Brooklyn Law Review

Volume 80 | Issue 2

Article 5

2015

Reading *Riley* Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest

Tristan M. Ellis

Follow this and additional works at: https://brooklynworks.brooklaw.edu/blr

Recommended Citation

Tristan M. Ellis, *Reading Riley Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest, 80 Brook. L. Rev. (2015).* Available at: https://brooklynworks.brooklaw.edu/blr/vol80/iss2/5

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Brooklyn Law Review by an authorized editor of BrooklynWorks.

Reading Riley Broadly

A CALL FOR A CLEAR RULE EXCLUDING ALL WARRANTLESS SEARCHES OF MOBILE DIGITAL DEVICES INCIDENT TO ARREST

INTRODUCTION

Mobile digital devices play an increasingly prevalent role in American life.¹ A recent Pew Research Center study estimates that 91% of American adults own a cellular phone, and approximately 56% own a "smartphone"²—an item not defined by the study,³ but "may be thought of as a handheld computer integrated within a mobile telephone."⁴ By comparison, only 73% of American adults owned a cell phone in 2006.⁵ Similarly, tablet computer ownership has quickly risen from 4% in 2010, to 34% in 2013.⁶ These figures illustrate how rapidly consumers adapt to technological changes.

The ubiquity of mobile technology in American society highlights the need for clear Fourth Amendment standards that may be readily applied to emerging technology by law enforcement officials, courts, and citizens alike.⁷ At first blush,

⁴ William L. Hosch, *Smartphone*, BRITANNICA ONLINE ENCYCLOPEDIA (Oct. 3, 2013), http://www.britannica.com/EBchecked/topic/1498102/smartphone.

- ⁵ Brenner, *supra* note 2.
- ⁶ Id.

⁷ See Riley v. California, 134 S. Ct. 2473, 2491 (2014) (noting the Court's "general preference to provide clear guidance to law enforcement through categorical rules"); Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: Applying the Search-Incident-To-Arrest Exception to the Cell Phone as "Hybrid*", 60 DRAKE L. REV.

¹ See Riley v. California, 134 S. Ct. 2473, 2484, 2489-90 (2014) (noting that "modern cell phones... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

² Joanna Brenner, *Pew Internet: Mobile*, PEW INTERNET (Sept. 18, 2013), http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

³ The study relies on users to define the nature of the device, that is, whether "cell phone owners say that their phone is a smartphone," and similarly, whether "cell phone owners say that their phone operates on a smartphone platform common to the U.S. market." Aaron Smith, *Smartphone Ownership 2013*, PEW INTERNET (June 5, 2013), http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx.

the question of what happens to a person's mobile device when she or he is arrested may not seem to bear on the lives of most device users. However, the gravity of this question is heightened by the fact that a police officer may, without a warrant, arrest a person for "committ[ing] even a very minor criminal offense in his presence,"8 even if state law does not authorize an arrest for the particular offense.⁹ Indeed, some scholars have found that one in three Americans will be arrested by age 23.¹⁰ Moreover, when executing an arrest, "it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."11 This authority to search extends to "the area within the control of the arrestee,"¹² that is, "the area into which an arrestee might reach in order to grab . . . evidentiary items."¹³ The Supreme Court has begun to offer clarity as to how this authority to search interplays with mobile digital technology. In Riley v. California, the Supreme Court erred on the side of privacy and held that police officers must obtain a warrant before searching a cell phone, "even when a cell phone is seized incident to arrest."¹⁴ Before *Riley*, courts struggled over the degree to which the "well settled [and] ... traditional exception to the warrant requirement of the Fourth Amendment"¹⁵ applied to cellular phones and smartphones.¹⁶

- ⁸ Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001).
- ⁹ Virginia v. Moore, 553 U.S. 164, 166-67, 176 (2008).

- ¹¹ Chimel v. California, 395 U.S. 752, 762-63 (1969).
- ¹² United States v. Robinson, 414 U.S. 218, 224 (1973).
- ¹³ Chimel, 395 U.S. at 763.
- ¹⁴ Riley v. California, 134 S. Ct. 2473, 2493 (2014).
- ¹⁵ *Robinson*, 414 U.S. at 224.

^{429, 480 (}noting the need for "a bright-line rule that can be readily applied by officers in the field"); *see also* Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 58 (2008) (noting that, with respect to specific proposals to address the search-incident-to-arrest rule outlined in the article, "despite the flaws associated with each proposal, all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant").

¹⁰ Robert Brame, et al., *Cumulative Prevalence of Arrests from Ages 8 to 23 in a National Sample*, 129 PEDIATRICS, Jan. 2012, at 21, 25, *available at* http://pediatrics.aappublications.org/content/early/2011/12/14/peds.2010-3710.full.pdf. The study is controlled for race. *Id.* at 22 (noting "a supplemental oversample of minority youth").

¹⁶ See, e.g., United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), aff'd sub nom. Riley v. California, 134 S. Ct. 2473, 2493 (2014); United States v. Murphy, 552 F.3d 405 (4th Cir. 2009), cert. denied, 556 U.S. 1196 (2009); Smallwood v. State, 113 So. 3d 724 (Fla. 2013); State v. Smith, 920 N.E.2d 949 (Ohio 2009), cert. denied, 131 S. Ct. 102 (2010).

Indeed, smartphones pose special problems for Fourth Amendment analysis.¹⁷ The unique character "both [of] the quantity and quality of the information stored on a smartphone, coupled with its constant presence at its user's side" cautions against channeling smartphones through current standards.¹⁸ "[M]odern cell phones are capable of storing at least...four million pages of Microsoft Word documents "¹⁹ With "the ability to access distant computers remotely[,]...a smartphone's capacity might be...of near infinite proportions."20 Furthermore, smartphones accommodate a wide range of uses, spanning far beyond telephone calls.²¹ Internet, maintain e-mail Users may browse the correspondences, take photographs, engage in personal banking, and connect to social media,22 as well as access thousands of other features through downloadable applications.²³ Moreover, the hardware of the devices themselves have quickly progressed: a new Nokia model boasts a "whopping 41-megapixel [camera] sensor,"24 and Apple's "iPhone 5S" features a "fingerprint

¹⁹ 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. 41, 46 (2012).

²⁰ Zamani, *supra* note 18, at 172.

²¹ Jenna Wortham, *Cellphones Now Used More for Data Than for Calls*, N.Y. TIMES (May 13, 2010), http:// www.nytimes.com/2010/05/14/technology/personaltech/ 14talk.html; *see also Riley*, 134 S. Ct. at 2489 ("The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone.").

 $^{22}~$ See Gershowitz, supra note 7, at 41-43; see also Riley, 134 S. Ct. at 2489 (noting the advanced capabilities of "[e]ven the most basic phones").

²³ Harry McCracken, Who's Winning, iOS or Android? All the Numbers, All in One Place, TIME (Apr. 16, 2013), http://techland.time.com/2013/04/16/ios-vs-android/ (noting that "[b]oth Apple and Google currently claim more than 800,000 third-party programs for their respective platform"); see also Riley, 134 S. Ct. at 2490 ("Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life.... There are over a million apps available in each of the two major app stores").

²⁴ Jefferson Graham, Smartcam Shootout: iPhone 5s, Lumia 1020, Galaxy S4, USA TODAY (Sept. 26, 2013, 5:59 AM), http://www.usatoday.com/story/tech/ columnist/talkingtech/2013/09/25/smartphone-camera-comparison-iphone-5s-lumia-1020-galaxy-s4/2868951/.

¹⁷ See, e.g., Riley, 134 S. Ct. at 2488-89; Bryan Andrew Stillwagon, Note, Bringing an End to Warrantless Cell Phone Searches, 42 GA. L. REV. 1165, 1168-69, 1206 (2008); H. Morley Swingle, Smartphone Searches Incident to Arrest, J. MISSOURI BAR, Jan.-Feb. 2012 at 36, 36-37; J. Patrick Warfield, Note, Putting a Square Peg in a Round Hole: The Search-Incident-to-Arrest Exception and Cellular Phones, 34 AM. J. TRIAL ADVOC. 165, 165-67 (2010).

¹⁸ Daniel Zamani, Note, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169, 171 (2010); *see also Riley*, 134 S. Ct. at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

scanner, which uses touch sensors and laser-cut sapphire crystal to take a high-resolution image of a fingerprint and store it inside the phone."²⁵ The more recent "iPhone 6" has improved on this technology.²⁶ Indeed, developers have not yet fully realized the smartphone's "full potential."²⁷

Cell phones and smartphones, however, are the beginning of the analysis, not the end.²⁸ New technology is constantly emerging.²⁹ Consider Moore's Law, the microchip industry's name for "the ability to pack twice as many transistors on the same sliver of silicon every two years"³⁰ thereby allowing for such technological developments as the smartphone.³¹ In the past 30 years, this "rare exponential growth factor" has brought about "a 3,500-fold increase" in processing speeds. ³² However, one industry expert recently

²⁷ Zamani, *supra* note 18, at 198.

²⁸ See Joshua A. Engel, Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices, 41 U. MEM. L. REV. 233, 296 (2010) ("The development of smart phones is not the first and will not be the last time that the courts will be asked to determine precisely what protection the Fourth Amendment affords people."); Mary Graw Leary, Reasonable Expectations of Privacy for Youth in a Digital Age, 80 MISS. L.J. 1035 1071-72 (2011) (noting that "[e]lectronic communication technology in mobile media devices such as the smartphone, iPhone, PDA, and laptop computer raise particular concerns about the traditional [Fourth Amendment] test"); see also United States v. Lustig, 3 F. Supp. 3d 808, 816 (S.D. Calif. 2014) ("Citizens carry in their hands, pockets, handbags, and backpacks: laptop computers, iPhones, iPads, iPods, Kindles, Nooks, Surfaces, tablets, phablets, Blackberries, flip phones, smart phones, contract phones, no-contract phones, and digital cameras. Some even wear Google Glass. These devices often (or perhaps usually) contain private and sensitive information, photographs, sound recordings, and GPS location history."); Brief of the American Civil Liberties Union et al. as Amici Curiae in Support of Petitioner, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132), 2014 WL 950807, at *6 n.2 [hereinafter ACLU Brief] (grouping "[s]martphones" with "other portable electronic devices," and using "[c]ell phone . . . as shorthand to refer to the entire range of portable electronic devices capable of storing personal information, which . . . should be treated alike").

²⁹ See infra Part III.

³⁰ Rick Merritt, *Moore's Law Dead by 2022, Expert Says*, EE TIMES (Aug. 27, 2013, 4:50 PM), http://www.eetimes.com/document.asp?doc_id=1319330.

³¹ Dean Takahashi, What Chip Designers Will Do When Moore's Law Ends, VENTURE BEAT (Aug. 27, 2013, 8:00 AM), http://venturebeat.com/2013/08/27/what-chipdesigners-will-do-when-moores-law-ends/. Moore's law has also allowed, for example, the development of hand-held calculators in 1967, before which only desktop units were available. Jacob Clifton, *How Calculators Work*, HOW STUFF WORKS, http://electronics.howstuffworks.com/gadgets/other-gadgets/calculator.htm (last visited Feb. 15, 2015).

³² Merritt, *supra* note 30.

²⁵ Gerry Smith, *iPhone Fingerprint Scanner Comes with a Catch*, HUFFINGTON POST (Sept. 11, 2013, 5:29 AM), http://www.huffingtonpost.com/2013/ 09/10/iphone-fingerprint-scanner_n_3900529.html.

²⁶ Antone Gonsalves, *iPhone 6 Fingerprint Scanner Found Accurate Enough for Apple Pay*, CSO (Sept. 23, 2014, 3:17 PM), http://www.csoonline.com/article/2687372/data-protection/iphone-6-fingerprint-scanner-found-accurate-enough-for-apple-pay.html.

declared that "2020 [is] the earliest date we could call [Moore's Law] dead."³³ Indeed, Gordon Moore, the law's namesake,³⁴ "himself reiterated that his law will *not* last forever."³⁵ Still, Intel has optimistically asserted the principle to be "alive and well."³⁶ Yet even with the questioned future vitality of Moore's Law, technology will continue to advance.³⁷

Confronted with perpetual and rapid advances in mobile digital devices, courts will continue to "constantly struggl[e] with applying previous case law to new technology."³⁸ Thus, analysis of the scope of Fourth Amendment protection as applied to new technology should be forward-looking.³⁹ By the time a particular case reaches upper appellate review, a device may be considerably outmoded, diminishing the policy value of the court's opinion.⁴⁰ Therefore, courts should adopt clear

³⁵ Bryan Gardiner, *IDF: Gordon Moore Predicts End of Moore's Law (Again)*, WIRED (Sept. 18, 2007, 4:07 PM), http://www.wired.com/business/2007/09/idf-gordon-mo-1/ (emphasis in original).

³⁶ Rik Myslewski, Intel Reveals 14nm PC, Declares Moore's Law 'Alive and Well', THE REGISTER (Sept. 10, 2013), http://www.theregister.co.uk/2013/09/10/ intel_reveals_14nm_pc_declares_moores_law_alive_and_well/.

³⁷ See Takahashi, *supra* note 31 (stating that "[e]ngineers can work tasks such as 3D stacking, improved packaging, better cooling, longer battery life, better input-output system, improved memory, and better chip architecture," in addition to software improvements).

³⁸ Warfield, supra note 17, at 191-92; Orin Kerr, Governor Brown Vetoes Bill on Searching Cell Phones Incident to Arrest, VOLOKH CONSPIRACY (Oct. 10, 2011, 2:29 am), http:// volokh.com/2011/10/10/governor-brown-vetoes-bill-on-searching-cell-phones-incidentto-arrest/ ("Changing technology is a moving target, and courts move slowly....").

³⁹ *Cf.* Kyllo v. United States, 533 U.S. 27, 36 (2001) (noting that when applying Fourth Amendment to thermal imaging of the home, "the rule [the Court] adopt[s] must take account of more sophisticated systems that are already in use *or in development*") (emphasis added); *see also* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (arguing that, with regards to the Fourth Amendment implications of wiretapping, "our contemplation cannot be only of what has been *but of what may be.* The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping" (emphasis added) (internal quotations omitted)).

