Article

Cell Phone Searches in a Digital World: Incorporating Function as well as Form in Fourth Amendment Analysis

Steven I. Friedland*

I. INTRODUCTION

> *Look at that chair, we understand it because its form and function are the same thing, which is how the manufactured world has been for hundreds of years . . . . And then incredibly and relatively recently, there's this opportunity but with a set of problems to create objects whose forms don't hint at what they do. And they're packed with incredible sophistication and capability.*[1]

Both state and federal courts are split[2] on whether searches of cell phone contents in the possession of a person subject to a lawful arrest are permissible under the Fourth Amendment.[3] The Supreme Court has had the opportunity to review two cell phone search cases in its 2013–2014 term after accepting certiorari in *United States v. Wurie*,[4] a First Circuit

---

* Professor of law and senior scholar at Elon University School of Law. The author wishes to thank Caroline Johnson and Susanna Guffey for their terrific research assistance. The author also wishes to thank Meagan Moffitt for her superb administrative support. Finally, the author thanks Professor Jancy Hoeffel.

[1] Marco della Cava, *Jony Ive: The Man Behind Apple's Magic Curtain*, USA TODAY (Sept. 19, 2013, 6:04 PM), http://www.usatoday.com/story/tech/2013/09/19/apple-jony-ive-craig-federighi/2834575/, <http://perma.cc/Z4H6-G2QD> (internal quotation marks omitted) (quoting Jony Ive, the Apple designer behind iMacs and iPod).

[2] This split—described in detail in Part III—involves disparate outcomes and rationales by both federal and state courts involving various kinds of cell phone technology.

[3] U.S. CONST. amend. IV (guaranteeing "[t]he right of the people to be secure in their persons . . . and effects, against unreasonable searches and seizures," and affirming that "no Warrants shall issue, but upon probable cause.").

[4] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014) (No. 13-212). Cert was granted to answer "whether the Fourth Amendment permits the police, without obtaining a warrant, to review the call log of a cell phone found on a person who has been lawfully arrested." Petition for Writ of Certiorari at I, *Wurie*, 134 S. Ct. 999 (No. 13-212).

case, and *People v. Riley*,[5] a state court case. *Wurie* involved a police search of a cell phone's faceplate, the telephone number of a person who had just called the phone, and the name associated with that number. *Riley* involved the search of a "smartphone" by police officers who searched and located incriminating texts on the phone.

The current split in courts evidences a central contradiction. On the one hand, Fourth Amendment exceptions need predictability and clarity to guide the relationship between the public and government agents engaged in crime interdiction. Technological advances, on the other hand, cloud the application of the seemingly bright-line search and seizure rules by separating form from function and introducing new facts into the calculus that transform both pre-digital understandings and the resulting legal analysis.[6] In the past, the Supreme Court has tended to eschew considering the particular sensory-enhancing technology involved and its impact on reality in its Fourth Amendment analysis. Instead, the Court's analysis has tended to return to the pre-digital world of form, rather than function.[7] This is especially true with the bright-line "wingspan" test adopted in *Chimel v. California*[8] that police only have authority to search incident to lawful arrest the arrestee's person and area within her immediate control.[9]

The bright lines of the wingspan test established in *Chimel* worked

---

[5] People v. Riley, No. D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013), *review denied*, No. S209350 (May 1, 2013), *cert. granted in part*, 134 S. Ct. 999 (2014) (No. 13-132). Cert was granted to answer whether "the Fourth Amendment permits police officers to conduct a warrantless search of the digital contents of an individual's cell phone seized from the person at the time of arrest." Petition for Writ of Certiorari at i, *Riley*, 134 S. Ct. 999 (No. 13-132).

[6] Professor Orin Kerr explains this concept thusly: "A law created for one world may have a very different impact when applied to the facts of a different era. As a result, changing technology and social practice often trigger a need for legal adaptation." Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 403 (2013). Professor Kerr's comment is also reflected in a constitutional application of Gresham's Law, where Fourth Amendment general principles may marginalize specific provisions that might be appropriately applicable to situations where advanced technology is implicated. *See* Steven R. Smith, *Gresham's Law in Legal Education*, 17 J. CONTEMP. LEGAL ISSUES 171, 173–76 (2008) (explaining that Gresham's Law—"cheap money drives out dear, if they exchange for the same price"—can be applied to non-monetary situations by analogy to show how easier, more simplistic approaches may be attractive but often result in less value).

[7] For example, in *United States v. Jones*, Justice Sotomayor noted in her concurrence that while some forms of surveillance do not involve physical intrusion, the government will increasingly be capable of monitoring suspects by using "vehicle tracking devices or GPS-enabled smartphones" and lamenting that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance." 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring). However, the majority refused to address the dilemma Justice Sotomayor raised: "We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved . . . but there is no reason for rushing forward to resolve them here." *Id.* at 954 (majority opinion).

One major exception to this general proposition can be found in *Kyllo v. United States*, where the Court directly addressed the thermal-imaging technology at issue in the case: "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search—at least where (as here) the technology in question is not in general public use." 533 U.S. 27, 34 (2001) (citation omitted) (internal quotation marks omitted).

[8] 395 U.S. 752 (1969).

[9] *Id.* at 768.

well in a world configured by physical doors and walls.[10] Unfortunately, the bright-line rules created for physical spaces simply do not neatly apply to technologies that have created different types of barriers and access to information. The Court's refusal to adequately address advancing technology has eroded Fourth Amendment protection.[11] However, the search of cell phones incident to lawful arrest provides a chance for courts to recognize and tackle the sea change that is occurring in a device-driven, information society.[12] Without new restrictions, the ability of police to obtain access to this vast amount of material will provide an unprecedented opportunity for law enforcement—cell phones offer a huge source of discretionary information for police and investigators, who will continue to seek advantage and efficiency through technology.

Courts considering these searches have used a wide variety of comparisons and analogues.[13] These comparisons and analogues generally have not worked, and the facially neutral narratives the courts have used have been fractured and unsatisfying. This Article suggests that the preferable solution for cell phone searches incident to arrest is to consider the specific functionality of cell phones, not their form. Functionally, cell phones are portals to information past, present, and future, requiring presumptive privacy protection. A functional approach uses multiple considerations, including hyper-local information[14] related to the following factors: (1) the invasiveness, duration, and intent[15] of the government conduct; and (2) the nature, exposure, and impact of the

---

[10] *See, e.g.*, *id.* at 763 (recounting the easily understood doctrine that disallows the routine search of rooms "other than that in which an arrest occurs" absent a search warrant (citing Katz v. United States, 389 U.S. 347, 352 (1967)).

[11] This erosion was foreshadowed by *Kyllo v. United States*, where the Court indicated that an intrusion into a constitutionally protected area by technology enhancement may not be a search if the "technology in question" is one that is generally available for public use. 533 U.S. at 34 (finding the use of thermal-imaging to detect heat emanating from a private residence unconstitutional).

[12] Looking at the increasing number of mobile devices and data connections bears out this change. For example, in the United States, "mobile data traffic in 2013 was equivalent to 51x the volume of U.S. mobile traffic . . . in 2008." *VNI Mobile Forecast Highlights, 2013–2018*, CISCO, http://www.cisco.com/c/dam/assets/sol/sp/vni/forecast_highlights_mobile/index.html#~Country (selecting "United States" and "2013 Year in Review") (on file with TEX. J. C.L. & C.R., *available at* http://perma.cc/9EYD-AT89).

