. 2012) (holding digital cameras precluded from warrantless search under Fourth Amendment for similar reason); 80 N.E.3d at 323 (disregarding evidence destruction argument given lack of Internet connectivity and unlikelihood of remote wiping). The law may become convoluted if state courts begin applying an Internet connectivity factor to determine which digital devices are worthy of heightened protection instead of applying the existing *Riley* framework. *See* Brief and Record Appendix of Appellant, Kevin A. Mauricio, *supra* note 4, at 22-24.

54. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014) (restating warrant requirement); 80 N.E.3d at 322-23 (holding digital cameras not excluded from warrant requirement under Article 14); *see also* Commonwealth v. Madera, 521 N.E.2d 738, 740 (Mass. 1988) (acknowledging Article 14 more protective than Fourth Amendment for Massachusetts citizens). The SJC's ruling prevents the Commonwealth from appealing the vacation of Mauricio's conviction to the Supreme Court because the decision was not based on a federal constitutional issue; instead, the SJC relied upon the robust protection against unreasonable searches and seizures provided by Article 14 jurisprudence. *See* 80 N.E.3d at 322-24. The SJC's decision in *Mauricio* may also curb the government's ability to produce evidence in future litigation, because law enforcement is now required to obtain a warrant before searching digital cameras. *See id.* at 324-25.

55. *See* Riley v. California, 134 S. Ct. 2473, 2484-85 (2014) (concluding inherent risks justifying search-incident-to-arrest doctrine in *Robinson* not present in cell phone data); United States v. Robinson, 414 U.S. 218, 224 (1973) (discussing differing interpretations of area within arrestee's control).

as incident to an arrest.[56] Nevertheless, the *Riley* Court determined that extending the application of the *Robinson* rule to cell phones would be inappropriate given the unlikelihood that electronic data on a digital camera would put an arresting officer in harm's way.[57] For example, in *Mauricio*, the safety of officers did not depend on searching the digital images contained in the camera because the device was already in police custody.[58] Furthermore, the evidence stored in the digital camera was not in danger of being remotely destroyed because it was impossible to remotely erase the images without Internet connectivity.[59] In summary, it is proper to require a warrant before law enforcement can conduct a search of a digital camera and delve into the extensive private information contained on such devices.[60]

The SJC tailored the reasoning in *Riley* to reveal how digital cameras and cell phones implicate analogous privacy concerns.[61] This determination results in a clearer and more efficient standard for searches of digital cameras discovered at the time of an arrest; generally, law enforcement must first obtain a warrant before searching the data on a digital camera.[62] Although circuit courts have not yet decided whether the protections that the Supreme Court afforded cell phones applies to other digital devices, federal courts should follow the district court's decision in *Whiteside* and require a warrant to search digital cameras found during a search incident to arrest.[63] Thus, the SJC

56. *See* United States v. Robinson, 414 U.S. 218, 226, 236 (1973) (holding search and seizure of person and items within control permissible under Fourth Amendment).

57. *See* Riley v. California, 134 S. Ct. 2473, 2484-85 (2014) (declining to extend *Robinson*'s categorical rule to cell phone data).

58. *See* 80 N.E.3d at 323 (surmising digital cameras pose less risk than cell phones).

59. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (acknowledging potential risk to officer safety posed by unknown physical objects, but not digital data); 80 N.E.3d at 323 (discussing twin threats of harm and evidence destruction); MacLean, *supra* note 32, at 48-51 (justifying failure of cell phone data to meet either exigency threat). The SJC focused its reasoning on highlighting how digital data within the camera does not endanger officers when secured, and how evidence is not at risk of being remotely destroyed when the camera lacks Internet connectivity. *See* 80 N.E.3d at 323.

60. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (declaring warrant required for search of cell phones); United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (stating warrant requirement in *Riley* applicable to digital cameras); 80 N.E.3d at 322 (applying *Riley* reasoning to state constitutional analysis). Similar to *Mauricio*, *Whiteside* involved a digital camera that stored photographs on a memory card. *See* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *1 (S.D.N.Y. June 29, 2015). Before the officer was able to view the camera's data, he had to remove the memory card from the digital camera and insert it into a computer. *See id.*

61. *See* 80 N.E.3d at 323 (discussing digital camera's ability to reveal individual's intimate private life details).

62. *See id.* at 324 (highlighting digital cameras fall outside search-incident-to-arrest exception to warrant requirement); *see also* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (comparing evidence seized from cell phone in *Riley* to evidence contained in digital camera). The *Riley* Court emphasized that "the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery." Riley v. California, 134 S. Ct. 2473, 2493 (2014).

63. *See* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) (protecting devices with vast storage capacity from warrantless searches); 80 N.E.3d at 324 (noting

correctly applied the principles established in *Riley*, which generally protect cell phones from warrantless searches to the digital camera context.[64]

In *Mauricio*, the SJC encountered the question of whether the Fourth Amendment's general requirement to obtain a warrant before searching cell phones should extend to searches of digital cameras. The SJC was careful not to rule on this unsettled Fourth Amendment issue, and instead applied the reasoning from *Riley* and the more robust protections of Article 14 to ultimately hold that, because digital cameras implicate similar privacy interests to cell phones—which the Supreme Court has already granted heightened protection—law enforcement officers must obtain a warrant before conducting a search of data stored on a digital camera. Consequently, the SJC held evidence on Mauricio's digital camera inadmissible because officers had ample time to obtain a search warrant while the digital camera remained in police custody. As this body of law grows, courts should look to *Mauricio* when evaluating how to effectively protect individual privacy rights in an age where digital devices are nearly inseparable from the individual.

Matthew Rosencranz

officers had opportunity to obtain search warrant for digital camera); Gioseffi, *supra* note 32, at 428 (discussing preference for warrant requirements); MacLean, *supra* note 32, at 67-68 (suggesting additional fact-specific tests strain courts). Although the SJC discussed *Whiteside* in a footnote, both courts followed *Riley*'s line of reasoning to establish greater protection for devices with extensive storage capacity, and determined that digital cameras fall outside the search-incident-to-arrest exception. *See* 80 N.E.3d at 323 n.1; *see also* United States v. Whiteside, No. 13 Cr. 576(PAC), 2015 WL 3953477, at *4-5 (S.D.N.Y. June 29, 2015) (recognizing similar concerns present in digital camera and cell phone searches).

64. *See* 80 N.E.3d at 322-24 (justifying logic of warrant requirement for digital cameras); *see also* Riley v. California, 134 S. Ct. 2473, 2489-91 (2014) (discussing significance of private information accessible through cell phones and acknowledging consequences of warrantless searches).