⁴⁰ See Orin Kerr's commentary on the devices at issue in *Riley*. Orin Kerr, *Two Petitions on Searching Cell Phones Reach the Supreme Court*, VOLOKH CONSPIRACY (Aug. 19, 2013, 1:09 AM), http://www.volokh.com/2013/08/19/doj-files-certpetition-in-wurie/ (noting that "two cert petitions], Petition for a Writ of Certiorari, *Riley v. California*, 2013 WL 3934033 (U.S.) (No. 13-132), and Petition for a Writ of Certiorari, *United States v. Wurie*, 2013 WL 4404658 (U.S.) (No. 13-212),] have been filed seeking review of how the Fourth Amendment applies to searching a cell phone incident to arrest[,]" and further noting that, given the differences in technology between the two cases, "[r]eviewing [the] case with an earlier model phone[, i.e. *Wurie*,]

³³ Id. At least one prominent physicist recently made a similar claim. See Shawn Knight, *Physicist Predicts Moore's Law Will Collapse in About 10 Years*, TECHSPOT (May 1, 2012, 4:00 PM), http://www.techspot.com/news/48409-physicistpredicts-moores-law-will-collapse-in-about-10-years.html.

³⁴ The "law" is named after Gordon Moore: "Gordon Moore, chairman emeritus of Intel, predicted in 1965 that the number of transistors—basic on-off switches that are the fundamental building blocks of modern electronics—on a chip would double every two years or so." Takahashi, *supra* note 31.

BROOKLYN LAW REVIEW

guidelines establishing when, if ever, a police officer may search any personal digital electronic device without a warrant.⁴¹ The Supreme Court in *Riley* intimates a logical answer by requiring police to obtain a warrant to search a cell phone.⁴² But *Riley*'s holding is limited to cell phones.⁴³ Courts should anticipate the questions that future developments in technology will create regarding *Riley*'s reach by creating a clear rule extending *Riley* to exclude personal electronic devices altogether from the search-incident-to-arrest warrant exception.⁴⁴ This broad reading would take into account the ubiquity of technological use as well as the increased intimacy

⁴³ See Riley, 134 S. Ct. at 2493.

⁴⁴ For an argument that smartphones should be excluded from the searchincident-to-arrest warrant exception, see Stillwagon, supra note 17, at 1206 ("When the intrusion cannot reasonably be justified by purposes such as officer protection, evidence preservation, or arrestee containment, a simple seizure of the device must suffice until a warrant can be procured."). For arguments that warrants should also be required for other digital devices, off of which this note builds, see ACLU Brief, supra note 28, at *6 & n.2; Brief of Center for Democracy & Technology and Electronic Frontier Foundation as Amici Curiae in Support of Petitioner in No. 13-132 and Respondent in No. 13-212, Riley v. California, 134 S. Ct. 2473 (2014) (No's 13-132 & 13-212), 2014 WL 950808, at *13 [hereinafter Center for Democracy & Electronic Frontier Foundation Brief]; Brief of Amici Curiae Criminal Law Professors in Support of Petitioner Riley and Respondent Wurie, Riley v. California, 134 S. Ct. 2473 (2014) (No's 13-132 & 13-212), 2014 WL 931832, at *1 [hereinafter Criminal Law Professors Brief]. For an argument suggesting that searches incident to arrest be generally limited to situations where the item searched reasonably might contain "evidence related to the crime of arrest" and where "the arrestee remains capable of accessing the item" see Derek A. Scheurer, Are Courts Phoning it in? Resolving Problematic Reasoning in the Debate Over Warrantless Searches of Cell Phones Incident to Arrest, 9 WASH. J.L. TECH. & ARTS 287, 325, 327 (2014) ("[T]his rule by design is not limited to 'cell phones,' which are a technology in flux and already can be seen functionally overlapping with other portable computers, such as laptops and tablets."); see also Donald A. Dripps, "Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure, 103 J. CRIM. L. & CRIMINOLOGY 49, 109 (2013) ("The anti-rummaging principle, then, suggests curtailing the warrantless seizure and search of digital devices incident to arrest.")

would lead to a decision with facts that are atypical now and are getting more outdated every passing month").

⁴¹ See Engel, *supra* note 28, at 296-97.

⁴² Riley v. California, 134 S. Ct. 2473, 2493 (2014); ACLU Brief, *supra* note 28, at *6 n.2 (noting the impact that the Court's decision will have on the permissible scope of other electronic devices incident to arrest); Brief Amici Curiae of National Press Photographers Association and Thirteen Media Organizations in Support of Petitioner Riley and Respondent Wurie, Riley v. California, 134 S. Ct. 2473 (2014) (No's 13-132 & 13-212), 2014 WL 975499, at *18 [hereinafter National Press Photographers Brief] ("We are also at the dawn of the age of 'wearable' devices—*e.g.*, glasses and watches and other 'clothing'—that will contain even more sensitive information. Whatever rule this Court fashions here will determine the level of protection accorded to these evolving technologies.").

that consumers share with their mobile devices,⁴⁵ ultimately respectful of the sanctity of the individual's "virtual home."⁴⁶

Part I of this note provides a brief overview of Fourth Amendment jurisprudence that is necessary to understand how the Amendment's protections should apply to mobile devices. Part II discusses how state and lower federal courts have applied the Fourth Amendment to cell phones—an issue decided in *Riley*,⁴⁷ but a useful starting point nonetheless for examining more advanced personal electronic devices. Part III examines how more advanced personal electronic devices should fit into the Fourth Amendment framework, and how they should be characterized in light of traditional Fourth Amendment concerns. Starting from the context of existing mobile devices, this note will explain why the privacy interests in these devices not only suggests that a clear, bright-line rule is needed in light of constantly changing technology,⁴⁸ but that courts should create this rule by explicitly extending *Riley* to all mobile digital devices.49

⁴⁶ See ACLU Brief, supra note 28, at *2-3, *9 ("Cell phones and other portable electronic devices are, in effect, our new homes ... our virtual homes ... Our electronic worlds, in a very real sense, *are* our new homes and our Fourth Amendment traditions demand that they be respected as such."); Brief of the National Association of Criminal Defense Lawyers and the Brennan Center for Justice at New York University School of Law as Amici Curiae in Support of Petitioner, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132), 2014 WL 975495, at *8 [hereinafter Criminal Defense Lawyers and Brennan Center Brief] ("[O]ur mobile devices are the doorways to our virtual homes.") *Cf. In re* United States, 665 F. Supp. 2d. 1210, 1213 (D. Or. 2009) (noting that, regarding "[i]nternet communications," "the Fourth Amendment's privacy protections for the home may not apply to our 'virtual homes' online").

⁴⁷ See Riley, 134 S. Ct. at 2493.

⁴⁸ See Engel, supra note 28, at 296-97; Kerr, supra note 38 ("Changing technology is a moving target, and courts move slowly..."); Gerard T. Leone, Linn Foster Freedman & Kathryn M. Silvia, Any Calls Texts, or Photos May Be Used Against You: Warrantless Cell Phone Searches and Personal Privacy, BOSTON BAR J., Spring 2014, 27, 30 ("Tomorrow, technology will turn another corner..."); Drew Liming, Calling for a Standard: Why Courts Should Apply a New Balancing Test in Cell Phone Searches Incident to Arrest, Note, 51 AM. CRIM. L. REV. 715, 728 (2014) ("[C]ell phone technology has developed rapidly.").

⁴⁹ Several amici in *Riley* argued that warrants should also be required for other digital devices, and this note builds on these claims, arguing the importance of extending *Riley. See* ACLU Brief, *supra* note 28, at *6 n.2; Center for Democracy & Electronic Frontier Foundation Brief, *supra* note 44, at *13; Criminal Law Professors Brief, *supra* note 44, at *1; *see also* Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of* Riley v. California, 2014 CATO SUP. CT. REV. 307, 328-29 (2014) ("*Riley* addressed digitally stored information on a cell phone, but it is difficult to see how

⁴⁵ See Riley, 134 S. Ct. at 2490; see also John Boudreau, Your Phone, Your Life: New Apps Change How You Use Mobile Devices, SAN JOSE MERCURY NEWS (Mar. 15, 2009), http://www.mercurynews.com/ci_11900793?IADID=Search-www.mercurynews.comwww.mercurynews.com (quoting B.J. Fogg, a Stanford University researcher) ("Because their smart-phone is with them everywhere they go, people develop far closer attachments to the devices than to their home PCs or laptops 'Nothing is as close to us all the time—not even your spouse or partner."").

I. FOURTH AMENDMENT FRAMEWORK

The Supreme Court "has inferred that a warrant must generally be secured" before a search by law enforcement may be executed.⁵⁰ This is because "bypassing a neutral predetermination" of the scope of a search [impermissibly] leaves individuals secure from Fourth Amendment violations 'only in the discretion of the police."⁵¹ However, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."⁵² Hence observation of evidence that is in "plain view" of a "police officer [where she] ha[s] a prior justification for an intrusion"53—that is, "situations '[w]here the initial intrusion that brings the police within plain view of such [evidence] is supported... by one of the recognized exceptions to the warrant requirement"⁵⁴—does not "involve any invasion of privacy,"⁵⁵ and thus does not invoke the Fourth Amendment,⁵⁶ even if that observation was not inadvertent.⁵⁷ Moreover, even if there "is . . . a 'search' within the intendment of the Fourth Amendment,"58 the Supreme Court has recognized several exceptions to the search warrant requirement,⁵⁹ particularly the "search incident to arrest,"60 and "exigent circumstances"61 exceptions.62

- ⁵¹ Katz v. United States, 389 U.S. 347, 358-59 (1967) (citation omitted).
- ⁵² Id. at 358-59 (citing Lewis v. United States, 385 U.S. 206, 210 (1966)).

 $^{54}\,$ Arizona v. Hicks, 480 U.S. 321, 326 (1987) (alterations in original) (quoting Coolidge, 403 U.S. at 465).

⁵⁶ See Illinois v. Andreas, 463 U.S. 765, 771-72 (1983).

 $^{57}\,$ Horton, 496 U.S. at 133-34 (citing Hicks, 480 U.S. at 325; Andreas, 463 U.S. at 771).

⁵⁸ Andreas, 463 U.S. at 771-72.

- ⁶⁰ Chimel v. California, 395 U.S. 752, 762 (1969).
- ⁶¹ Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).
- 62 See Riley v. California, 134 S. Ct. 2473, 2486-87, 2493-94 (2014).

a different result could possibly apply to searches incident to arrest of the contents of tablets, laptops, or thumb drives. All share the characteristics relied on by the *Riley* Court, and a warrant therefore should be required to conduct such searches."). Before *Riley*, this argument has been made regarding smartphones. *See, e.g.,* Adam M. Gershowitz, *Seizing a Cell Phone Incident to Arrest: Data Extraction Devices, Faraday Bags, or Aluminum Foil as a Solution to the Warrantless Cell Phone Search Problem, 22* WM. & MARY BILL RTS. J. 601, 602 (2013); Stillwagon, *supra* note 17, at 1206-07.

⁵⁰ Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

⁵³ Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971); *see also* Horton v. California, 496 U.S. 128, 136 (1990) ("It is, of course, an essential predicate to any valid warrantless seizure of incriminating evidence that the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed.").

⁵⁵ *Horton*, 496 U.S. at 133.

 $^{^{59}~}See$ California v. Acevado, 500 U.S. 565, 582 (1991) (Scalia, J., concurring) (noting that "[i]n 1985, one commentator cataloged nearly 20 such exceptions, Since then, we have added at least two more").

A. Search Incident to Arrest

The Supreme Court has long recognized the right of police officers to conduct a search of an arrestee without a warrant as a "search incident to a lawful arrest."⁶³ In 1969, the Court defined the scope of these searches in *Chimel v. California.*⁶⁴ In that case, "officers...looked through the [accused's] entire three-bedroom house" while executing an arrest warrant, notwithstanding that "[n]o search warrant had been issued."⁶⁵ The area that was searched "includ[ed] the attic, the garage, and a small workshop."⁶⁶ Although "[i]n some rooms the search was relatively cursory[,]" in others "the officers directed the petitioner's wife to open drawers" and shift their contents to reveal potential evidence.⁶⁷

The Court held that a search incident to arrest was only justified "of the arrestee's person and the area 'within his immediate control."⁶⁸ The Court defined this area as "the area from within which [the arrestee] might gain possession of a weapon or destructible evidence."⁶⁹ However, the search that had been conducted extended "far beyond the petitioner's person and the area from within which he might have obtained either a weapon or something that could have been used as evidence against him."⁷⁰ Because the search extended beyond that area, the Court concluded that the search's scope was not reasonable and thus violated the Fourth Amendment.⁷¹

Such searches are justified because of the risk that the arrestee might obtain weapons that she "might seek to use in order to resist arrest or effect [her] escape."⁷² Moreover, "it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction."⁷³ This authority allows "police officers to open and search through all items on an arrestee's

- ⁷⁰ *Id.* at 768.
- 71 *Id*.
- ⁷² *Id.* at 763.
- ⁷³ Id.

⁶³ Chimel, 395 U.S. at 755 (citing Weeks v. United States, 232 U.S. 383, 392 (1914)).

 $^{^{64}}$ Id. at 768.

⁶⁵ Id. at 753-54.

⁶⁶ Id.

⁶⁷ *Id.* at 754.

⁶⁸ *Id.* at 763.

 $^{^{69}}$ *Id*.

person, even if they are in a closed container, and even without suspicion that the contents of the container are illegal."⁷⁴

This principle is "stated clearly enough, but in the early going after *Chimel* it proved difficult to apply, particularly in is critical considering that there were approximately 250 million registered vehicles in the United States as of 2009,76 providing ample opportunities for police encounters. The Supreme Court offered further guidance in this area in Arizona v. Gant,⁷⁷ a case in which the arrestee's car was searched after he "was arrested for driving with a suspended license, handcuffed, and locked in the back of a patrol car."78 An earlier case, New York v. Belton,⁷⁹ appeared to many lower courts "to have set down a simple, bright-line rule" allowing a police officer to conduct a search of a vehicle when she arrests an occupant, "regardless of whether the arrestee in any particular case was within reaching distance of the vehicle at the time of the search."80 However, in Gant, the Court "h[e]ld that Belton does not authorize a vehicle search incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle," except "when it is reasonable to believe that evidence of the offense of arrest might be found in the vehicle."81 The Court further concluded that "[t]he safety and evidentiary justifications underlying Chimel's reaching-distance rule determine Belton's scope."82 This reliance on the underlying purpose for the holding in *Chimel* is crucial when considering how the search-incident-to-

⁷⁷ 556 U.S. 332 (2009).