Moreover, "46.5 million net new devices . . . were added to the mobile network in 2013" (32.3 million of those were smartphones) and it is estimated that there will be "2.0 mobile connections per capita . . . by 2018, up from 1.2 mobile connections per capita in 2013." *VNI Mobile Forecast Highlights, 2013–2018*, CISCO, http://www.cisco.com/c/dam/assets/sol/sp/vni/forecast_highlights_mobile/index.html#~Country (selecting "United States" and "Network Connections") (on file with TEX. J. C.L. & C.R., *available at* http://perma.cc/9279-7AMN).

[13] Analogue as used in this Article means "something that is similar to something else in design, origin, use, etc." MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/analogue, <http://perma.cc/7UF5-9S4E>.

[14] "Local information structures" are pluralistic and focus on frameworks within a specific, applicable context. *See* discussion *infra* Part V.A.

[15] By including intent, the test limits government discretion to engage in invasive tactics. Even the Third Amendment reflects concern about invading the privacy of a home. U.S. CONST. amend. III (guaranteeing that "No Soldier shall, in the time of peace be quartered in any house, *without the consent of the Owner*, nor in time of war, but in a manner to be prescribed by law.") (emphasis added).

invasion,[16] particularly whether the technology is in "general public use"[17] or not.

Part II of this Article discusses what a cell phone is. Part III then explores the basic doctrine for searches incident to a lawful arrest and the current split in the case law. Part IV shows why existing analogies based on pre-digital physical reality generally fail. Part V contains the Article's proposal to use functionality in evaluating whether the police conducted a lawful search of a cell phone incident to arrest.

II. WHAT IS A CELL PHONE?

"Information is power."[18]

The question about what constitutes a cell phone seems almost trivial, but the answer is evolving, depending on the nature of the technology associated with the device and how it is used. The devices at the heart of the digital age, such as tablets and cell phones, are not merely accessories in the transition to new cultures and understandings, but rather the instruments of new realities[19] that drive the transformation,[20] particularly with respect to data accumulation and

---

[16] In light of new realities and rationales for searches incident to arrest, searches of smartphones incident to lawful arrests should generally be considered privacy encroachments, requiring some legitimate and articulable reason for the search. In *Katz v. United States*, the Supreme Court emphasized, "the Fourth Amendment protects people, not places." 389 U.S. 347, 351 (1967). The Court went on to explain that while the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy,'" it does protect individual privacy against the particular *kinds* of governmental intrusion with which the Fourth Amendment is concerned. *Id.* at 350–51.

[17] Kyllo v. United States, 533 U.S. 27, 34 (2001). The *Kyllo* Court indicated that an intrusion into a constitutionally protected area by technology enhancement is a search, at least when "the technology in question is not in general public use." *Id.* This idea has already become outdated within the past decade because of how quickly technology use spreads from one sector of society to another.

[18] Eric Schmidt, *The Courage to Be Unreasonable*, U. PA. ALMANAC SUPPLEMENT, May 26, 2009, at IV, *available at* http://www.upenn.edu/almanac/volumes/v55/n34/pdf_n34/Commencement2009.pdf, <http://perma.cc/XS55-6A7U>. In a commencement speech at the University of Pennsylvania in 2009, the executive chairman of Google discussed the implications behind advancing technology, "connected-ness," and the "opportunity to have everyone in the world have access to all the world's information." *Id.* at III–IV.

[19] In the 1960s, social theorist and critic Marshall McLuhan suggested that the dominant electronic media in any given era might actually transform society by influencing how the brain works and processes information, thereby *creating* new patterns of thought and behavior. *See generally* MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN (1964).

[20] For example, these devices have led younger Americans to "adopt new ways of getting around," which is changing the nation's transportation landscape: driving is not their default option; they tend to "choose the best mode of transportation, such as driving, transit, biking or walking, based on the trip they are planning"; they "consider public transportation the best option for digital socializing and one of the most likely ways to connect with the communities they live in"; they work "while they travel'; and "Internet and mobile communications are fueling a wave of new transportation services enabled by technology, such as car-sharing, bike-sharing and ride-sharing." Larry Copeland, *Young People Driving Less*, USA TODAY (Oct. 1, 2013, 10:37 PM), http://www.usatoday.com/story/news/nation/2013/10/01/social-media-driving-millennials/2898093/, <http://perma.cc/TES5-734Z>.

analysis.[21] These realities not only affect the experience of daily life but also feature an increasing separation of form and function, where a phone is not just a phone—if it is primarily used that way at all. While people laughed at the shoe phone worn by secret agent Maxwell Smart in the television show and film *Get Smart*, it has presaged reality.[22]

A. Evolution of Cell Phones

Cell phones, introduced commercially by Motorola in the early 1980s,[23] are now used worldwide.[24] For many people, cell phones are the primary means of structured communication, even replacing home "landlines,"[25] and the number of mobile-exclusive users is growing exponentially.[26] It is estimated that, as of January 2014, 90% of adults in the United States has a cell phone.[27] While the cell phone was initially and primarily used to make telephone calls, it has become a multifunctional tool that can more appropriately be called a pocket supercomputer.[28]

---

[21] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted) ("the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."). While an analysis of Third-Party Doctrine is beyond the scope of this Article, it is worth noting several relevant points. It is much more difficult to define and maintain freedom from government and private intrusion given government-private partnerships and the routing of almost all information through third parties. An all-or-nothing definition of privacy is no longer functional. Information travels, is stored with various companies, and is accessible by many. Information has great value, from biometrics, to DNA, to social security and credit card numbers.

[22] An Australian scientist has built a working version of a shoe phone using twenty-first century technology, anticipating "serious applications for [the kind of technology used in the shoe, paired with monitoring sensors] in the medical field." David Greig, *The Smart Phone—Maxwell Smart, That Is*, GIZMAG (Mar. 5, 2009), http://www.gizmag.com/shoe-phone/11166/, <http://perma.cc/FGX3-NLJV>.

[23] Maggie Shiels, *A Chat with the Man Behind Mobiles*, BBC NEWS (Apr. 21, 2003, 9:41 AM), http://news.bbc.co.uk/2/hi/uk_news/2963619.stm, <http://perma.cc/GS7S-Y4LR>. The first Motorola prototype was produced in 1973. *Id.*

[24] *Global Mobile Statistics 2013 Part A*, MOBITHINKING, http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers, <http://perma.cc/843L-D5G7> (approximately 96% of the world's population has a subscription to a mobile phone and the penetration of cell phones even in developing nations is around is 89%).

[25] *Id.* (reporting that "[m]obile subscriptions outnumber fixed lines 6:1").

[26] STEPHEN J. BLUMBERG & JULIAN V. LUKE, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JANUARY – JUNE 2013, 1 (2013), *available at* http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201312.pdf, <http://perma.cc/4ULV-9A6Q> (noting that "[t]wo in every five American Homes (39.4%) had only wireless telephones . . . during the first half of 2013—an increase of 1.2 percentage points since the second half of 2012"). Similar trends appear in data usage: during the period 2013 to 2018, mobile data traffic in the United States is estimated to "grow 3 times faster than fixed IP traffic." *VNI Mobile Forecast Highlights, 2013–2018*, CISCO, http://www.cisco.com/c/dam/assets/sol/sp/vni/forecast highlights_mobile/index.html#~Country (selecting "United States" and "2018 Forecast Highlights") (on file with TEX. J. C.L. & C.R., *available at* http://perma.cc/JE28-F3RM).

[27] *Mobile Technology Fact Sheet*, PEW RES. INTERNET PROJECT, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/, <http://perma.cc/EXN2-9MUV>.