⁷⁸ Id. at 335.

⁸¹ Gant, 556 U.S. at 335.

⁸² Id.

⁷⁴ Adam Gershowitz, Password Protected? Can a Password Save Your Cell Phone from a Search Incident to Arrest?, 96 IOWA L. REV. 1125, 1132-33 (2011) (citing United States v. Robinson, 414 U.S. 218, 235-36 (1973)).

⁷⁵ Davis v. United States, 131 S. Ct. 2419, 2424 (2011) (internal citations and quotation marks omitted) (quoting New York v. Belton, 453 U.S. 454, 458-59 (1981)).

⁷⁶ See U.S. CENSUS BUREAU, THE STATISTICAL ABSTRACT OF THE UNITED STATES: 2012, at 688 (2012), available at http://www.census.gov/compendia/statab/2012/tables/12s1096.pdf (noting the presence of approximately 246,283,000 registered automobiles in the United States in 2009, roughly a 30% increase from 1990).

 $^{^{79}\,}$ 453 U.S. at 460 ("hold[ing] 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." (footnotes omitted)).

⁸⁰ Davis, 131 S. Ct. at 2424 (citing Thornton v. United States, 541 U.S. 615, 628 (2004) (Scalia, J., concurring)).

arrest exception interplays with consumer technology.⁸³ In *Riley*, the Court explained how the concerns sounded in *Chimel* do not reverberate in the digital domain of a person's cell phone.⁸⁴

B. Exigent Circumstances

The Supreme Court has recognized another exception to the Fourth Amendment's search warrant requirement in situations where "the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable...."⁸⁵ In other words, the Supreme Court "looks to the totality of the circumstances" and decides if a police "officer faced an emergency that justified acting without a warrant...."⁸⁶ Under this principle, the "Court has identified several exigencies that may justify a warrantless search of a home"⁸⁷:

Under the "emergency aid" exception, for example, "officers may enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury." Police officers may enter premises without a warrant when they are in hot pursuit of a fleeing suspect. And—what is relevant here—the need "to prevent the imminent destruction of evidence" has long been recognized as a sufficient justification for a warrantless search.⁸⁸

Indeed, the exception has wide ranging applications. In *Kentucky v. King*, the Supreme Court approved of police entering a home without a warrant where they "smelled marijuana smoke emanating from the apartment," knocked and announced their presence, and then determined that "drug-related evidence was about to be destroyed" because "it sounded as [though] things were being moved inside the apartment."⁸⁹ "In such a situation," the Court concluded, "the exigent circumstances rule applies."⁹⁰ The Court has even gone

⁸³ See Smallwood v. State, 113 So. 3d 724, 735-36 (Fla. 2013). The court concluded that "*Gant* demonstrates that... once an arrestee is physically separated from an item or thing... the dual rationales for th[e] search[-incident-to-arrest] exception no longer apply[,]" and thus held that "once a cell phone has been removed from the person of the arrestee, a warrant must be secured pursuant to *Gant* before officers may conduct a search." *Id.*

⁸⁴ Riley v. California, 134 S. Ct. 2473, 2485-88 (2014).

 $^{^{85}\,}$ Mincey v. Arizona, 437 U.S. 385, 394 (1978) (quoting McDonald v. United States, 335 U.S. 451, 456 (1948)).

⁸⁶ Missouri v. McNeely, 133 S. Ct. 1552, 1559 (2013).

⁸⁷ Kentucky v. King, 131 S. Ct. 1849, 1856-57 (2011).

⁸⁸ Id. at 1856 (internal citations and quotation marks omitted).

⁸⁹ *Id.* at 1854 (alteration in original).

 $^{^{90}}$ Id.

so far as to find exigency in the dissipation of "the percentage of alcohol in the blood," justifying a warrantless "[e]xtraction of blood samples for testing."⁹¹ However, this is not a per se rule⁹² and requires "a finding of exigency in a specific case."⁹³ This is because to evaluate the reasonableness of a search is a "factspecific" inquiry that requires courts to assess a claimed exigency "on its own facts and circumstances."⁹⁴

The exigent circumstances warrant exception is important when considering warrantless searches of mobile devices as well, because as the Supreme Court has pointed out, even if the search-incident-to-arrest exception does not apply, this exception may.⁹⁵ In United States v. Wurie, a decision upheld by the Supreme Court in *Riley*, the Court of Appeals for the First Circuit "h[e]ld 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 *Chimel*'s underlying justifications do not apply.⁹⁶ However, the court also "assume[d] that the exigent circumstances exception" meant that such "immediate, warrantless search[es]" would be permissible if police "ha[d] probable cause to believe that the phone contains evidence of a crime, as well as a compelling need to act quickly that makes it impracticable for them to obtain a warrant...."97 The Supreme Court confirmed this assumption.⁹⁸ This recognized exception provides an additional consideration for analyzing the reasonableness of warrantless searches of mobile devices.

II. WARRANTLESS SEARCHES OF CELL PHONES

Although the Supreme Court has already decided that law enforcement officials may not search a cell phone incident to arrest,⁹⁹ examining the ways in which courts and scholars have analyzed cell phones and smartphones in the Fourth Amendment context nonetheless serves as a useful starting point. They offer good examples of how courts have struggled to

⁹¹ Schmerber v. California, 384 U.S. 757, 770-71 (1966).

⁹² See Missouri v. McNeely, 133 S. Ct. 1552, 1556 (2013).

⁹³ Id. at 1563.

 $^{^{94}\,}$ Id. at 1559 (quoting Go-Bart Importing Co. v. United States, 282 U.S. 344, 357 (1931)) (internal quotation marks omitted).

⁹⁵ Riley v. California, 134 S. Ct. 2473, 2494 (2014); see also United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013), aff'd sub nom. Riley, 134 S. Ct. at 2493.

⁹⁶ Wurie, 728 F.3d at 13.

⁹⁷ Id.

⁹⁸ *Riley*, 134 S. Ct. at 2494.

⁹⁹ Id. at 2493.

fit new technology into the existing Fourth Amendment framework,¹⁰⁰ and provide some insight as to how the Fourth Amendment should apply to more advanced digital devices.¹⁰¹ Before the Court's decision in *Riley*, lower federal courts were split over the application of warrant exceptions to cell phones,¹⁰² and state courts that had decided the issue were equally divided.¹⁰³ Additionally, commentators have suggested various approaches for dealing with smartphones,¹⁰⁴ including requiring a search warrant in all cases.¹⁰⁵ This commentary is useful, but the problems that arise as personal mobile technology continues to develop quickly go beyond simply cell phones and smartphones.¹⁰⁶

¹⁰³ See Wurie, 728 F.3d at 5-6.

¹⁰⁴ See, e.g., Patrick Brown, Note, Searches of Cell Phones Incident to Arrest: Overview of the Law as it Stands and a New Path Forward, 27 HARV. J.L. & TECH. 563, 579 (2014) (suggesting a "simple, three-part test for searches of cell phones incident to arrest. Such searches are constitutional when: (1) police have a lawful physical right of access to the phone, (2) the information searched is stored on the phone, and (3) no reasonable expectation of privacy attaches to the information searched because that information has been exposed to third parties."); MacLean, *supra* note 19, at 43 ("[N]either Chimel justification pertains to cell phone memory searches incident to lawful arrest; therefore, such searches are unconstitutional without a search warrant issued by a neutral magistrate, or when some other traditional exception to the warrant requirement applies."); Park, *supra* note 7, at 432 ("[C]ell phones should be permitted to be searched incident to a valid custodial arrest when likely to yield evidence related to the reason for arrest by a relevant limited intrusion into data in which there is a diminished expectation of privacy.").

¹⁰⁵ Gershowitz, *supra* note 49, at 602 ("[T]he lower courts (and eventually the Supreme Court) should only allow police to seize cell phones incident to arrest. Then, while waiting for a search warrant, police should preserve the cell phone data"); Stillwagon, *supra* note 17, at 1208 ("[I]t is the duty of courts to uphold the Fourth Amendment to the Constitution, to protect the privacy of citizens, and to bring an end to warrantless cell phone searches.").

¹⁰⁶ See Center for Democracy & Electronic Frontier Foundation Brief, supra note 44, at *12 ("New devices such as smart watches and Google Glass will increase the types and amounts of electronically-stored personal information that individuals carry with them each day."); National Press Photographers Brief, supra note 42, at *18 ("We are also at the dawn of the age of 'wearable' devices—e.g., glasses and watches and other 'clothing'—that will contain even more sensitive information."); Engel, supra note 28, at 296; Andrew Guthrie Ferguson, Personal Curtilage: Fourth Amendment Security in Public, 55 WM. & MARY L. REV. 1283, 1312 (2014) ("New technological devices have and will continue to be able to see, hear, smell, and touch citizens in ways that were simply impossible in prior eras.").

¹⁰⁰ See, e.g., Wurie, 728 F.3d at 1; United States v. Murphy, 552 F.3d 405 (4th Cir. 2009), cert. denied, 129 S. Ct. 2016 (2009); Smallwood v. State, 113 So. 3d 724 (Fla. 2013); State v. Smith, 920 N.E.2d 949 (Ohio 2009), cert. denied, 131 S. Ct. 102 (2010).

¹⁰¹ See Engel, supra note 28, at 296-97; Scheurer, supra note 44, at 327.

¹⁰² See Lyle Denniston, U.S. Appeals on Cellphone Privacy, SCOTUS BLOG (Aug. 16, 2013, 4:37 PM), http://www.scotusblog.com/2013/08/u-s-appeals-on-cellphone-privacy/ (noting that "[t]he issue . . . has divided lower courts").

A. Cases Finding the Warrantless Search of a Cell Phone Reasonable

Before *Riley*, courts utilized a variety of approaches to justify the search of a cell phone without a warrant, and indeed, a majority of courts addressing this issue to varying degrees "ha[d] ultimately upheld warrantless cell phone data searches."107 In People v. Diaz,108 the Supreme Court of California upheld the warrantless search of a defendant's cell phone as an item that "was 'immediately associated with [defendant's] person,"¹⁰⁹ and thus was per se reasonable under United States v. Robinson.¹¹⁰ Although the search at issue was of the arrestee's text messages,¹¹¹ the decision articulated a bright-line Fourth Amendment rule including all searches of an arrestee's cell phone incident to arrest.¹¹² The court was not persuaded by the defendant's argument that "cell phones contain quantities of personal data . . . and therefore implicate heightened privacy concerns that warrant treating them like the footlocker in [United States v.] Chadwick."113 While the dissent found this argument persuasive,¹¹⁴ the majority rejected the conclusion that "whether a warrant is necessary for a search of an item properly seized from an arrestee's person incident to a lawful custodial arrest depends in any way on the character of the seized item."¹¹⁵ In a later decision reversed by the Supreme Court in Riley, the Fourth District Court of Appeal relied upon *Diaz* because the trial court found "the cell phone... was on [the defendant's] person at the time of the arrest," and thus the court held that his "cell phone was immediately associated with his person when he was arrested,

¹¹¹ *Diaz*, 244 P.3d at 502-03.

 112 Id. at 505-06 ("Because the cell phone was immediately associated with the defendant's person, [the officer who conducted the search] was 'entitled to inspect' its contents without a warrant at the sheriff's station 90 minutes after defendant's arrest, whether or not an exigency existed." (quoting *Robinson*, 414 U.S. at 236, internal citation omitted)).

¹¹³ *Id.* at 506 (alterations and internal quotation marks omitted).

¹¹⁵ Id. at 506-07.

¹⁰⁷ See Wurie, 728 F.3d at 5.

¹⁰⁸ 244 P.3d 501 (Cal. 2011).

 $^{^{109}\,}$ Id. at 505 (alteration in original) (quoting United States v. Chadwick, 433 U.S. 1, 15 (1977)).

 $^{^{110}~}Id.$ at 506 (citing United States v. Robinson, 414 U.S. 218, 236 (1973)). Robinson held "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." Robinson, 414 U.S. at 235.

 $^{^{114}~}$ Id. at 513 (Werdegar, J., dissenting) ("The potential intrusion on informational privacy involved in a police search of a person's mobile phone, smartphone or handheld computer is unique among searches of an arrestee's person and effects.").

and therefore the search of the cell phone was lawful whether or not an exigency still existed."¹¹⁶

Other pre-*Riley* courts, "to varying degrees, relied on the need to preserve evidence on a cell phone."¹¹⁷ In United States v. Flores-Lopez,¹¹⁸ the Court of Appeals for the Seventh Circuit relied on the evidentiary justifications of Chimel v. California to uphold a warrantless search of a defendant's cell phone to learn its telephone number.¹¹⁹ The court "said it was conceivable . . . that a confederate of the defendant would have wiped the data from the defendant's cell phone before the government could obtain a search warrant."120 Although it found the intrusion into the defendant's phone to be "slight,"121 the court did "not consider what level of risk to personal safety or to the preservation of evidence would be necessary to justify a more extensive search of a cell phone without a warrant," but nonetheless decided it "can certainly imagine justifications for a more extensive search."¹²² The court further posited that "[a] modern cell phone is in one aspect a diary writ large,"123 and moreover, that "[i]t's not even clear that we need a rule of law specific to cell phones If police are entitled to open a pocket diary . . . , they should be entitled to turn on a cell phone to learn its number."124

Similarly, in *Commonwealth v. Phifer*,¹²⁵ the Supreme Judicial Court of Massachusetts relied on the evidence-gathering rationale of *Chimel* to justify a warrantless cell phone search¹²⁶: "The evidence at issue here consists of the contents of the recent call list on the defendant's cellular telephone [T]he officers here had probable cause to believe the telephone's recent call list would contain evidence relating to the crime for which he was arrested"¹²⁷ However, the court narrowed its holding "that the limited search of the defendant's cellular telephone to

 121 Id.

- 124 Id. at 807.
- $^{\rm 125}~~979$ N.E.2d 210 (Mass. 2012).

 $^{^{116}\,}$ People v. Riley, D059840, 2013 WL 475242, at *6 (Cal. Ct. App. Feb. 8, 2013) (citations and internal quotation marks omitted), rev'd sub nom. Riley v. California, 134 S. Ct. 2473 (2014).

 ¹¹⁷ United States v. Wurie, 728 F.3d 1, 5 (1st Cir. 2013), (citing United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007)), aff'd sub nom. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

¹¹⁸ 670 F.3d 803 (7th Cir. 2012).

¹¹⁹ Id. at 806, 810.

 $^{^{120}}$ Id. at 809.

 $^{^{122}}$ Id. at 810.

 $^{^{123}}$ Id. at 805.

 $^{^{126}}$ Id. at 213, 216.

 $^{^{127}}$ Id. at 215.

examine the recent call list was a permissible search incident to the defendant's lawful arrest,"¹²⁸ by continuing to assert that "[w]e do not suggest that the assessment necessarily would be the same on different facts, or in relation to a different type of intrusion into a more complex cellular telephone."¹²⁹ The court suggested that "the privacy of the myriad types of information stored in a cellular telephone" might alter the calculus when considering whether a person's "reasonable expectation of privacy is diminished... when subject to a lawful arrest and taken into custody."¹³⁰

B. Cases Finding the Search of a Cell Phone Required a Warrant

Just as the Massachusetts high court was tepid in its holding that permitted a warrantless cell phone search,¹³¹ other courts before the *Riley* decision were careful in invalidating such searches. For example, the U.S. District Court for the Middle District of Florida found that an officer's search of a defendant's cell phone was not a lawful search incident to arrest where the defendant was arrested for driving with a suspended license.¹³² In that case, "[w]hile the defendant was in custody," the officers called the "last caller," and searched the defendant's phone "including a digital photo album," which revealed "photos of an intimate nature involving a woman as well as a photo of marijuana plants in . . . a marijuana 'grow house."¹³³ The search, however, was to "rummag[e] for information related to the odor of marijuana emanating from the vehicle," that is, unrelated to the offense for which the defendant was arrested.¹³⁴ Nonetheless, the court was careful to express the view that "[w]here a defendant is arrested for drugrelated activity, police may be justified in searching the contents of a cell phone for evidence related to the crime of arrest, even if the presence of such evidence is improbable."135

Other courts have been bolder with their disapproval of warrantless searches of cell phones. In *United States v. Wurie*—the decision ultimately upheld by the Supreme Court

¹²⁸ *Id.* at 216.

 $^{^{129}}$ Id.

¹³⁰ *Id.*

¹³¹ *Id.*

¹³² United States v. Quintana, 594 F. Supp. 2d 1291, 1300-01 (M.D. Fla. 2009).

¹³³ Id. at 1295-96.

¹³⁴ *Id.* at 1300.

¹³⁵ Id.

in *Riley*—the Court of Appeals for the First Circuit found "it necessary to craft a bright-line rule that applies to all warrantless cell phone searches,"¹³⁶ and "h[e]ld that the searchincident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person."¹³⁷ The court recognized that "a modern cell phone is a computer, and a computer is not just another purse or address book," because it possesses "immense" storage capacity, and stores "information [that] is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records."¹³⁸ The court went so far as to note that:

iPhones can now connect their owners directly to a home computer's webcam, ... so that users can monitor the inside of their homes remotely. [Thus,] [a]t the touch of a button a cell phone search becomes a house search, and that is not a search of a "container" in any normal sense of that word, though a house contains data.¹³⁹

Still, the court noted its assumption "that the exigent circumstances exception would allow the police to conduct an immediate, warrantless search of a cell phone's data where they have probable cause to believe that the phone contains evidence of a crime, as well as a compelling need to act quickly that makes it impracticable for them to obtain a warrant."¹⁴⁰

The Supreme Court of Ohio used similar language in *State v. Smith* holding that "an officer may not conduct a search of a cell phone's contents incident to a lawful arrest without first obtaining a warrant."¹⁴¹ In sweeping language, the court stated:

Although cell phones cannot be equated with laptop computers, their ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain. Once the cell phone is in police custody, the state has satisfied its immediate interest in collecting and preserving evidence.... But because a person has a high expectation of privacy in a cell phone's contents, police must then obtain a warrant before intruding into the phone's contents.¹⁴²

 142 Id.

 $^{^{136}~}$ United States v. Wurie, 728 F.3d 1, 6 (1st Cir. 2013), $af\!f\,'d\,sub\,nom.$ Riley v California, 134 S. Ct. 2473 (2014).

 $^{^{137}}$ Id. at 13.

¹³⁸ *Id.* at 8 (internal quotation marks omitted).

¹³⁹ Id. at 8-9 (citations and internal quotation marks omitted).

¹⁴⁰ *Id.* at 13.

¹⁴¹ State v. Smith, 920 N.E.2d 949, 951-52, 955 (Ohio 2009).

The court further concluded that cell phones are not "closed container[s] for purposes of a Fourth Amendment analysis," and thus the underlying justifications of the search-incident-toarrest exception—"officer safety and the preservation of evidence"—are inapplicable to them.¹⁴³ Despite this bright-line pronouncement, it is worth noting that the court commented on the lack of "evidence that either justification was present in [the] case."¹⁴⁴ And additionally, the court suggested that "there may be some instances in which a warrantless search of a cell phone is necessary to identify a suspect," although the court did not address that issue.¹⁴⁵

A different approach was taken in *United States v. Park* to invalidate a warrantless cell phone search.¹⁴⁶ In that case, the defendants were arrested after the search of the premises from which they were seen leaving, and for which police had a search warrant, yielded "evidence of an indoor marijuana cultivation operation."¹⁴⁷ The defendants' phones were searched sometime during the booking process.¹⁴⁸ The court first found that the search "was not contemporaneous with [the] arrest."149 It then noted that "[t]he searches at issue [in this case went] far beyond the original rationales for searches incident to arrest, which were to remove weapons ... and the need to prevent concealment or destruction of evidence[;]...[i]nstead, the purpose was purely investigatory."¹⁵⁰ Finally, "due to the quantity and quality of information that can be stored on a phone, [it] should...be characterized...as cellular а 'possession[] within an arrestee's immediate control [that has] [F]ourth [A]mendment protection at the station house."¹⁵¹ Thus, the district court held "that once officers seized defendants' cellular phones at the station house, they were required to obtain a warrant to conduct the searches."152

These cases demonstrate how courts have struggled to fit mobile technology into the existing Fourth Amendment

¹⁴³ *Id.* at 954-55.

 $^{^{144}}$ Id. at 955.

 $^{^{145}}$ Id. at 956.

 $^{^{146}\,}$ United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *1 (N.D. Cal. May 23, 2007).

¹⁴⁷ *Id.* at *1-2.

¹⁴⁸ *Id.* at *3.

¹⁴⁹ *Id.* at *8.

 $^{^{150}}$ *Id*.

 $^{^{151}~}$ Id. at *9 (second and third alterations in original) (quoting United States v. Monclavo-Cruz, 662 F.2d 1285, 1291 (9th Cir. 1981)).

¹⁵² *Id.* at *1.

rubric.¹⁵³ Shifting focus from cell phones to smartphones "drastically changes" the analysis.¹⁵⁴ Where more steps are required to access the data, "it becomes harder to analogize [digital devices] to a closed container or a wallet containing an address list."¹⁵⁵ And moreover, it is becoming increasingly difficult to distinguish between different types of devices.¹⁵⁶ Indeed, "the line between cell phones and personal computers has grown increasingly blurry."¹⁵⁷

The lack of uniformity before *Riley* created special problems for those wishing to sue to vindicate their rights, because the doctrine of qualified immunity shields officers from civil suit "insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known."¹⁵⁸ Similarly, the "good faith exception to the exclusionary rule" means that evidence is not excluded unless "a reasonably well trained officer would have known that the search was illegal in light of all the circumstances."¹⁵⁹ This underscores the need for clarity in Fourth Amendment jurisprudence.¹⁶⁰ Furthermore, the problems arising from the need to analogize cell phones are exacerbated when considering the capabilities of technology more advanced than smartphones.¹⁶¹

¹⁵⁶ United States v. Wurie, 728 F.3d 1, 7-8 (1st Cir. 2013), *aff'd sub nom*. Riley v. California, 134 S. Ct. 2473, 2493 (2014) (failing to see a principled distinction between the cell phone at issue and "a laptop computer or tablet device such as an iPad").

¹⁵⁷ Park, 2007 WL 1521573, at *8 (suggesting that to allow the warrantless search of the cell phone would likewise permit the police to "lawfully seize and search an arrestee's laptop computer as a warrantless search incident to arrest"); *see also Riley*, 134 S. Ct. at 2489 ("The term 'cell phone' is itself a misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."); ACLU Brief, *supra* note 28, at *6 n.2.

¹⁵⁸ Newhard v. Borders, 649 F. Supp. 2d 440, 444-45, 447, 450 (W.D. Va. 2009) (quoting Pearson v. Callahan, 555 U.S. 223, 231 (2009); Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982)) (internal quotation marks omitted) (finding that officers sued for violations of an arrestee's Fourth Amendment rights pursuant to 42 U.S.C. § 1983 for the warrantless search of the arrestee's cell phone were entitled to qualified immunity).

¹⁵⁹ United States v. Lustig, 3 F. Supp. 3d 808, 819 (S.D. Calif. 2014) (quoting Herring v. United States, 555 U.S. 135, 145 (2009); United States v. Leon, 468 U.S. 897, 922 & n.23 (1984)) (internal quotation marks omitted) (finding that the good faith exception applied to a search incident to arrest of the defendant's cell phones).

¹⁶⁰ Warfield, *supra* note 17, at 193.

¹⁶¹ Center for Democracy & Electronic Frontier Foundation Brief, *supra* note 44, at *12 ("New devices such as smart watches and Google Glass will increase the types and amounts of electronically-stored personal information that individuals carry

¹⁵³ See Warfield, supra note 17, at 191-92 (noting that "courts will be constantly struggling with applying previous case law to new technology[; t]he decisions of *Wurie* and *Smith* are at odds as to whether a cell phone can be searched as a search incident to a lawful arrest").

¹⁵⁴ Gershowitz, *supra* note 7, at 40-41.

¹⁵⁵ *Id.* at 43.

BROOKLYN LAW REVIEW

III. PUTTING PERSONAL DIGITAL ELECTRONIC DEVICES IN A FOURTH AMENDMENT CONTEXT

Justice Brandeis predicted that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."¹⁶² It is important to recall that the Fourth Amendment offers security in "persons, houses, papers, and effects,"¹⁶³ and although "the Fourth Amendment protects people, not places,"¹⁶⁴ the Supreme Court has suggested that the home enjoys strong protection.¹⁶⁵ This is because the "home" can be a person's "most intimate and familiar space."¹⁶⁶ It is "the principal repository of our most intimate papers and effects."¹⁶⁷ Indeed, "[i]n the home, . . . *all* details are intimate details, because the entire area is held safe from prying government eyes."¹⁶⁸

Justice Brandeis's cautionary note has borne out with new technology.¹⁶⁹ Recent decades have witnessed the "rapid integration of computers into nearly every facet of society."¹⁷⁰ As a result, "[c]omputer searches and home searches are similar in

¹⁶³ U.S. CONST. amend. IV.

¹⁶⁵ See, e.g., Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (noting that "when it comes to the Fourth Amendment, the home is first among equals"); Kyllo v. United States, 533 U.S. 27, 33 (2001) (noting that in "a private home . . . [is] where privacy expectations are most heightened" (quoting Dow Chem. Co. v. United States, 476 U.S. 227, 237 n.4 (1986) (internal quotation marks omitted)); Payton v. New York, 445 U.S. 573, 585-86 (1980) (noting that "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed" (quoting United States v. United States Dist. Ct., 407 U.S. 297, 313 (1972))); ACLU Brief, *supra* note 28, at *6.

¹⁶⁶ Jardines, 133 S. Ct. at 1419 (Kagan, J., concurring).

- ¹⁶⁷ ACLU Brief, *supra* note 28, at *6.
- ¹⁶⁸ Kyllo, 533 U.S. at 37.

¹⁶⁹ ACLU Brief, *supra* note 28, at *35-36 (quoting *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting)); National Press Photographers Brief, *supra* note 42, at *24 (quoting Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting)).

 $^{170}\,$ Zamani, supra note 18, at 173; see also Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").

with them each day."); National Press Photographers Brief, *supra* note 42, at *18 ("We are also at the dawn of the age of 'wearable' devices—*e.g.*, glasses and watches and other 'clothing'—that will contain even more sensitive information."); Engel, *supra* note 28, at 296; Ferguson, *supra* note 106, at 1312 ("New technological devices have and will continue to be able to see, hear, smell, and touch citizens in ways that were simply impossible in prior eras.").

¹⁶² Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting); see also ACLU Brief, supra note 28, at *35 (quoting Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting)); National Press Photographers Brief, supra note 42, at *24 (quoting Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting)).

¹⁶⁴ Katz v. United States, 389 U.S. 347, 351 (1967).

many ways."¹⁷¹ This is because "[a] laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records."¹⁷² A personal computer may be thought of as "the digital equivalent of its owner's home, capable of holding a universe of private information."¹⁷³ Perhaps "[t]he first step should be to compare computers to homes and sealed containers,"¹⁷⁴ and consider further that cell phones might be analogous to some degree to computers.¹⁷⁵

Like personal computers, cell phones and smartphones also serve as gateways to users' "virtual homes."¹⁷⁶ "They can contain voluminous quantities of information about the most intimate details of our lives, 'papers and effects' of the sort that earlier generations of Americans kept in the bureaus and cabinets of their houses."¹⁷⁷ Smartphones pose the additional concern that they, and other devices, might be used to remotely access files on computers located within the home itself.¹⁷⁸ Present cell phone technology even allows users to view the inside of their homes through cameras stationed remotely so that "[a]t the touch of a button," the search of a cell phone almost literally "becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though

¹⁷¹ Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 538 (2005) (further noting that "[i]n both cases, the police attempt to find and retrieve useful information hidden inside a closed container. At the same time, significant differences exist... Understanding how the Fourth Amendment should apply to computer searches requires appreciating those differences").