[28] *Id.* ("As of May 2013, 63% of adult cell owners use their phones to go online [and] 34% of [those]

It was not long ago that supercomputers took up several large rooms and were measured in multiples of cubic feet.[29] Over the years, as computing times rapidly decreased and the space required for processing shrank,[30] it was only a matter of time before these computers were married to the cell phone. So-called smartphones are much more than phones: many are equipped with Internet access, can provide applications that create a GPS system, can make reservations at restaurants, can transmit and receive e-mails and texts, and can link to calendars and contact lists.[31] Furthermore, the amount of information processed on smartphones is expected to increase forty-seven times between 2013 and 2018.[32] In short, these devices now can—and will increasingly be able to—store and disseminate huge amounts of data, which is a wellspring of evidence for criminal investigators.[33]

B. Expanding Capabilities

The information that cell phones store and utilize also can be very personal, such as information relating to personal health, family, religion, and critical decisions relating to autonomy (e.g., abortion, illness, doctors, and even personal hygiene).[34] The applications contained in phones—combined with the photos stored in it, the notes taken, e-mails

---

go online mostly using their phones, and not using some other device such as a desktop or laptop computer."); *see also Cell Phone Activities 2013*, PEW RES. INTERNET PROJECT (Sept. 19, 2013), http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/, <http://perma.cc/8TZQ-NVE6> (reporting that, beyond making phone calls, many users text, access the Internet, send and receive e-mail, get directions, listen to music, and make video calls with their phones).

[29] *See, e.g.*, WIKIPEDIA, http://en.wikipedia.org/wiki/File:CDC_6600.jc.jpg, <http://perma.cc/A2HW-JE5J> (last modified Jan. 21, 2010) (showing a picture of the IBM CDC 6600, first delivered in 1964, and "generally considered to be the first successful supercomputer.").

[30] The capacity of computers has increased exponentially since their development in the last part of the twentieth century, doubling in short periods of time. In fact, "Moore's Law" (actually a supposition) posits that the advances of transistors on integrated circuits doubles every two years. *Moore's Law Inspires Intel Innovation*, INTEL, http://www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html, <http://perma.cc/M22W-PJN2>; *see also* AL GORE, THE FUTURE: SIX DRIVERS OF GLOBAL CHANGE 53 (2013) (describing the exponential growth of processing power).

[31] The capabilities of smartphones include: sending and receiving phone calls, e-mails, instant messages, and texts; connecting to Bluetooth devices, the Internet, GPS, and Wi-Fi; taking digital photos, listening to MP3s, and playing videos; and, storing an organizer, scheduler, and address book. R. KELLY RAINER JR. & CASEY G. CEGIELSKI, INTRODUCTION TO INFORMATION SYSTEMS—SUPPORTING AND TRANSFORMING BUSINESS 242 (2011), *available at* http://www.cse.hcmut.edu.vn/~chauvtn/ebusiness_systems/Texts/0470473525%20-%20Introduction%20to%20Information%20Systems%20-%20Supporting%20and%20Transforming%20Business.pdf, <http://perma.cc/RBN3-UH4P> (explaining that while "[n]ot all of these new devices have all these capabilities . . . they are heading rapidly in that direction.").

[32] GORE, *supra* note 30, at 53.

[33] *See, e.g.*, Jake Laperruque, *CDT Asks Supreme Court to Bar Warrantless Search of Cell Phones*, CENTER FOR DEMOCRACY & TECH. (Sept. 5, 2013), https://cdt.org/cdt-asks-supreme-court-to-bar-warrantless-search-of-cell-phones/, <http://perma.cc/K5CG-8KDP> (contending that "the phone in one's pocket can contain more private information than an entire warehouse.").

[34] *See, e.g.*, Kerr, *supra* note 6, at 405 (surveying the "deeply personal" information that can be stored in a cell phone).

and text messages sent and received, and the calendar with lists of professional and personal appointments—can create a quite detailed and private picture of a person. This picture might be more complete than even that known by friends and business colleagues.

Cell phone technology continues to expand. For example, Near-Field Communication (NFC) allows direct cell phone-to-cell phone communication.[35] Other expanding technologies include: a Bluetooth health-device protocol that connects a phone to heart monitors and cardio equipment;[36] mobile security;[37] smart skin phones that take any digital image and display it across the skin of the phone;[38] and a combination phone, laptop tablet, and digital camera.[39]

To protect cell phone data, some phones have capabilities that allow for remote tracing or wiping of information.[40] Newer phones may have an activation lock that requires a password for reactivation and a custom message displayed even after a remote erase.[41] This feature is designed to deter theft of the phone for resale.[42] The iPhone 5s features fingerprint-scanning touch identification, although its security value has been questioned because of potential copying and unauthorized access.[43]

---

[35] The phones are held back-to-back to swap information. Companies such as McDonald's and Walgreens have adopted some NFC-equipped terminals for use with this technology to make commercial transactions. John Brandon, *8 Groundbreaking Mobile Tech Advancements for 2012*, POPULAR MECHANICS, http://www.popularmechanics.com/technology/gadgets/news/8-groundbreaking-mobile-tech-advancements-for-2012#slide-1.

[36] *E.g.*, *Runtastic Bluetooth Smart Heart Rate Monitor*, AMAZON, http://www.amazon.com/gp/product/B00B84JQSE/, <http://perma.cc/3QR7-YHML>.

[37] *E.g.*, *Privacy, Security and Usage*, CARRIER IQ, http://www.carrieriq.com/privacy/, <http://perma.cc/7QZS-6HDF> (explaining how mobile device diagnostic data is transmitted through a secure, encrypted channel directly from the device to an operator's network server). It should be noted that Carrier IQ was subject to controversy in late 2011, after a report acknowledged that the software was inadvertently logging keystrokes on cell phones. Sari Horwitz, *Carrier IQ Faces Federal Probe into Allegations Software Tracks Cellphone Data*, WASH. POST, Dec. 11, 2011, http://www.washingtonpost.com/business/economy/feds-probing-carrier-iq/2011/12/14/gIQA9nCEuO_story.html, <http://perma.cc/JB9P-L8V3>. Despite Congress's call to the Federal Trade Commission to probe the company, the FTC has not pursued legal action directly against Carrier IQ. Wendy Davis, *Carrier IQ Loses Bid to Send Privacy Case to Arbitration*, MEDIAPOST NEWS (Apr. 4, 2013, 1:41 PM), http://www.mediapost.com/publications/article/222977/carrier-iq-loses-bid-to-send-privacy-case-to-arbit.html, <http://perma.cc/HR5Y-UAYB>.

[38] *E.g.*, Jack Purcher, *Samsung Patent Intros a Wild Concept for Smart Device-Skins*, PATENT BOLT (Mar. 9, 2012), http://www.patentbolt.com/2012/03/samsung-patent-intros-a-wild-concept-for-smart-device-skins.html, <http://perma.cc/6FH4-N4QP> (describing the "smart device-skin" for which Samsung filed a patent application in 2011).

[39] *E.g.*, Jonathan Fincher, *Concept Fujitsu Lifebook Comes with Removable Smartphone, Tablet, and Digital Camera*, GIZMAG (Jan. 23, 2012), http://www.gizmag.com/concept-fujitsu-lifebook-2013/21183/, <http://perma.cc/WQZ3-WJUS>.

[40] *E.g.*, *iCloud*, APPLE, http://www.apple.com/icloud/find-my-iphone.html, <http://perma.cc/ZN7K-6CN3>.

[41] *E.g.*, Wilson Rothman, *Activation Lock May Be Most Important iOS7 Feature*, NBC NEWS (Sept. 18, 2013, 1:31 PM), http://www.nbcnews.com/tech/security/activation-lock-may-be-most-important-ios-7-feature-f4B11187477, <http://perma.cc/SBS2-GZRN>.