¹⁷² United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

¹⁷³ State v. Rupnick, 125 P.3d 541, 552 (Kan. 2005).

¹⁷⁴ Kerr, *supra* note 171, at 549.

 $^{^{175}\,}$ See State v. Smith, 920 N.E.2d 949, 953 (Ohio 2009) (citing Park, 2007 WL 1521573, at *8).

¹⁷⁶ ACLU Brief, *supra* note 28, at *2-3, *9; Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *8.

¹⁷⁷ ACLU Brief, *supra* note 28, at *2, *6 (citing "correspondence (personal texts and emails), records of our commercial transactions and political activities, photographs, contact lists revealing our associations, and access to our activities on the internet and in the cloud"; and further noting that "[s]martphones and other portable electronic devices are the equivalent of the cabinets, desks, bookshelves, and bureaus in an eighteenth century home"). A smartphone may represent a person's entire library. Brief for the American Library Association and the Internet Archive as Amici Curiae Supporting Riley and Wurie, Riley v. California, 134 S. Ct. 2473 (2014) (No's 13-132 & 13-212), 2014 WL 950806,, at *13 [hereinafter American Library Association Brief] ("A smartphone is a portal to a person's entire electronic library; in fact, for millions of Americans, it *is* their primary library.").

¹⁷⁸ See Zamani, supra note 18, at 185-86.

a house contains data."¹⁷⁹ So a comparison to the home serves as a useful intellectual crutch,¹⁸⁰ "serv[ing] to illustrate the deficiencies of property analogies in the context of smartphones."¹⁸¹ However, mobile devices "can potentially reveal more information about a user than even a search of one's home computer might."¹⁸²

Moreover, technological advances in personal electronic devices bring the continued integration of various aspects of life into a single access point.¹⁸³ To this end, digital devices increasingly serve as a means to access our "virtual homes."¹⁸⁴ Currently, "modern cellular phones have the capacity for storing immense amounts of private information . . . [including] address books, calendars, voice and text messages, email, video and pictures."¹⁸⁵ Aside from any tangible analogues, "[i]ndividuals can [also] store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages."¹⁸⁶ Even user-downloaded applications on the device can portray a snapshot of a person's life.¹⁸⁷ Cell phones may also contain other sensitive information such as Internet "browsing

¹⁸³ It is telling, for example, that one manufacturer advertises its latest model as a "Life Companion." See Geoff Gasior, Samsung Intros Galaxy S4 "Life Companion", TECH REPORT (Mar. 15, 2013, 9:20 AM), http://techreport.com/news/ 24506/samsungintros-galaxy-s4-life-companion (commenting that the moniker "seems a bit silly but strikes me as fairly accurate"); see also Riley, 134 S. Ct. at 2489-90 ("[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."); Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *8 ("Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living.").

¹⁸⁴ ACLU Brief, *supra* note 28, at *2-3, *9 ("Our electronic worlds, in a very real sense, *are* our new homes and our Fourth Amendment traditions demand that they be respected as such."); Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *8 ("[O]ur mobile devices are the doorways to our virtual homes."). *Cf. In re* United States, 665 F. Supp. 2d. 1210, 1213 (D. Or. 2009) (noting that, regarding "[i]nternet communications," "the Fourth Amendment's privacy protections for the home may not apply to our 'virtual home' online").

¹⁸⁵ United States v. Park, No. CR 05-375, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

¹⁷⁹ United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012).

¹⁸⁰ See, e.g., Riley v. California, 134 S. Ct. 2473, 2491 (2014) (comparing a search of remotely stored data to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house").

¹⁸¹ Zamani, *supra* note 18, at 172.

¹⁸² *Id.* at 170 (citing Boudreau, *supra* note 45); *see also Riley*, 134 S. Ct. at 2491 ("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.").

 $^{^{186}}$ Id.

¹⁸⁷ *Riley*, 134 S. Ct. at 2490.

history, purchases, and financial and medical records."¹⁸⁸ Before the advent of mobile digital devices, this is precisely "the kind of information one would have stored in one's home and that would have been off-limits to officers performing a search incident to arrest."¹⁸⁹

The intimacy of this information is potentially heightened when considering wearable technology,¹⁹⁰ the camera of which can be "like a black-box device for yourself."¹⁹¹ Consider, for example, a device called "Google Glass," essentially a "wearable computer" that functions like "futuristic glasses."¹⁹² Google sold 10 thousand models of the prototype in the spring of 2013.¹⁹³ Currently, consumers can purchase an "Explorer Edition" of the device for \$1500¹⁹⁴:

The module contains a five-megapixel camera and is capable of capturing and either storing or transmitting audio and video recordings of the wearer's activities and experiences. The wearer also has access to a heads-up display that can be used to view maps, browse websites, communicate with or without video, send texts and social media posts, or conduct any other activity currently possible on the screen of his favorite smartphone or tablet.¹⁹⁵

device's Although the future isuncertain,¹⁹⁶ other manufacturers might produce similar models; for instance, since 2006, Apple has been developing a product comparable to Google Glass.¹⁹⁷ Some media outlets have already

¹⁹² Cory Jassen, *Google Glass*, TECHOPEDIA.COM, http://www.techopedia.com/ definition/28524/google-glass (last visited Feb. 16, 2015); *see also* Holly K. Jones, *Productivity, Privacy Risks of Google Glass and Similar Devices, Part 1*, HR HERO, (Aug. 27, 2013), http://www.hrhero.com/techforhr/2013/08/productivity-privacy-risks-ofgoogle-glass-and-similar-devices-part-1/.

¹⁹³ Thompson, *supra* note 191.

 $^{194}\,$ GOOGLE PLAY, https://play.google.com/store/devices/details?id=glass_cotton (last visited Feb. 16, 2015).

¹⁹⁵ Jones, *supra* note 192.

¹⁹⁶ Henry Blodget, *Google Glass is Dead on Arrival—Here's Why*, DAILY TICKER (Aug. 23, 2013 11:34 AM), http://finance.yahoo.com/blogs/daily-ticker/google-glass-dead-arrival-why-153427339.html.

¹⁹⁷ Charlie Osborne, Apple Has Developed 'Glass' Since 2006, SMARTPLANET (Sept. 24, 2013, 11:39 PM), http://www.smartplanet.com/blog/bulletin/apple-has-developediglass-since-2006/.

¹⁸⁸ United States v. Wurie, 728 F.3d 1, 8 (1st Cir. 2013), aff'd sub nom. Riley, 134 S. Ct. 2473 (2014).

 $^{^{189}\,}$ Id. at 8 (citing Chimel v. California, 395 U.S. 752 (1969)); see also Riley, 134 S. Ct. at 2490-91 (comparing a cell phone search to "ransacking" a house).

¹⁹⁰ National Press Photographers Brief, *supra* note 42, at *18.

¹⁹¹ Clive Thompson, *Googling Yourself Takes on a Whole New Meaning*, N.Y. TIMES (Aug. 30, 2013), http://www.nytimes.com/2013/09/01/magazine/googling-yourself-takes-on-a-whole-new-meaning.html (noting that, for example, one user of a camera-equipped wearable computer device was "struck by a car and his camera caught the license-plate number").

accommodated the device's platform.¹⁹⁸ Other industries have capitalized on the technology as well.¹⁹⁹ Insurance companies have started providing coverage for Google Glass.²⁰⁰ Some commentators have even expressed optimism about the integration of Google Glass into the legal profession.²⁰¹

anticipate wider Several states also consumer acceptance of Google Glass. For instance, New Jersey has proposed legislation that makes "[t]he use of a wearable computer with head mounted display by an operator of a moving motor vehicle on a public road or highway... unlawful."202 The New Jersey bill is specifically aimed at Google Glass,²⁰³ but the bill anticipates wider industry and consumer acceptance of this new technology by defining "wearable computer with head mounted display" as "a computing device which is worn on the head of an individual and projects visual information into the field of vision of the wearer."204 Other states have proposed similar bills.²⁰⁵ States' concern about drivers wearing Google

²⁰⁰ See Claire Cain Miller, Google Glass to Be Covered by Vision Care Insurer VSP, N.Y. TIMES (Jan. 28, 2014), http://www.nytimes.com/2014/01/28/technology/ google-glass-to-be-covered-by-vision-care-insurer-vsp.html (noting that Google Glass is covered by "VSP, the nation's biggest optical health insurance provider").

²⁰¹ See Kristin Bergman, Cyborgs in the Courtroom: The Use of Google Glass Recordings in Litigation, 20 RICH. J.L. & TECH. 11 (2014) (discussing Google Glass and similar wearable technology and their possible use as an in-court litigation tool); Dan Giancaterino, Legal Research Revolutionized, GP SOLO May-June 2014, at 28, 31, available at http://www.americanbar.org/publications/gp_solo/2014/may_june/legal_ research_revolutionized.html (discussing the viability of Google Glass as "another effective legal research tool").

 $^{202}\,$ Gen. Assemb. 1802, 216th Leg., 1st Ann. Sess., $\$ 1(a) (N.J. 2014), available at http://www.njleg.state.nj.us/2014/Bills/A2000/1802_I1.PDF.

 203 Id.

 204 *Id.* The bill assesses violators a \$100 penalty in section 1(b), but does not invoke the state's "automobile insurance eligibility points" provisions except when the putative law "is used as an alternative offense in a plea agreement to any other offense in Title 39 of the Revised Statutes that would result in the assessment of motor vehicle points," *id.* at § (1)(c), (d), although the bill would "take effect immediately," *id.* at § 2.

²⁰⁵ See, e.g., Assemb. 8496, 237th Leg. Sess. (N.Y. 2014), available at http://assembly.state.ny.us/leg/?default_fld=&bn=A08496&term=2013&Text=Y; H.D. 1281, 434th Sess. (Md. 2014), available at http://mgaleg.maryland.gov/2014RS/bills/hb/hb1281f.pdf; S. 35, 62d Leg., Budget Sess. (Wyo. 2014), available at http://legisweb.state.wy.us/ 2014/Introduced/SF0035.pdf; H.R. 155, 147th Gen. Assemb., 1st Reg. Sess. (Del. 2013), available at http://legis.delaware.gov/LIS/lis147.nsf/vwLegislation/HB+155/\$file/legis.html.

¹⁹⁸ See, for example, the New York Times' invitation to "Experience the award-winning journalism of The New York Times on Google Glass," indicating an icon reading, "Connect my Glass," *available at* http://www.nytimes.com/googleglass (last accessed Feb. 15, 2015).

¹⁹⁹ For instance, Starwood Hotels and Resorts invites guests to "[e]xperience SPG in a whole new way with the SPG on Glass app. Search over 1,100 hotels and resorts, access up-to-date account information and view upcoming stay details. SPG for Glass also lets you get turn-by-turn directions, explore photos, book and call any hotel." SPG App for Google Glass, STARWOOD PREFERRED GUEST, http://www.spgforglass.com/ (last visited Feb. 20, 2015).

Glass is more than hypothetical: a California woman was cited for wearing her Google Glass while driving in violation of the state's vehicle code provision prohibiting "operating a videodisplay in front of the driver's head rest where it can distract the driver."²⁰⁶ The citation was dismissed because there was insufficient evidence that the Google Glass was turned on, and because there was no specific state vehicle code provision addressing the device.²⁰⁷

Another example of emerging wearable technology is the "smartwatch"—a "watch[] [that] pair[s] with your cellphone/tablet to provide easy access to calls, messages, and offer[s] a portable camera and a slew of apps (depending on the model)"²⁰⁸—and there are "dozens" of these types of mobile devices in development.²⁰⁹ Moreover, some models are "standalone," able to "run independently" without the aid of another device,²¹⁰ thus placing them in a category beyond simply a smartphone extension. These are but two examples of the expanding mobile digital device market,²¹¹ perhaps harbingers of personal electronic devices yet to come.²¹²

Google Glass users may risk accidentally recording video content, increasing the likelihood that what was captured was not intended to be "projected in front of someone else's

²⁰⁶ Heather Kelly, *Ticket for Driving in Google Glass Dismissed*, CNN (Jan. 17, 2014, 1:22 PM), http://www.cnn.com/2014/01/16/tech/innovation/google-glass-ticket-dismissed/.

 $^{^{207}}$ Id.

²⁰⁸ Zara Stone, *SmartWhat? Smartwatch. Just, Why?*, ABC NEWS (Sept. 5, 2013), http://abcnews.go.com/ABC_Univision/smartwatch-whats-deal-web-connected-wrist-candy/ story?id=20168783.

²⁰⁹ Christopher Mims, Almost Every Major Consumer Electronics Manufacturer is Now Working on a Smart Watch, QUARTZ (July 5, 2013), http://qz.com/101058/smart-watch-explosion/.

²¹⁰ Saqib Khan, Omate TrueSmart is Yet Another Smartwatch with Impressive Features, VALUEWALK (Sept. 23, 2013, 10:05 AM), http://www.valuewalk.com/ 2013/09/omate-truesmart-yet-another-smartwatch-impressive-features/.

²¹¹ See Highlights from 2014 Consumer Electronics Show, PHYS.ORG (Jan. 11, 2014), http://phys.org/news/2014-01-highlights-consumer-electronics.html [hereinafter Highlights 2014] (commenting that the 2014 Consumer Electronics Show will showcase different types of "wearable technology," "[f]rom connected socks and bras to baby clothing").

²¹² See Engel, *supra* note 28, at 296 (arguing that "[t]he development of smart phones is not the first and will not be the last time that the courts will be asked to determine precisely what protection the Fourth Amendment affords people. Furthermore, the development of smart phones is not the first and will not be the last time that the courts will be confronted with a new technology that renders the prior answers to that question obsolete"); *see also* Barry Neild, *How Mobiles of the Future Will Get Under Our Skin*, CNN (Feb. 23, 2012, 10:26 AM), http://www.cnn.com/2012/02/23/tech/mobile/technology-mobilefuture/ (suggesting "that currently available medical diagnostic hardware could become standard [with mobile devices], offering real time biometrics that will detect health problems, alert physicians, and prevent serious illness").

BROOKLYN LAW REVIEW

eves."213 This is problematic because "no police officer would be able to know in advance" if searching a particular device, or application within that device, will reveal "intimate' details."214 Moreover, given that the files stored on a device might be "intermingl[ed],"²¹⁵ courts "would have to develop а jurisprudence specifying which ['digital'] home activities are 'intimate' and which are not."216

The Stakes Α.

The stakes are high. The Supreme Court has already protected the potentially intimate information stored on a person's cell phone by requiring police officers to get a warrant before conducting a search.²¹⁷ In addition to the personal details a cell phone search may reveal,²¹⁸ many people store sensitive private information on their digital devices that they might find to be embarrassing and damaging to their reputation if seen by unintended viewers, even if the content does not implicate any illegal conduct. Consider the practice known as "sexting"—a term derived from a "blend of sex and texting" that is defined as "the sending of sexually explicit messages or images by cell phone,"²¹⁹ or "texting naked or sexually suggestive photos of yourself."220 Indeed, it is increasingly becoming "perfectly normal" to "sext[] with a romantic partner."²²¹ A recent study has suggested that "[s]exting ... is

²¹³ Samantha Murphy Kelly, No, You Can't Borrow My Google Glass, MASHABLE (June 19, 2013), http://mashable.com/2013/06/19/google-glass-borrow-no/.

²¹⁴ See Kyllo v. United States, 533 U.S. 27, 38-39 (2001) (discussing why "[l]imiting the prohibition of thermal imaging to 'intimate details' would not only be wrong in principle; it would be impractical in application"); see also Riley v. California, 134 S. Ct. 2473, 2492 (2014) (noting why a proposed limitation on the scope of cell phone searches would be inadequate: "officers would not always be able to discern in advance what information would be found where"); ACLU Brief, supra note 28, at *4.

²¹⁵ See United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) (noting "a far greater potential 'for the "intermingling" of documents and a consequent invasion of privacy when police execute a search for evidence on a computer" (quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001))).

²¹⁶ See Kyllo, 533 U.S. at 38-39 (discussing why "[l]imiting the prohibition of thermal imaging to 'intimate details' would not only be wrong in principle; it would be impractical in application").

²¹⁷ *Riley*, 134 S. Ct. at 2490, 2495.

²¹⁸ Id. at 2489-90.

²¹⁹ Sexting, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/ sexting (last accessed Feb. 16, 2015).

²²⁰ Benny Evangelista, Sexting Now a Normal Dating Ritual for Young Adults, Study Says, S.F. GATE (July 24, 2012, 5:52 PM), http://blog.sfgate.com/ techchron/2012/07/24/sexting-now-a-normal-dating-ritual-for-young-adults-study-says/.

rapidly becoming part of the dating process."²²² This study further concluded that "sexting is not related to sexual risk behavior or psychological well-being."²²³ One of the "co-principal investigator[s] of the study" suggested that "[t]he findings contradict the public perception of sexting, which is often portrayed in the media and elsewhere as unsavory, deviant, or even criminal behavior."²²⁴ This lends credence to the conclusion that an individual may have completely legally innocent and legitimate reasons to be concerned about the extent of Fourth Amendment protection of the content of one's device from the prying eyes of the law enforcement officials.²²⁵

The argument that a person's mobile device may contain sensitive content that makes a person's right to be secure from unreasonable searches paramount is not to say, however, that the Fourth Amendment offers protection because of any "general constitutional 'right to privacy" in the Amendment.²²⁶ While the Fourth Amendment does protect privacy, "[t]he Amendment does not protect the merely subjective expectation of privacy, but only those expectation[s] that society is prepared to recognize as 'reasonable."²²⁷ There is "[n]o single factor" that is determinative of "whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by a warrant."²²⁸ Yet, critically, one of the factors that the Court has identified is "our societal understanding that certain areas deserve the most scrupulous protection from government

 227 Oliver v. United States, 466 U.S. 170, 177 (1984) (second alteration in original) (quoting Katz, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted)).

 $^{228}\,$ Id. at 177-78 (citing Rakas v. Illinois, 439 U.S. 128, 152-53 (1978) (Powell, J., concurring)).

²²² Deborah Gordon-Messer et al., *Sexting Among Young Adults*, 52 J. OF ADOLESCENT HEALTH 301, 301 (2012), *available at* http://deepblue.lib.umich.edu/ bitstream/handle/2027.42/106606/Sexting%20among%20young%20adults.pdf?sequence =1&isAllowed=y.

 $^{^{223}\,}$ Gordon-Messer et al., supra note 222, at 301. The study did note, however, that "further research is needed to examine the association between sexting and mental health." Id. at 306.

²²⁴ Laura Bailey-Michigan, For Young Adults, "Sexting" Just Part of Dating, FURTURITY (July 26, 2012), http://www.futurity.org/for-young-adults-sexting-justpart-of-dating/.

²²⁵ See Gershowitz, supra note 7, at 44.

²²⁶ Katz v. United States, 389 U.S. 347, 350 (1967) (stating that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy"); *see also* Newhard v. Borders, 649 F. Supp. 2d 440, 449-50 (W.D. Va. 2009) ("[W]hether or not [the plaintiff'-arrestee] had a constitutional right to privacy in the nude pictures," the court concluded "that [his] claim to a constitutional right of privacy in the [nude] images on the cell phone is dubious, at best.").

invasion."²²⁹ Given the potentially sensitive nature of information stored on mobile devices,²³⁰ it is important to consider the potential repercussions if the authority to determine the scope of a search of a mobile device is removed from the hands of "a neutral and detached magistrate" and given to "officer[s] engaged in the often competitive enterprise of ferreting out crime."²³¹

To this end, consider the case where "a public school teacher was arrested for driving while intoxicated."232 In this case, "[t]he arresting officer patted [the arrestee] down pursuant to a search incident to arrest and found a cell phone in his pocket. The officer opened the phone's photograph folder and discovered pictures of the schoolteacher and his naked girlfriend 'in sexually compromising positions."²³³ The arresting officers "allegedly alerted several additional [officers], deputies, and members of the public that the private pictures were available for their viewing and enjoyment."234 Whatever recourse these individuals ultimately received to remedy the harm from the police misconduct, surely they would have preferred—and likely expected if the recent "sexting" studies are any indication—that the police not search their phones in the first place. This is, after all, the level of protection for cell phones that the Supreme Court has since declared the Fourth Amendment provides,²³⁵ which is little consolation for people whose phones were searched pre-*Riley*.²³⁶

It is admittedly unlikely that the Court would be willing to rely on arguably "vulgar" content as a basis for recognizing

 $^{\rm 234}$ $\,$ Newhard, 649 F. Supp. 2d at 444 (internal quotation marks omitted).

 $^{235}\;$ Riley v. California, 134 S. Ct. 2473, 2483, 2493 (2014).

²²⁹ Id. at 178 (citing Payton v. New York, 445 U.S. 573 (1980)).

²³⁰ See, e.g., Riley v. California, 134 S. Ct. 2473, 2489-90, 2494-95 (2014); United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, *8 (N.D. Cal. May 23, 2007); ACLU Brief, *supra* note 28, at *2.

²³¹ Johnson v. United States, 333 U.S. 10, 13-14 (1948).

 $^{^{232}\,}$ Swingle, supra note 17, at 36 (citing Newhard v. Borders, 649 F. Supp. 2d 440, 444 (W.D. Va. 2009)).

²³³ Id. (quoting Newhard, 649 F. Supp. 2d at 444).

²³⁶ Cf. Davis v. United States, 131 S. Ct. 2419, 2423-24 (2011) ("hold[ing] that searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule"); United States v. Spears, No. 4:14-cr-82-O, 2014 WL 3407930, at *3-4 (N.D. Tex. July 14, 2014) (acknowledging *Riley*'s retroactive application, but applying *Davis* to admit cell phone evidence). *But see* United States v. Collazo, No. 3:13-00209, 2014 WL 3853841, at *10 (M.D. Tenn. Aug. 6, 2014) (suppressing cell phone evidence in light of *Riley*); United States v. Jenkins, No. 3:13-00209, 2014 WL 2933192, at *4 (S.D. Ill. June 30, 2014) (suppressing cell phone evidence in light of *Riley*); see also Groh v. Ramirez, 540 U.S. 551, 555-56, 563 (2004) (noting how an officer might violate Fourth Amendment rights and be immune from civil suit through qualified immunity).

Fourth Amendment protection. Indeed, *Riley* does not rest on those grounds.²³⁷ Further, Justice Scalia has lamented that "[w]e indeed live in a vulgar age."²³⁸ He recently reiterated that he is "nervous about our civic culture[,]" in part because society has "coarsened in so many ways."²³⁹ In particular, he finds the "coarseness of manners" in "modern society" upsetting, including "constant use of the F-word," as well as the prevalence of nudity in movies and television.²⁴⁰ Given this concern, it seems likely that Justice Scalia—and maybe other members of the bench—would convey limited sympathy for a party seeking to vindicate their privacy interests where the underlying conduct is arguably "vulgar." Yet the Court should recognize changing perceptions of acceptable behavior, and reflect rather than guide what "society is prepared to recognize as 'reasonable."²⁴¹

B. A Call to Explicitly Extend Riley to all Mobile Digital Devices

In holding that police officers may not search a cell phone incident to arrest, the Supreme Court has laid a groundwork for similar searches of any mobile digital device.²⁴² The Court explained that "[t]he term 'cell phone' is itself a misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."²⁴³ The Court thus shed light on the path forward for other digital devices that can be thought of as

²³⁹ Jennifer Senior, *In Conversation: Antonin Scalia*, N.Y. MAG., Oct. 14, 2013, at 25, *available at* http://nymag.com/news/features/antonin-scalia-2013-10/#print.

²³⁷ *Riley*, 134 S. Ct. at 2494-95 (concluding that "[m]odern cell phones.... hold for many Americans 'the privacies of life" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))). But note that in discussing how "[m]obile application software on a cell phone, or 'apps'.... can form a revealing montage of the user's life," the Court cited "apps for improving your romantic life." *Riley*, 134 S. Ct. at 2490.

 $^{^{238}\,}$ Lee v. Weisman, 505 U.S. 577, 637 (1992) (Scalia, J., dissenting). In this Establishment Clause case, Scalia further urged: "But surely 'our social conventions,' have not coarsened to the point that anyone who does not stand on his chair and shout obscenities can reasonably be deemed to have assented to everything said in his presence." *Id.* (citation omitted).

²⁴⁰ *Id.* at 26.

²⁴¹ See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); see also Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *3 ("Reasonableness is not fixed to a particular technology level... leaving the citizenry at the 'mercy of advancing technology.' Rather, as technology advances, and society's use of that technology creates new privacy expectations, what is reasonable is viewed anew." (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001))).

 $^{^{242}}$ See ACLU Brief, supra note 28, at *6 n.2; Center for Democracy & Electronic Frontier Foundation Brief, supra note 44, at *13.

²⁴³ Riley v. California, 134 S. Ct. 2473, 2489 (2014).

"minicomputers" or are capable of putting "vast quantities of personal information literally in the hands of individuals."²⁴⁴ Many of the features of cell phones upon which the Court relied have little to do with the telephonic capabilities of the device.²⁴⁵

Before the Court decided *Riley*, some scholars suggested that their analysis of cell phones and smartphones should apply to mobile devices generally.²⁴⁶ But courts should not only "impose tighter limits"²⁴⁷ and "exclude these devices from the traditional doctrines,"²⁴⁸ as the Court did in *Riley*,²⁴⁹ they should adopt a bright-line rule that excludes them altogether from the search-incident-to-arrest exception by explicitly extending *Riley*.²⁵⁰ Waiting for new digital technology to be adopted by consumers before courts adopt functional standards applicable to a given device diminishes the privacy protected by the Fourth Amendment.²⁵¹ A clear rule excluding all digital devices from a search incident to arrest would readily

 $^{249}\,$ Riley, 134 S. Ct. at 2489 (concluding that "any extension of . . . reasoning [applicable to physical objects] to digital data has to rest on its own bottom").

²⁵⁰ See Pincus, supra note 49, at 328-29 ("*Riley* addressed digitally stored information on a cell phone, but it is difficult to see how a different result could possibly apply to searches incident to arrest of the contents of tablets, laptops, or thumb drives. All share the characteristics relied on by the *Riley* Court, and a warrant therefore should be required to conduct such searches.").

²⁵¹ See Orin Kerr's pre-*Riley* comment discussing the different technology at issue before the Court. Kerr, *supra* note 40 (noting that "two cert petitions], Petition for a Writ of Certiorari, *Riley v. California*, 2013 WL 3934033 (U.S.) (No. 13-132), and Petition for a Writ of Certiorari, *United States v. Wurie*, 2013 WL 4404658 (U.S.) (No. 13-212),] have been filed seeking review of how the Fourth Amendment applies to searching a cell phone incident to arrest[,]" and further noting that, given the differences in technology between the two cases, "[r]eviewing [the] case with an earlier model phone[, i.e. *Wurie*,] would lead to a decision with facts that are atypical now and are getting more outdated every passing month"); *see also* Kerr, *supra* note 38 ("Changing technology is a moving target, and courts move slowly...").

 $^{^{244}}$ Id. at 2485. But note that the Court also cited "an element of pervasiveness that characterizes cell phones but not physical records." Id. at 2490. Emerging technology, by definition, is not pervasive.

²⁴⁵ *Id.* at 2489-90.