[42] *Id.*

[43] Tom Olzak, *Apple Touch ID: Do Security Advantages Outweigh Risks?*, TECHREPUBLIC (Sept. 18, 2013, 1:15 PM), http://www.techrepublic.com/blog/it-security/apple-touch-id-do-security-advantages-outweigh-risks/#, <http://perma.cc/S779-Z5EE>.

Specific computing functions of cell phones have the potential to create huge amounts of data. One example is the phone's location data. To promote the best cell phone tower signal, cell phone companies track the location of cell phones, and these locations can be identified "with remarkable precision and accuracy."[44] This data, known as historical cell phone location information, provides a fairly accurate picture of the movements of the cell phone throughout a day—and consequently, those of its owner.[45]

Portable substitutes for towers, often called Stingrays, are also utilized to track phones. Stingrays, a form of International Monitor Surveillance Instrument (IMSI), are devices that mimic cell phone towers to collect location data on nearby cell phones.[46] Data from all cell phones within a given range are received, including phones not targeted.[47] Police departments in several states have used Stingrays in crime interdiction.[48]

The huge quantities of collected electronic information can be stored and accessed from databases, providing new opportunities and sedimentary layers for historical sleuthing, as well as preserving information in perpetuity—retained data can create a trail for others to follow days, weeks, months, or years later.[49]

C. Separation of Form and Function

The mobility of cell phones is almost taken for granted, particularly when compared to the fixed nature of telephone landlines that many homes no longer use. Even the first mobile phones now look awkward,

---

[44] State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (describing how cell phones identify themselves with nearby cell towers every seven seconds and explaining that this real-time data can be collected and used to reconstruct a phone's movement over time).

[45] *Id.* (explaining how increasingly accurate cell phone location data serves to "reveal a great deal of personal information about an individual," such as disclosing "where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate.").

[46] Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, ABC NEWS 10 (Mar. 6, 2014, 11:25 PM), http://www.news10.net/story/news/investigations/watchdog/2014/03/06/ cellphone-spying-technology-used-throughout-northern-california/6144949/, <http://perma.cc/7RZ7-NE5V>. Government investigators, including the FBI, have been using stingrays since the 1990s. Declan McCullagh, *FBI Prepares to Defend 'Stingray' Cell Phone Tracking*, CNET NEWS (Mar. 27, 2013, 4:57 PM), http://news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking/, <http://perma.cc/M86B-CBVD>.

[47] *Id.*

[48] John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013, 5:10 PM), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/, <http://perma.cc/4KPM-A7XQ>.

[49] *See, e.g.*, *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart, <http://perma.cc/J2J-FD8G> (showing the retention periods that major cell phone service providers use for certain data such as: call records; cell tower usage indicating user location; text message metadata and content; pictures; and IP destination information indicating where the call, text, or email was sent).

big, and antiquated.[50] In addition, the mobility and elasticity of information used and stored in cell phones provides another important distinction from the sole function of landlines. The cell phone not only stores information sent to it by others but also sends out location information on a regular basis. This flow of information can be aggregated and evaluated by computers specially programmed to assess bytes of information,[51] colloquially known as Big Data.[52] The nature of information can be changed according to how it is aggregated and where.[53] We are often unaware that aggregations are even taking place. Thus, phones are no longer merely phones but important communication centers, data centers, and a locus for the digital culture.

Overall, given a cell phone's potential and actual uses, the consequences for telephonic communications are astounding. If a phone is not just a phone anymore, what is it: a data and information storage container; a data aggregator; a two-way radio; a tracking and transportation device; a linkage device; a portal to information, past, present, and future; or, some combination of these and other analogues? In short, a cell phone is a transformational device for the twenty-first century in the way that the automobile was a transformational device for the twentieth century.[54]

D. Phones in Other Forms

The separation of form and function can be even more clearly seen in the development of other "smart" devices. There is now a

---

[50] *See* Brett Molina, *The Mobile Phone Turns 40 Years Old*, USA TODAY (Apr. 4, 2013, 11:15 AM), http://www.usatoday.com/story/tech/personal/2013/04/03/mobile-phone-turns-40/2048889/, <http://perma.cc/D2S8-WB8B> (describing the original DynaTac from 1973 as ten inches long and weighing two and a half pounds and stating that the DynaTac was "a behemoth by today's standards," with most modern smartphones weighing between four and six ounces).

[51] *E.g.*, *Hadoop Systems*, IBM, http://www-03.ibm.com/software/products/en/category/SWP12, <http://perma.cc/M75J-WB6L>.

[52] *E.g.*, *Big Data*, IBM, http://www.ibm.com/big-data/us/en/, <http://perma.cc/NV6V-SNEG>.

[53] *See, e.g.*, Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, 90 HARV. BUS. REV. 61, 62 (2012) (describing how the nature of customer information has been changed by online shopping databases: it is no longer a simple listing of what customers buy, but is an analyzable set of data that can help retailers target certain customers based on "what else they looked at; how they navigated through the site; how much they were influenced by promotions, reviews, and page layouts; and similarities across individuals and groups.").

[54] For example, most cell phones are capable of mobile Internet and Cloud connectivity, two "rapidly evolving, potentially transformative technologies." JAMES MANYIKA ET AL., DISRUPTIVE TECHNOLOGIES: ADVANCES THAT WILL TRANSFORM LIFE, BUSINESS, AND THE GLOBAL ECONOMY 2–3 (2013), *available at* http://www.mckinsey.com/~/media/mckinsey/dotcom/insights%20and%20pubs/mgi/research/technology%20and%20innovation/disruptive%20technologies/mgi_disruptive_technologies_full_report_may2013.ashx, <http://perma.cc/N9AP-28RW>. These technologies are transformative because they contribute to social change, where new ways of doing things supplant the status quo, "rendering old skills . . . irrelevant." *Id.* at 1. In fact, mobile Internet and Cloud technologies are advancing at an explosive rate and, together, have created a culture of users who "go about their daily routines with new ways of knowing, perceiving, and even interacting with the physical world." *Id.* at 6.

commercially produced smart watch, in which Dick Tracy's cartoon reality is now functional.[55] The watch tells time but is multifunctional: it contains computing functions and has the capability of making phone calls, as well. While it might be worn as a watch, such an item is functionally less a watch than simply another form of interconnective device. Smart glasses have been developed as well. For example, Google has created Google Glass—the device is worn like a pair of eyeglasses, but calling it "glasses" would be a misnomer, given it is so much more of a multifunctional device than a monolithic tool. Google Glass can record what the wearer sees, can send a message by telling it to do so, can share what is seen, and can produce directions on the glass.[56]

In due course, the Supreme Court will need to address a broader question: whether the search of devices that are part of the Internet of Things—data driven smart devices that allow for remote operation and adjustment[57]—is permissible. In this way, the Supreme Court will have to deal less with form than with function.

III. THE SEARCH INCIDENT TO LAWFUL ARREST EXCEPTION

A. Basic Doctrine

It is well established that a search incident to a lawful arrest can be conducted without a warrant and is thus considered an exception to the warrant preference of the Fourth Amendment.[58] The origins of this exception are rooted in English antecedents of American law. Judge Benjamin Cardozo, while on the New York Court of Appeals, wrote in the case of *People v. Chiagles*[59]:

> [T]here is one exception that has been established as firmly as the rule [against unreasonable search and seizure] itself. The government may search the person of the accused when

---

[55] A Pebble watch is customizable, contains Internet-connected applications, and is capable of connecting to iPhone and Android phones via Bluetooth. *Pebble: E-Paper Watch for iPhone and Android*, KICKSTARTER, https://www.kickstarter.com/projects/597507018/pebble-e-paper-watch-for-iphone-and-android, <http://perma.cc/LCC9-4E6F>.

[56] *Welcome to a World Through Glass*, GOOGLE, http://www.google.com/glass/start/what-it-does/, <http://perma.cc/3W2X-BPJE>.

[57] Michael Chui et al., *The Internet of Things*, MCKINSEY QUARTERLY, Mar. 2010, *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things, <http://perma.cc/U43E-EFTP> ("sensors and actuators embedded in physical objects—from roadways to pacemakers—are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet. These networks churn out huge volumes of data that flow to computers for analysis.").

[58] United States v. Robinson, 414 U.S. 218, 235 (1973) (holding that a search conducted incident to a lawful arrest "is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment.").

[59] 237 N.Y. 193 (1923).

> legally arrested to discover and seize the fruits or evidences of crime. . . . There is no dearth of illustrative precedents both in our own country and abroad.[60]

The Supreme Court has established the purpose and scope of a search under this exception, as Justice Scalia observed:

> In *Chimel v. California*, we held that a search incident to arrest was justified only as a means to find weapons the arrestee might use or evidence he might conceal or destroy. We accordingly limited such searches to the area within the suspect's "immediate control"—i.e., "the area into which an arrestee might reach in order to grab a weapon or evidentiary ite[m]."[61]

The "immediate control" test described in *Chimel* connoted a person's wingspan and accessible items within reach.[62] This included bags or containers in his possession or reach.[63]

In *Thornton v. United States*,[64] another case evaluating the scope of the exception, Justice Scalia cited authorities in his concurrence for both a broad exception, allowing the search without any particularized justification,[65] and a narrower one, based on the more specific dual rationales of imminent destruction of evidence or officer safety.[66] Both approaches were viewed as deeply rooted—for example, the narrower approach had supporting authority dating back to 1758.[67]

Several significant cases served to develop the exception doctrine by recognizing its nuance and complexity while others spoke to the advancing technology of the times, such as forensic science and the automobile.

In *United States v. Robinson*,[68] the Court was confronted with the

---

[60] *Id.* at 195 (citations omitted) (internal quotation marks omitted). Judge Cardozo hinted at a still broader rationale, explaining that the exception originated with the idea that a thief caught in the act could be searched with little concern for the rights of his person. *Id.* at 196 ("The right goes back beyond doubt to the days of the hue and cry, when there was short shrift for the thief who was caught 'with the mainour,' still 'in seisin of his crime.'" (citing Pollock & Maitland History of English Law)).

[61] Thornton v. United States, 541 U.S. 615, 624 (2004) (Scalia, J., concurring) (citation omitted).

[62] Chimel v. California, 395 U.S. 752, 768 (1969), *abrogated by* Davis v. United States, 131 S. Ct. 2419 (2011).

[63] *Id.*

[64] 541 U.S. 615 (2004).

[65] Explaining the nexus or proximity approach, Justice Scalia stated that there is a "general interest in gathering evidence *related to the crime of arrest* with no mention of the more specific interest in preventing its concealment or destruction." *Id.* at 629–30 (Scalia, J., concurring) (emphasis added) (citing authorities from as far back as 1829).

[66] *Id.* at 630 (explaining that "*Chimel*'s narrower focus on concealment or destruction of evidence also has historical support."). Justice Scalia also points out that some authorities, while supporting the broader purpose for a search (to gather evidence of the crime of arrest with no other exigency required), limit the scope of the search itself to the arrestee's *person*, impliedly supporting *Chimel*'s narrower limitation. *Id.* at 631.

[67] *Id.*

[68] 414 U.S. 218 (1973).

question of whether a crumpled cigarette pack could be seized and searched as part of the exception.[69] In *Robinson*, the police lawfully arrested the defendant for driving without a license and then searched his person after the arrest.[70] They found a crumpled cigarette pack and removed the contents, which were small packages of heroin.[71] The Court recognized the dual rationales for the search incident to arrest—protecting officer safety and preventing the imminent destruction of evidence—and held that these rationales applied to containers found on the arrestee, including the pack at issue.[72]

In applying these rationales, the *Robinson* Court chose to adopt a bright-line test—the "container" rule—instead of a case-by-case analysis relying on the exigencies of the situation.[73] Under this new rule, police were given a green light to conduct searches incident to lawful arrests regardless of any suspicion or cause to believe their safety was in danger or that evidence would be compromised if they did not search.[74] However, in *United States v. Chadwick*,[75] the Court held that once "personal property not immediately associated with the person of the arrestee" had been secured—ensuring officer safety and protection of evidence—"a search of that property is no longer an incident of the arrest."[76]

United States v. Edwards[77] provided a different fact pattern. A day after being arrested and taken to jail, Edwards's clothing was seized and paint chips stuck to the clothing were taken as evidence of the crime.[78] The Court found that such a seizure was permissible even though it occurred ten hours after the arrest and detention of the defendant because he could have been searched at the time of his arrest.[79]

Finally, *New York v. Belton*[80] and *Arizona v. Gant*[81] show how searches incident to arrest are influenced by local contexts and facts, such as arrest in an automobile. *Belton* held that a car's passenger compartment could be searched as part of the search incident to arrest exception when persons were arrested *in* their cars—an increasing occurrence in the late 1900s.[82] *Belton* was seen as a way to deal with this

---

[69] *Id.* at 223.
[70] *Id.* at 220–22.
[71] *Id.* at 223.
[72] *Id.* at 234, 236.
[73] *Id.* at 235.
[74] *Id.*
[75] 433 U.S. 1 (1977) (involving the warrantless search of a footlocker under the control of law enforcement agents), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565 (1991).
[76] *Id.* at 15.
[77] 415 U.S. 800 (1974).
[78] *Id.* at 801–02. The microscopic analysis of paint flakes can be used to link an object to a crime scene or to a person (associative evidence), or to serve a variety of other evidentiary functions. ROBERT C. SHALER, CRIME SCENE FORENSICS: A SCIENTIFIC METHOD APPROACH 495 (2011).
[79] *Edwards*, 415 U.S. at 801, 807–08.
[80] 453 U.S. 454 (1981), *abrogated by* Davis v. United States, 131 S. Ct. 2419 (2011).
[81] 556 U.S. 332 (2009).
[82] *Belton*, 453 U.S. at 462–63 (finding the search of a jacket was incident to a lawful custodial arrest

recurring theme and was motivated by a desire to construct "a straightforward rule, easily applied, and predictably enforced."[83] *Gant* upset the *Belton* bright-line rule by finding that such a search was not warranted when the suspect had been taken into custody *outside* the car,[84] with some exceptions.[85]

B. Divided Approaches in the Lower Courts

The courts that have confronted the issue of whether a search of a cell phone falls within the search incident to lawful arrest exception have reached widely divergent results.[86] The two cases in which the Supreme Court has granted certiorari—*Wurie* and *Riley*—also have different outcomes, facts, and rationales. Even the relevant technology levels of the cell phones are different, reflecting the continuing, almost dizzying, advancements of technology on a regular basis. The rest of this section is divided into two parts: those cases finding that a search of a cell phone is permitted under the exception and those that find that it is not permitted.

1. Permitted Cell Phone Searches

Several circuit and state courts permitting cell phone searches incident to arrest without a warrant have utilized rationales based on location, whether the cell phone was a container, and even trivial invasiveness. Predictably, there was no singular rationale used by these courts.[87]

---

because the jacket was inside the car within the arrestee's immediate control).

[83] *Id.* at 459, 460.