²⁴⁶ See, e.g., ACLU Brief, supra note 28, at *6 & n.2; Center for Democracy & Electronic Frontier Foundation Brief, supra note 44, at *13; Criminal Law Professors Brief, supra note 44, at *1; Samuel J. H. Beutler, Note, The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest, 15 VAND. J. ENT. & TECH. L. 375, 401(2013) (arguing "that the appropriate test for the scope of a cell phone search incident to arrest should concern the function of a cell phone" and therefore "be limited to the traditional functions of a cell phone– namely, phone calls and text messages"); Scheurer, supra note 44, at 327; see also Engel, supra note 28, at 296-97 (arguing that "courts should recognize that certain electronic devices are reasonably likely to contain intimate personal information about a person, and to exclude these devices from the traditional doctrines," for example, by "impos[ing] tighter limits on law enforcement's review of cell phone data than... law enforcement's review of what numbers were dialed").

²⁴⁷ Engel, *supra* note 28, at 296.

²⁴⁸ Id. at 297.

encompass new technological advances 252 and allow the increasing privacy interests at stake "the protection for which the Founders fought." 253

The Supreme Court has vacillated between proclaiming bright-line Fourth Amendment rules and more fact-specific inquiries.²⁵⁴ However, the Court has already recognized the need for a bright-line rule to govern cell phone searches incident to arrest: police officers must "get a warrant."²⁵⁵ The Court explained in *Riley* its "general preference to provide clear guidance to law enforcement through categorical rules."²⁵⁶ In response to the proposal that the Court deviate from this preference and adopt a standard for cell phone searches modeled on Arizona v. Gant,257 the Court stated that "Gant relied on 'circumstances unique to the vehicle context."²⁵⁸ In particular, it noted "a reduced expectation of privacy' and 'heightened law enforcement needs' when it comes to motor vehicles."259 The Court recognized that not only do "cell phone searches bear neither of those characteristics," but a standard for cell phones fashioned after *Gant* "would prove no practical limit at all."260 Nor would a standard that permitted a search of digital content on a cell phone with "a pre-digital counterpart" be sufficient protection of the privacy interests in cell phones.²⁶¹ These same concerns logically extend to other digital devices.²⁶²

A bright-line rule would also avoid the problems arising from Riley by requiring officers in the field to determine whether the particular mobile device in a given case is

 $^{^{252}\,}$ ACLU Brief, supra note 28, at *6 & n.2; Center for Democracy & Electronic Frontier Foundation Brief, supra note 44, at *13; Criminal Law Professors Brief, supra note 44, at *1.

²⁵³ *Riley*, 134 S. Ct. at 2495.

²⁵⁴ Missouri v. McNeely, 133 S. Ct. 1552, 1564 (2013) (rejecting a "categorical approach" to the exigent circumstance exception that would permit warrantless blood sampling of suspected drunk drivers because, in that context, a "broad categorical approach... would dilute the warrant requirement in a context where significant privacy interests are at stake"); Hon. Daniel T. Gillespie, *Bright-Line Rules: Development of the Law of Search and Seizure During Traffic Stops*, 31 LOY. U. CHI. L.J. 1, 27-28 (1999) (noting that early courts created bright-line rules for automobile searches, but that later cases made the rules "murky and difficult... to comprehend").

²⁵⁵ *Riley*, 134 S. Ct. at 2495.

²⁵⁶ Id. at 2491.

²⁵⁷ 556 U.S. 332 (2009).

²⁵⁸ Riley, 134 S. Ct. at 2492 (quoting Gant, 556 U.S. at 343).

 $^{^{259}\,}$ Id. at 2492 (quoting Thornton v. United States, 541 U.S. 615, 631 (2004) (Scalia, J., concurring)).

 $^{^{260}}$ Id.

²⁶¹ Id. at 2493.

²⁶² Pincus, *supra* note 49, at 328-29.

reasonable to search.²⁶³ A rule extending *Riley* would supply officers with clear guidance by prohibiting the search of all digital devices.²⁶⁴ Each year, a law enforcement officer making an arrest may confront an increasingly diverse array of "wearable [mobile] technology."²⁶⁵ In the absence of an explicit rule forbidding the searches of all digital devices, an officer would make an initial decision whether a particular device could be searched, and so the ultimate determination of the reasonableness by "a neutral search's and detached magistrate"²⁶⁶ would be an after-the-fact occurrence.²⁶⁷ In light of the high stakes involved due to the potentially sensitive nature of information stored on these devices,²⁶⁸ this type of post hoc analysis is inadequate protection because it would not prevent the intrusion itself,²⁶⁹ nor does it reflect the realities of rapid consumer acceptance of new technology.²⁷⁰

While the Fourth Amendment is about privacy, it is also about security in that privacy. Although the right shields an individual's privacy interest, by its plain language, it also guarantees "[t]he right...to be secure . . . against unreasonable searches."271 Indeed, the Court has stated that the harm from unreasonable searches "is not the breaking of his doors, and the rummaging of his drawers"; rather, "the essence of the offence" lies in "the invasion of his indefeasible right of *personal security*....²⁷² However, if the promise of the Fourth Amendment is "to forever secure the people ... against all unreasonable searches," and if "[t]his

²⁶⁶ Johnson v. United States, 333 U.S. 10, 13-14 (1948).

²⁷¹ U.S. CONST. amend. IV.

²⁷² Weeks v. United States, 232 U.S. 383, 391 (1914) (emphasis added) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

 $^{^{263}}$ See United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009), cert. denied, 556 U.S. 1196 (2009) (arguing that "to require police officers to ascertain the storage capacity of a cell phone before conducting a search would simply be an unworkable and unreasonable rule").

²⁶⁴ See Riley, 134 S. Ct. at 2491; Gillespie, *supra* note 254, at 3 ("The development of bright-line rules in search and seizure cases helps law enforcement officials [because they] can more easily instruct officers in broad, clear-cut terms as to the legal procedures for conducting searches and seizures.").

²⁶⁵ See Highlights 2014, supra note 211 and accompanying text.

 $^{^{267}}$ See Riley, 134 S. Ct. at 2493 (noting how a proposed "analogue test" left open the question of "how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact").

 $^{^{268}\,}$ See United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

²⁶⁹ Cf. United States v. Leon, 468 U.S. 897, 906 (1984) ("The wrong condemned by the Amendment is 'fully accomplished' by the unlawful search . . . itself." (quoting United States v. Calandra, 414 U.S. 338, 354 (1974))).

²⁷⁰ See Brenner, supra note 2.

protection reaches all alike, whether accused of [a] crime or not,"²⁷³ then courts must be sensitive to the ways in which mobile technology continues to change social conceptions of "persons, houses, papers, and effects."²⁷⁴

However, the lack of consistent application of the Fourth Amendment to cell phones before *Riley* demonstrates how consumers can be left without any true security from unreasonable searches in their devices.²⁷⁵ Yet, it is desirable that there be uniformity in the application of federal constitutional rights.²⁷⁶ And indeed, "the Constitution requires *'uniformity* of decisions throughout the whole United States, upon all subjects within [its] purview."²⁷⁷ It is a "fundamental principle' of our Constitution . . . that a single sovereign's laws should be applied equally to all."²⁷⁸ Therefore, courts should be forward-looking in crafting new Fourth Amendment rules to be applied to mobile technology in anticipation of future advances.²⁷⁹ A clear bright-line rule applied to all digital devices would avoid inevitable divergent lower court holdings.

²⁷⁵ See Engel, *supra* note 28, at 297 ("To continue to treat advanced devices like smart phones as containers under an analytical doctrine originally developed when such devices were nonexistent or new would be to permit the use of technology that is commonly available and used by the public to erode the privacy guarantees of the Fourth Amendment." (footnote omitted)).

²⁷⁶ See Justin F. Marceau, Un-Incorporating the Bill of Rights: The Tension Between the Fourteenth Amendment and the Federalism Concerns that Underlie Modern Criminal Procedure Reforms, 98 J. CRIM. L. & CRIMINOLOGY 1231, 1301 (2008) (citing Martin v. Hunter's Lessee, 14 U.S. (1 Wheat.) 304, 347-48 (1816)) ("[F]ederal review is the touchstone of uniformity and fairness in the application of federal law.").

²⁷⁷ Danforth v. Minnesota, 552 U.S. 264, 301-02 (2008) (Roberts, C.J., dissenting) (alteration in original) (quoting *Martin v. Hunter's Lessee*, 14 U.S. (1 Wheat.) at 347-48).

²⁷⁸ Id. at 301-02 (2008) (Roberts, C.J., dissenting) (quoting Justice Sandra Day O'Connor, Our Judicial Federalism, 35 CASE W. RES. L. REV. 1, 4 (1984-85)).

²⁷⁹ Cf. Kyllo, 533 U.S. at 36 (noting that when applying Fourth Amendment to thermal imaging of the home, "the rule [the Court] adopt[s] must take account of more sophisticated systems that are already in use or in development") (emphasis added); see also Olmstead v. United States, 277 U.S. 438, 471, 474 (1928) (Brandeis, J., dissenting) (arguing that, with regards to the Fourth Amendment implications of wiretapping, "our contemplation cannot be only of what has been but of what may be. The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping.") (internal quotations omitted and emphasis added); Blake Stubbs, Note, Technological Ubiquity and the Evolution of Fourth Amendment Rights, 62 DRAKE L. REV. 575, 598 (2014) ("Legal professionals and judicial officials—and the American

²⁷³ Id. at 392.

²⁷⁴ See U.S. CONST. amend. IV; ACLU Brief, supra note 28, at *2-3, *9; Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *3, *8; National Press Photographers Brief, supra note 42, at *14-15 (noting the need for "drawing a line so as not to permit 'technology to erode the privacy guaranteed by the Fourth Amendment") (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)); see also Riley v. California, 134 S. Ct. 2473, 2490-91 (2014) (comparing a cell phone search to "ransacking [a] house").

Moreover, a bright-line rule applying *Riley* to all mobile digital devices is the best way to protect the privacy interests of innocent people whose devices are searched.²⁸⁰ For the innocent victim of a Fourth Amendment violation who is not exposed to criminal proceedings, there are serious hurdles to vindication: any criminal procedural remedies such as the exclusionary rule are not helpful,²⁸¹ and qualified immunity poses serious barriers to a civil suit.²⁸² The availability of other remedies²⁸³ in state law tort claims, for example²⁸⁴—offers some peace of mind regarding outrageous police behavior, but the Fourth Amendment's guarantee to be secure in one's privacy requires that it be given its own means of vindication.²⁸⁵ A bright-line rule forbidding warrantless searches of digital devices incident to arrest might help victims of a violation show that the right was "clearly established" as needed to defeat an officer's claim to qualified immunity.²⁸⁶ Whether or not a bright-line rule would help a person overcome qualified immunity's hurdles to a civil remedy, however, a clear rule would provide definite

 281 See United States v. Leon, 468 U.S. 897, 911 (1984) (noting that the exclusionary rule's purpose is to have a "deterrent effect").

 $^{283}\,$ For pre-Riley arguments for a legislative solution, see, e.g., Kerr, supra note 38; Scheurer, supra note 44, at 290.

people—must ensure that law enforcement agencies do not abuse their modern tools in a way that circumvents or undermines the Fourth Amendment's guarantees.").

 $^{^{280}}$ Riley v. California, 134 S. Ct. 2473, 2490 (2014) (noting that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate"); Pincus, *supra* note 49, at 328-29.

²⁸² See Newhard v. Borders, 649 F. Supp. 2d 440, 447-50 (W.D. Va. 2009) ("It is unnecessary to address the broader question of whether the various officers' alleged misconduct violated Newhard's constitutional rights because, regardless of whether those rights existed and were actually violated, none of those rights were 'clearly established' at the time of the alleged misconduct. As such, the [police officer defendants] should all [be] entitled ... to qualified immunity from Newhard's § 1983 claims." (footnote omitted)).

²⁸⁴ See Newhard, 649 F. Supp. 2d at 444, 450 (stating that the arrestee plaintiff's remedy for police officers' displaying nude pictures of the arrestee and his girlfriend from the arrestee's cell phone "may fall within the ambit of state tort law," despite the lack of a remedy for a "violat[ion of] any constitutional rights that were 'clearly established").

²⁸⁵ See Riley, 134 S. Ct. at 2491 (noting that "the Founders did not fight a revolution to gain the right to government agency protocols"); Leon, 468 U.S. at 900, 906 (noting, when considering the use of the exclusionary rule where the "evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but [was] ultimately found to be unsupported by probable cause[,]" that "the use of [the] fruits of a past unlawful search... works no new Fourth Amendment wrong. The wrong condemned by the Amendment is fully accomplished by the unlawful search... itself, and the exclusionary rule is neither intended nor able to cure the invasion of the defendant's rights which he has already suffered." (emphasis added) (internal citations and quotations marks omitted)).

²⁸⁶ Cf. Newhard, 649 F. Supp. 2d at 447.

boundaries to "[t]he wrong condemned by the Amendment [that] is fully accomplished by the unlawful search . . . itself."²⁸⁷ Additionally, standing limitations prevent third parties affected by Fourth Amendment violations from bringing constitutional claims.²⁸⁸

One court concluded that the Fourth Amendment does not protect, for instance, text messages that a person sends to a third party and that are discovered during a subsequent lawful search, because that person "runs the risk that" someone other than the intended recipient would be in possession of the phone and see the message.²⁸⁹ In another case, a district court elaborated: "An individual must have a 'legitimate expectation of privacy' to contest a search on Fourth Amendment grounds."290 In that case, the plaintiff's nude images on a third person's cell phone were at issue, and because the plaintiff's "subjective expectation of privacy in the images on the cell phone [was] not disputed, the only question [was] whether her expectation was 'objectively reasonable' under the circumstances."291 Finding that "the images could have been exposed to a variety of different parties without [her] permission under a multitude of possible scenarios,"292 the court concluded that the plaintiff "lacked an objectively reasonably expectation of privacy in the images ... [and therefore] lack[ed] standing."293 Hence, a clear bright-line rule that offers individuals true security from unreasonable searches with respect to their digital devices is critical if the Fourth Amendment is to be given its due deference.²⁹⁴

There are, of course, countervailing governmental interests that push back against the application of a bright-line rule excluding the search of mobile digital devices incident to arrest: the data could "be vulnerable to two types of evidence destruction unique to digital data—remote wiping and data encryption."²⁹⁵ These methods might permit evidence

²⁹³ *Id.* at 440.

²⁸⁷ See Leon, 468 U.S. at 906 (citations and internal quotation marks omitted).