[84] *Gant*, 566 U.S. at 351. The Court explained that while the *Belton* opinion "has been widely understood to allow a vehicle search incident to the arrest of a recent occupant even if there is no possibility the arrestee could gain access to the vehicle at the time of the search," the instant search was unreasonable because "police could not reasonably have believed either that Gant could have accessed his car at the time of the search or that evidence of the offense for which he was arrested might have been found therein." *Id.* at 341, 344.

[85] *Id.* at 346–47 (detailing exceptions to include "when . . . it is reasonable to believe the vehicle contains evidence of the offense of arrest," when an officer "has reasonable suspicion that an individual" is dangerous and might retrieve a weapon from the vehicle, or when an officer "reasonably suspects a dangerous person may be hiding" in the vehicle).

[86] It is assumed for the purposes of this Article that police who obtain data from a cell phone are engaged in a search and are doing so without a warrant. The focus of this Article is whether the search is justified because it is incident to a lawful arrest.

[87] *See* United States v. Florez-Lopez, 670 F.3d 803 (7th Cir. 2012) (finding the search of a cell phone to be a trivial invasion); United States v. Murphy, 552 F.3d 405 (4th Cir. 2009) (using location rationale to find the warrantless search of a cell phone found on the arrestee's person was permitted); United States v. Finley, 477 F.3d 250 (5th Cir. 2007) (using location rationale to find the warrantless search of a cell phone on the arrestee's person was permitted *and* using container rationale to find that the cell phone was a type of container); People v. Diaz, 244 P.3d 501 (Cal. 2011) (using location rationale to find a warrantless search of a cell phone on the arrestee's person permitted); Hawkins v. State, 723 S.E.2d 924 (Ga. 2012) (using container rationale to find that a cell phone is similar to a

a. The Location Rationale

People v. Riley held that a search of Riley's cell phone incident to a lawful arrest was permissible without a warrant.[88] In *Riley*, several men standing near Riley's car shot at the car of a rival gang member.[89] Riley was implicated as one of the shooters.[90] Later that month, the police stopped Riley while he was driving and decided to impound his car upon finding he was driving with an expired license.[91] After Riley was arrested, the police searched the contents of a cell phone found on his person.[92] The police then conducted an impound inventory search of the car, finding several loaded handguns and "indicia of gang affiliation."[93]

The California Court of Appeal focused on the *location* of the cell phone when it was found, noting that the "key question is whether Riley's cell phone was 'immediately associated' with his 'person' when he was stopped."[94] Because the court found it was immediately associated with his person, the exception was triggered regardless of "whether or not an exigency still existed."[95]

b. The Container Rationale

In *United States v. Finley*,[96] the Fifth Circuit found that a cell phone was a type of container on the arrestee's person akin to the cigarette pack in *Robinson*, and that the cell phone was consequently fully subject to a search incident to a lawful arrest.[97] The court observed that it was well settled that such a search is within the exception but also qualifies as a reasonable search under the Fourth Amendment.[98] The court observed that the police are permitted to seek evidence to use at trial, and that the scope of such efforts includes containers found on the arrestee's person.[99]

---

closed container); Commonwealth v. Phifer, 979 N.E.2d 210 (Mass. 2012) (finding that a cell phone search is permitted when the phone was used as a component of the crime).

[88] No. D059840, 2013 WL 475242, at *6 (Cal. Ct. App. Feb. 8, 2013), *review denied*, No. S209350 (Cal. May 1, 2013), *cert. granted in part*, 134 S. Ct. 999 (2014) (No. 13-132).

[89] *Id.* at *1.

[90] *Id.*

[91] *Id.* at *2.

[92] *Id.* at *3.

[93] *Id.* at *1, *3. Ballistics testing confirmed that the bullets from the handguns matched the bullet casings found at the scene of the shooting. *Id.* at *1.

[94] *Id.* at *6 (citing People v. Diaz, 244 P.3d 501, 505 (Cal. 2011)).

[95] *Id.*

[96] 477 F.3d 250 (5th Cir. 2007).

[97] *Id.* at 259–60. The police arrested Finley as part of a drug bust; they searched Finley's person and seized a cell phone that was in his pocket. *Id.* at 253–54. A DEA Special Agent subsequently searched the phone's call records and text messages. *Id.* at 254.

[98] *Id.* at 259.

[99] *Id.* at 259–60.

c. The Trivial Invasiveness Rationale

In *United States v. Flores-Lopez*,[100] the Seventh Circuit said the nature of the intrusion "might be so trivial that its seizure would not infringe the Fourth Amendment" at all and used pre-digital parallels such as diaries and address books to justify the search of a cell phone incident to lawful arrest.[101] Unconcerned by any privacy implications, the court noted, "[w]e are quite a distance from the use of the iCam to view what is happening in the bedroom of the owner of the seized cell phone."[102]

2. *Prohibited Cell Phone Searches Incident to Lawful Arrest*

A number of other courts have held that the search of a cell phone is not automatically permitted under the incident to lawful arrest exception when the phone is on or near an arrestee because of the *nature* of the cell phone.

a. The Cell Phone as a Type of Computer

In *United States v. Wurie*, the defendant was arrested for selling drugs and was taken to the police station, where two cell phones, keys, and cash were found on him.[103] On one cell phone, there was an external caller ID screen that flipped open.[104] The phone was not a smartphone, meaning it had limited Internet connectivity and mini-computer capabilities.[105] The police observed that the phone was repeatedly receiving calls from a caller labeled "my house" according to what appeared on the external screen.[106] The officers opened the phone and pressed a button to access the phone's call log to determine the most

---

[100] 670 F.3d 803 (7th Cir. 2012).

[101] *Id.* at 807 (denying the need for a cell phone-specific rule of law and asserting instead that because police are entitled to open and leaf through a diary or address book to ascertain the owner's address, "they should be entitled to turn on a cell phone to learn its number" or "to read the address book").

[102] *Id.*

[103] 728 F.3d 1, 2 (1st Cir. 2013), *cert. granted*, 134 S. Ct. 999 (2014) (No. 13-212).

[104] *Id.*

[105] *See id.* (describing the phone as a "gray Verizon LG phone"). When the Supreme Court decides this case, the limited *nature* of this type of cell phone may be important since these phones do not have the same level of connectivity, informational storage capacity, or technological capacity as smartphones. *See* Transcript of Oral Argument at 13–14, *Wurie*, 134 S. Ct. 999 (No. 13-212) (suggesting that turning off wireless capabilities pre-search could be a limiting principle on a warrantless search of a cell phone incident to arrest).

[106] *Wurie*, 728 F.3d at 2.

recent caller.[107] The officers typed the resulting phone number into the white pages phone directory to yield an address for the telephone number, which happened to be near where the defendant had parked his car.[108] The defendant moved to suppress the evidence resulting from the search of the cell phone.[109] The First Circuit focused on whether exigent circumstances existed to justify the search.[110] Lacking those circumstances, the court reversed the denial of Wurie's motion to suppress and vacated his conviction.[111] The court emphasized that a cell phone was far more than a mere container or wallet, saying:

> We suspect that the eighty-five percent of Americans who own cell phones . . . would have some difficulty with the government's view that "Wurie's cell phone was indistinguishable from other kinds of personal possessions, like a cigarette package, wallet, pager, or address book, that fall within the search incident to arrest exception to the Fourth Amendment's warrant requirement."[112]

Significantly, the court described cell phones in general as specialized computers, noting that the immense storage capacity of Apple's iPhone 5, for example, was equivalent to "'four million pages of Microsoft Word documents.'"[113] The court also referred to the origins of the Fourth Amendment in order to advance the specter of discretionary police dragnets within a person's cell phone:

> Just as customs officers in the early colonies could use writs of assistance[114] to rummage through homes and warehouses, without any showing of probable cause linked to a particular place or item sought, the government's proposed rule would give law enforcement automatic access to "a virtual warehouse" of an individual's "most intimate communications and photographs without probable cause" if the individual is subject to a custodial arrest, even for something as minor as a traffic violation.[115]

The court conceded that the Supreme Court has not distinguished

---

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *See id.* at 13 (finding that a showing of exigent circumstances would permit a warrantless search of a cell phone incident to arrest in certain circumstances).