²⁸⁸ United States v. Payner, 447 U.S. 727, 731-32 (1980).

 $^{^{289}\,}$ State v. Hinton, 280 P.3d 476, 482 (Wash. Ct. App. 2012), rev'd 319 P.3d 9, 11 (Wash. 2014) (reversing on state constitutional grounds).

 $^{^{290}\,}$ Casella v. Borders, 649 F. Supp. 2d 435, 439 (W.D. Va. 2009) (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978)).

 $^{^{291}}$ Id.

 $^{^{292}}$ Id.

²⁹⁴ See Warfield, supra note 17, at 192-93 ("Although there are many bright line' tests in Fourth Amendment law, the standards for a search of a cell phone need to be truly demarcated. No one is served by ambiguous rules.").

²⁹⁵ Riley v. California, 134 S. Ct. 2473, 2486 (2014).

destruction even after police officers had seized a device.296 However, as the Supreme Court explained, these concerns are "afield" from Chimel's focus on the defendant's affirmative actions.²⁹⁷ unsupported by empirical evidence.²⁹⁸ and can be addressed through "specific means."299 Police officers can remove a cell phone's battery, or place it in a Faraday bag-"an enclosure that isolates the phone from radio waves" and is "essentially [a] sandwich bag[] made of aluminum foil."300 And, although courts should apply a bright-line rule for searches incident to arrest, in a particular case, a warrantless search might be justified under a different exception.³⁰¹ For instance, to the extent that a police officer in a particular case is presented a "now or never' situation" in which the "circumstances suggest[] that" the data stored on a defendant's device will be destroyed, police might "rely on exigent circumstances to search the phone immediately."302 Maintaining a general bright-line rule that requires a warrant to search a mobile digital device, but permitting some searches if justified by exigent circumstances, provides a "more targeted" method of contending with concerns over evidence loss.³⁰³

Finally, emerging technology—like Google Glass and other logical outgrowths—fundamentally alters the equation.³⁰⁴ Consider any minor infraction for which one might be arrested, such as driving with a suspended license, like the defendant in *United States v. Quintana*.³⁰⁵ The court invalidated the search of the defendant's cell phone because it was unrelated to "the

²⁹⁶ Id.

 $^{^{297}}$ Id. ("As an initial matter, these broader concerns about the loss of evidence are distinct from *Chimel*'s focus on a defendant who responds to an arrest by trying to conceal or destroy evidence within his reach.").

 $^{^{298}}$ *Id.* ("We have also been given little reason to believe that either problem is prevalent. The briefing reveals only a couple of anecdotal examples").

²⁹⁹ Id. at 2487.

³⁰⁰ Id.

³⁰¹ *Id.* at 2487-88.

³⁰² Id. at 2487 (quoting Missouri v. McNeely, 133 S. Ct. 1552, 1561-62 (2013)).

 $^{^{303}}$ Id. at 2487-88; see also McNeely, 133 S. Ct. at 1564-66 (adhering to the "totality of the circumstances analysis" for exigent circumstances as applied to warrantless blood sampling of suspected drunk drivers because "a categorical approach... would dilute the warrant requirement in a context where significant privacy interests are at stake").

³⁰⁴ See, e.g., National Press Photographers Brief, supra note 42, at *18; Steven I. Friedland, Cell Phone Searches in a Digital World: Incorporating Function As Well As Form in Fourth Amendment Analysis, 19 TEX. J. C. L. & C.R. 217, 226-27 (2014). (citing other "smart' devices" such as smart watches and Google Glass as clear examples of "[t]he separation of form and function" in cell phones).

³⁰⁵ United States v. Quintana, 594 F. Supp. 2d 1291 (M.D. Fla. 2009).

preservation of evidence related to the crime of arrest."³⁰⁶ *Riley* eschews any such rule, instead requiring a warrant absent some exigent circumstances.³⁰⁷ Indeed, even with cell phones,

[i]t would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone.³⁰⁸

But consider if the defendant had been wearing Google Glass one can readily imagine a colorable argument that the officer might reasonably believe the device captured evidence through footage of the defendant driving, especially since this footage may well have been captured inadvertently.³⁰⁹ One can easily conjure equally plausible scenarios: from texting while driving,³¹⁰ to violating a state law prohibiting the use of such devices while driving.³¹¹ These concerns about smartphones³¹² are compounded by the increasingly private nature of the information more advanced devices can collect.³¹³

In addition, Google Glass might allow individuals to take "sexting" to the next level.³¹⁴ In spite of the fact that

³¹² *Riley*, 134 S. Ct. at 2492; Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *17-18; Criminal Law Professors Brief, *supra* note 44, at *23-24.

³¹³ See Center for Democracy & Electronic Frontier Foundation Brief, supra note 44, at *12 ("New devices such as smart watches and Google Glass will increase the types and amounts of electronically-stored personal information that individuals carry with them each day."); Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *8 ("Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living."); National Press Photographers Brief, supra note 42, at *18 (noting that "wearable' devices... will contain even more sensitive information" than cell phones); Ferguson, supra note 106, at 1312.

³¹⁴ See Heather Kelly, Google Bans Porn on Google Glass, CNN (June 4, 2013, 2:25 PM), http://www.cnn.com/2013/06/03/tech/mobile/google-adult-glass/.

³⁰⁶ Id. at 1299-1301.

³⁰⁷ Riley v. California, 134 S. Ct. 2473, 2493-95 (2014).

³⁰⁸ Id. at 2492; see also Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *17-18; Adam M. Gershowitz, Texting While Driving Meets the Fourth Amendment: Deterring Both Texting and Warrantless Cell Phone Searches, 54 ARIZ. L. REV. 577, 579-80 (2012).

³⁰⁹ See Kelly, supra note 213.

³¹⁰ Gershowitz, *supra* note 308, at 579-80; *see also Riley*, 134 S. Ct. at 2492; Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *17-18.

³¹¹ See, e.g., Gen. Assemb. 1802, 216th Leg., 1st Ann. Sess.§ 1(a) (N.J. 2014), available at http://www.njleg.state.nj.us/2014/Bills/A2000/1802_I1.PDF; see also Criminal Law Professors Brief, supra note 44, at *20-21; Gershowitz, supra note 308, at 579-80 (discussing the possibility for police to search a cell phone for evidence of texting while driving).

BROOKLYN LAW REVIEW

"Google doesn't want porn on Glass,"³¹⁵ an "adult app company[,] MiKandi[,] recently sponsored a professional pornographic video shot with Google Glass."³¹⁶ The company has also released "the first porn app for Google Glass," although the company has faced roadblocks with Google's policy prohibiting "Glassware content that contains nudity, graphic sex acts, or sexually explicit material."³¹⁷ Nevertheless, "Glass has a built-in camera, and email, video chat, and texting capabilities," and hence Google cannot deter the determined "inner amateur pornographer" from making and sharing a video.³¹⁸ Thus, advancing technology expands the boundaries and intimate contents of "our virtual homes,"³¹⁹ magnifying both the heightened privacy concerns with existing devices, and the new Fourth Amendment concerns they present.³²⁰ Hence, courts should explicitly extend the Supreme Court's command to police in *Riley* to "get a warrant" to search a cell phone³²¹ to include all mobile digital devices.

CONCLUSION

The amount of data potentially revealed during a search of one's digital device can be staggering,³²² and may be "highly personal."³²³ The Supreme Court has heeded the call for protecting cell phones³²⁴ by requiring police to "get a warrant."³²⁵ But courts should read *Riley* broadly and explicitly require warrants for all mobile digital devices.³²⁶ With digital devices, content that is private may be stored directly alongside data

³²⁰ See Riley v. California, 134 S. Ct. 2473, 2489-91 (2014); see also, e.g., State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009); Gershowitz, supra note 7, at 40-41.

³²¹ *Riley*, 134 S. Ct. at 2495.

 $^{322}\,$ See, e.g., id. at 2489, 2491; Zamani, supra note 18, at 171-72 (suggesting that storage capacity of smartphones are "of near infinite proportions").

³¹⁵ Alexis Kleinman, Professional Glass Porn Is Here and Google Can't Stop It, HUFFINGTON POST (July 24, 2013, 9:13 PM), http://www.huffingtonpost.com/2013/ 07/24/google-glass-porn_n_3644321.html.

 $^{^{316}}$ Id.

³¹⁷ See Kelly, supra note 314.

³¹⁸ Kleinman, *supra* note 315.

³¹⁹ See ACLU Brief, supra note 28, at *2-3, 9; Criminal Defense Lawyers and Brennan Center Brief, supra note 46, at *8. Cf. In re United States, 665 F. Supp. 2d. 1210, 1213 (D. Or. 2009) (noting that, regarding "[i]nternet communications," "the Fourth Amendment's privacy protections for the home may not apply to our 'virtual homes' online").

³²³ United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007); see also, e.g., Riley, 134 S. Ct. at 2489-90.

³²⁴ Gershowitz, *supra* note 74, at 1131 ("[T]here is a strong need for judicial or legislative intervention to curb the search-incident-to-arrest doctrine for cell-phone searches.").

³²⁵ *Riley*, 134 S. Ct. at 2495.

³²⁶ See ACLU Brief, supra note 28, at *6 n.2.

which may also be the legitimate aim of an officer's search,³²⁷ and yet any rule that would require police "to know *in advance*" whether a search would reveal "intimate' details... would be impractical in application."³²⁸ With devices offering capabilities indistinguishable from a camera,³²⁹ easy—indeed, perhaps accidental—access to image capturing,³³⁰ and "near infinite" storage,³³¹ it becomes increasingly plausible that a search of a device's stored photographs would expose an individual's entire and boundless collection of captured images.³³²

The implications of mobile digital devices being interwoven into the fabric of American life³³³ are profound. Technology continues to facilitate the integration of a user's life into a single access point,³³⁴ and indeed, as Justice Brandeis predicted, allows "the Government, without removing papers from secret drawers, . . . to expose to a jury the most intimate occurrences of the home."³³⁵ This points to the obvious limitations of applying a container analogy to such devices,³³⁶ and further, how technology expands the scope and centrality of our "virtual homes."³³⁷ We should be concerned about the

- ³²⁹ Graham, *supra* note 24.
- ³³⁰ Kelly, *supra* note 216.
- ³³¹ Zamani, *supra* note 18, at 172.

³³² See Riley, 134 S. Ct. at 2489 (noting that "the data on a phone can date back to the purchase of the phone, or even earlier"). Cf. American Library Association Brief, *supra* note 177, at *13 ("A smartphone is a portal to a person's entire electronic library; in fact, for millions of Americans, it *is* their primary library.").

³³³ See Riley, 134 S. Ct. at 2489-90 ("[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."); Brenner, *supra* note 2.

³³⁴ It is telling, for example, that one manufacturer advertises its latest model as a "Life Companion." *See* Gaslor, *supra* note 183; *see also Riley*, 134 S. Ct. at 2489-90. Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *8 ("Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living."); Leone, Freedman & Silvia, *supra* note 48, at 30.

³³⁵ Olmstead v. United States, 277 U.S. 438, 471, 474 (1928) (Brandeis, J., dissenting); see also ACLU Brief, supra note 28, at *35 (quoting Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting)); National Press Photographers Brief, supra note 42, at *24 (quoting Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting)).

³³⁶ See, e.g., Riley, 134 S. Ct. at 2488-89; State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) ("We thus hold that a cell phone is not a closed container for purposes of a Fourth Amendment analysis."); Stillwagon, *supra* note 17, at 1168-69, 1206 ("Cell phones are not simply analogs of other personal items[.]").

³³⁷ See ACLU Brief, supra note 28, at *2-3, *9 ("Cell phones and other portable electronic devices are, in effect, our new homes[.]...our virtual homes....Our

 $^{^{327}}$ See Riley, 134 S. Ct. at 2492 ("[O]fficers would not always be able to discern in advance what information would be found where."); United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011).

³²⁸ See Kyllo v. United States, 533 U.S. 27, 38-39 (2001) (emphasis in the original) (discussing why "[l]imiting the prohibition of thermal imaging to 'intimate details' would not only be wrong in principle; it would be impractical in application").

extent to which law enforcement may rummage through our "virtual homes."³³⁸ Most cell phone users keep their phone nearby,³³⁹ and as devices become more mobile,³⁴⁰ our proximity to them will likely become more constant. And cell phone searches themselves already run the risk of revealing more private details of a person's life than a search of his or her house.³⁴¹ Courts should read *Riley* broadly when confronted with a warrantless search of any aspect of the "virtual home."³⁴² By explicitly forbidding police officers from searching all mobile digital devices as an incident of a lawful arrest, courts can fulfill the promise of security from unreasonable searches that the Fourth Amendment offers.

Tristan M. Ellis[†]

³³⁹ *Riley*, 134 S. Ct. at 2490.

electronic worlds, in a very real sense, *are* our new homes and our Fourth Amendment traditions demand that they be respected as such."); Criminal Defense Lawyers and Brennan Center Brief, *supra* note 46, at *8 ("[O]ur mobile devices are the doorways to our virtual homes.") *Cf. In re* United States, 665 F. Supp. 2d. 1210, 1213 (2009) (noting that, regarding "[i]nternet communications," "the Fourth Amendment's privacy protections for the home may not apply to our 'virtual home' online").

³³⁸ See Riley, 134 S. Ct. at 2490-91; ACLU Brief, *supra* note 28, at *2-3, *6 n.2 (noting implications the Court's decision will have on "laptops, thumb drives, and other portable electronic devices").

³⁴⁰ See Wearable Technology Future Is Ripe for Growth—Most Notably among Millennials, Says PwC US, PWC (Oct. 21, 2014), http://www.pwc.com/us/en/pressreleases/2014/wearable-technology-future.jhtml.

³⁴¹ *Riley*, 134 S. Ct. at 2491 ("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.").

 $^{^{342}\,}$ See ACLU Brief, supra note 28, at *2-3, *6 n.2; Pincus, supra note 49, at 328-29 and accompanying text.

[†] J.D. Candidate, Brooklyn Law School, 2015; M.A., Brandeis University, 2011; B.A., Brandeis University, 2009. Thank you to the *Law Review* staff for their thoughtful feedback and comments throughout the writing process.