[111] *Id.* at 13, 14.

[112] *Id.* at 8 (citation omitted).

[113] *Id.*

[114] A writ of assistance, also known as a general warrant, "did not confine its reach to a particular person, place, or object but allowed its bearer to arrest, search, and seize as his suspicions directed." William J. Cuddihy, *Fourth Amendment, Historical Origins of, in* 3 ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 1098, 1098 (Leonard W. Levy & Kenneth L. Karst eds., 2d ed. 2000).

[115] *Wurie*, 728 F.3d at 9. The court went on to say, "We are reminded of James Otis's concerns about 'plac[ing] the liberty of every man in the hands of every petty officer.'" *Id.*

between the types of items found in such searches or an item's "capacity to store private information"[116] as a litmus test for legitimacy but said that the searches of cell phones are qualitatively different:

> In our view . . . what distinguishes a warrantless search of the data within a modern cell phone from the inspection of an arrestee's cigarette pack or the examination of his clothing is not just the nature of the item searched, but the nature and scope of the *search itself.*[117]

b. A Cell Phone Is Not a Container

In *State v. Smith*,[118] the Ohio Supreme Court found that a cell phone search did not trigger either of the dual rationales for such an exception[119] and that the *Robinson* container conceptualization did not apply.[120] The court stated:

> Objects falling under the banner of "closed container" have traditionally been physical objects capable of holding other physical objects. Indeed, the United States Supreme Court has stated that in this situation, "container" means "any object capable of holding another object."[121]

c. Cell Phones Akin to Footlockers

In *United States v. Park*,[122] the court in the Northern District of California found that a cell phone within an arrestee's immediate control

---

[116] *Id.*

[117] *Id.* The court compares the personal nature of information stored on a cell phone to that stored in one's home, both of which contain information regarding private thoughts and activities. *Id.* at 8.

[118] 920 N.E.2d 949 (Ohio 2009).

[119] *Id.* at 955. The court explained that the evidence rationale were not triggered because, "[o]nce the cell phone is in police custody, the state has satisfied its immediate interest in collecting and preserving evidence and can take preventive steps to ensure that the data found on the phone are neither lost nor erased." *Id.* Moreover, the court stressed, "when the interests in officer safety and evidence preservation are minimized . . . this exception no longer applies." *Id.* at 952 (citing United States v. Chadwick, 433 U.S. 1, 15 (1977), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565 (1991)).

[120] *Id.* at 954 (explaining that, to trigger the closed-container rule from *Robinson*, the container must be capable of holding a physical object).

[121] *Id.* (citing New York v. Belton, 453 U.S. 454, 460 n.4 (1981), *abrogated by* Davis v. United States, 131 S. Ct. 2419 (2011)). The court went on to explain, "[e]ven the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container. We thus hold that a cell phone is not a closed container for purposes of a Fourth Amendment analysis." *Id.*

[122] No. CR-05-375-SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007).

should be considered akin to a footlocker as in *Chadwick*.[123] The court in *Park* stated, "modern cellular phones have the capacity for storing immense amounts of private information"[124] and consequently found that the dual rationales behind the exception to searches incident to lawful arrest had not been met:

> The searches at issue here go far beyond the original rationales for searches incident to arrest, which were to remove weapons to ensure the safety of officers and bystanders, and the need to prevent concealment or destruction of evidence. . . . Instead, the purpose was purely investigatory. Once the officers lawfully seized defendants' cellular phones, officers could have sought a warrant to search the contents of the cellular phones.[125]

d. Cell Phones Provide Remote Access to the Home

In the Florida Supreme Court decision *Smallwood v. State*,[126] the court looked at the potential for exposure and determined that the search of a cell phone is akin to giving the law enforcement officer a key to access the arrestee's home:

> Physically entering the arrestee's home office without a search warrant to look in his file cabinets or desk, or remotely accessing his bank accounts and medical records without a search warrant through an electronic cell phone, is essentially the same for many people in today's technologically advanced society.[127]

The court then focused on the nature of the intrusion, saying, "[w]e refuse to authorize government intrusion into the most private and personal details of an arrestee's life without a search warrant simply because the cellular phone device which stores that information is small enough to be carried on one's person."[128]

---

[123] *Id.* at *8; *Chadwick*, 433 U.S. at 13. The *Chadwick* Court held that it was unreasonable for federal agents to search a footlocker without a warrant because it was already under their "exclusive control." *Id.*

[124] *Park*, 2007 WL 1521573, at *8.

[125] *Id.*

[126] 113 So. 3d 724 (Fla. 2013).

[127] *Id.* at 738.

[128] *Id.*

e. The Owner Has a Possessory Right in the Cell Phone

Some courts have prohibited searches after focusing on aspects of phone searches other than invasion of privacy. For example, in 2012, the Seventh Circuit in *United States v. Burgard*[129] permitted a cell phone to be seized but not searched incident to lawful arrest.[130] The court treated the delayed *application* for a warrant as unreasonable and a violation of the owner's possessory rights in the seized object.[131] The court explained, "[t]he longer the police take to seek a warrant, the greater the infringement on the person's possessory interest will be . . . . But unnecessary delays also undermine the criminal justice process in a more general way: they prevent the judiciary from promptly evaluating and correcting improper seizures."[132] The court also pointed out that while there are no bright-line rules defining when a delay becomes unreasonable, "the Supreme Court has dictated that courts must assess the reasonableness of a seizure by weighing 'the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'"[133] This case aptly illustrates the intersection and overlap between property and privacy rights.

IV. WHY PRE-DIGITAL ANALOGUES DO NOT WORK

The unifunctional, physical boundaries used in pre-digital cases—such as the walls of a phone booth—no longer appear to apply to multifunctional technology that can enhance the sensory perception of law enforcement.[134] Consequently, as discussed above, courts have used an assortment of analogues to categorize cases that involve modern technological advances. These analogues draw many comparisons, which can lead to a variety of conclusions that are allegedly neutral and objective. This Part argues that the analogues often regress to pre-digital

---

[129] 675 F.3d 1029 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 183 (2012).

[130] *Id.* at 1034–35.

[131] *Id.* at 1034 (distinguishing the seizure from the search itself, which affects privacy interests).

[132] *Id.*

[133] *Id.* (citing United States v. Place, 462 U.S. 696, 703 (1983)).

[134] That is, the contents of a cell phone may be used as evidence of illegal activity without a police officer needing to witness the activity with her own eyes. As explained by the Court in *Kyllo v. United States*, sense-enhancing technology provides for something "more than naked-eye surveillance," enhances "ordinary perception," or makes the otherwise imperceptible, perceptible. 533 U.S. 27, 33, 38 n.5 (2001). For example, in *United States v. Deans*, law enforcement officers established a link between two defendants by searching the contents of a cell phone belonging to one of the defendants, rather than by seeing the two defendants together. 549 F. Supp. 2d 1085, 1093 (D. Minn. 2008), *aff'd sub nom.* United States v. Zeimes, — Fed App'x. —, 2014 WL 1673345 (8th Cir. Apr. 29, 2014).

concepts such as physical walls and doors, providing a poor fit for comparison.[135]

The judicial practice of comparing analogues is apparent in the realm of cell phone searches incident to lawful arrest. What is the proper analogue in the physical world for a cell phone, a digital device that seems to add features daily? It is clear that while cell phones are still called "phones," they are much more than that, and their functionality has grown in such a way that their telephonic capabilities play a diminishing role for some possessors. The nature of the comparison makes a difference, particularly when trying to locate these devices within a Fourth Amendment framework using case law from the pre-digital, physical world.

A. Analogue #1: Physical Proximity

The nexus or proximity approach provides the broadest and most abstract approach to analyzing cell phone searches incident to a lawful arrest.[136] It is fully based on the pre-digital physical world, with reference to space and physical distance.[137] This approach has the advantage of creating bright lines—if the object is within the wingspan of the arrestee, it may be searched without justification, as exemplified by *Gant*.[138]

The approach also offers the functional equivalent of the trespass test championed by Justice Scalia in *Jones v. United States*,[139] which involved a GPS device placed on the defendant's car without a valid warrant, and which was decided based on the physical trespass involved.[140] However, in *Olmstead v. United States*,[141] the Supreme

---

[135] For example, in his concurrence in *United States v. Jones*, Justice Alito bemoaned the use of earlier analogues to decide whether the use of twenty-first century surveillance techniques violated the Fourth Amendment. In *Jones*, the government attached a GPS device to the respondent's vehicle and monitored his movements for twenty-eight days. 132 S. Ct. 945, 948 (2012). The majority found this to be a physical occupation of private property and held that it was a search within the meaning of the Fourth Amendment at the time of its adoption. *Id.* at 949. Justice Alito complained that the Court had decided the case using eighteenth century tort law because the government had engaged in "conduct that *might have provided grounds in 1791* for a suit for trespass to chattels." *Id.* at 957 (Alito, J., concurring) (emphasis added). He went on to upbraid the majority for claiming that a similar situation could have occurred in 1791—it would have, he writes, "have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience."). *Id.* at 958 n.3.

[136] *See supra* note 65.

[137] *See, e.g.*, Thornton v. United States, 541 U.S. 615, 630 (2004) (Scalia, J., concurring) (distinguishing the broad nexus approach from a narrow focus on concealment or destruction of evidence and explaining that "[t]here is nothing irrational about broader police authority to search for evidence when *and where* the perpetrator of a crime is lawfully arrested.") (emphasis added).

[138] The Court in *Gant* also makes it very clear that "[i]f there is *no possibility* that an arrestee could reach into the area that law enforcement officers seek to search, both justifications for the search-incident-to-arrest exception are absent and the rule does not apply." 556 U.S. 332, 339 (2009) (emphasis added).

[139] 132 S. Ct. 945 (2012).

[140] *Id.* at 948–49.

Court's trespass analysis led it to the conclusion that wiretapping the telephone wires that run from a home to the outside world was not a violation of the Fourth Amendment because there was no actual "entry of the houses or offices of the defendants."[142]

The problem with this approach is that it provides no limits to the search of the objects within an arrestee's wingspan and does not provide any useful way of dealing with new multifunctional devices. That is, the proximity test overlooks the teachings of some Supreme Court cases by disregarding changing reality led by technological advances.[143] Some illustrations help explain this critique. If a person is arrested while standing near a desktop computer, would a full search of the contents of the computer, without any reasonable belief that the computer contains evidence, be lawful? If yes, would there be any limits on the search of photographs, e-mail, and web sites accessed by the user within the past year or *several* years? Perhaps most significantly, if the machine's data were stored on a cloud, meaning the data is in remote storage, could the police access the cloud as well as the device itself, if the device contained the password?

Now suppose a phone has remote capacities, meaning it can access cameras and other machines remotely. Would those be subject to access as well? For example, security cameras can be placed in a home and remotely accessed on a cell phone.[144] Would a search of the phone permit the application to be activated and the inside of the home viewed, without any more justification than that the phone was found on a person during an arrest?

Would discovery of passwords for social media such as Facebook allow the police to now access the Facebook page of the arrestee? Passwords serve as a form of key—does possessing this key give the police the power to access areas that are physically far away just because the key was on the arrestee?

Further suppose that the device was password protected and the lock was activated. Would that make a difference in the search? What if it were fingerprint protected—could the police force individuals to open their own phones for a search? If a person were able to hit a button that

---

[141] 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[142] *Id.* at 464–66.

[143] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (addressing a new technological situation in finding that government monitoring of a private home with a device not in general public use is a presumptively unreasonable search); California v. Carney, 471 U.S. 386, 393 (1985) (addressing a new technological situation in finding that "the overriding societal interests in effective law enforcement justify an immediate search [of the defendant's motor home] before the vehicle and its occupants become unavailable.").

[144] For example, the Belkin Company Netcam can be plugged into a ubiquitous electrical outlet, and operated through a downloaded application. Kevin Parrish, *Belkin Launches Wi-Fi Camera with Night Vision*, TOM'S GUIDE (Apr. 24, 2013, 5:40 PM), http://www.tomsguide.com/us/NetCam-Wi-Fi-Camera-Infrared-night-vision,news-16974.html, <http://perma.cc/ZP8J-5UMH>. It provides not only daytime surveillance, but is equipped with infrared technology to permit night views as well. *Id.* Furthermore, it is equipped with a microphone to allow for real-time audio surveillance. *Id.*

erased the data on the phone so that a police officer found nothing, would the act of erasure or attempted erasure provide a justification for the search? If the phone *were* erased, would the police be permitted to attempt to reconstruct the data on it?

The pre-digital Fourth Amendment cases further show how technology undermines the proximity test. In *California v. Ciraolo*,[145] the Court described a boundary for searches by reaffirming the doctrine of "open fields," which negated Fourth Amendment protection for areas that extended outside of a house into areas that might not be a field or even open.[146] Significantly, the Court looked at the physically unobtrusive manner in which the officers' observations took place, noting that the officers could see marijuana plants on the defendant's private property with the naked eye.[147] This doctrine essentially limited the right of privacy where private property was exposed to the public.[148] The Court also distinguished the part of the property directly surrounding a house called the "curtilage," which is presumptively private.[149] What if a cell phone had photos of the interior of the house or curtilage on it—are those areas no longer private? Could the police use those photos to then get a warrant on a different issue than the arrest to enter the house and curtilage?

These questions reveal that unifunctional analysis from the days of physical surveillance and first-hand sensory perception are distorted and sometimes fully eclipsed by advancing technology.[150]

B. Analogue #2: *Robinson* Containers

This analogue treats a cell phone like the cigarette pack in *Robinson*—as a container, it is fully within the automatic search zone of

---

[145] 476 U.S. 207 (1986) (involving the aerial observation of marijuana plants growing in the defendant's fenced yard).

[146] *Id.* at 213 (stressing that Fourth Amendment protections of the home have never extended to those parts of an individual's property viewable from "public thoroughfares," including situations where an "individual has taken measures to restrict some views of his activities.").

[147] *Id.* (noting that the observations "took place within public navigable airspace.").

[148] *Id.* ("'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'" (quoting Katz v. United States, 389 U.S. 347, 351 (1967))).

[149] The Court explained curtilage as "the area to which extends the intimate activity associated with the sanctity of a man's home and the privacies of life" and an area "intimately linked to the home, both physically and psychologically, where privacy expectations are most heightened." *Id.* at 212–13 (citations omitted) (internal quotation marks omitted).

[150] *United States v. Knotts*, for example, offered the Supreme Court an opportunity to look at the government use of beepers to track private individuals in public. 460 U.S. 276 (1983). The Court found that monitoring beeper signals did not invade "any legitimate expectation of privacy" and, therefore, was "neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment." *Id.* at 285. The Court held that because direct, visual surveillance would have revealed the same facts, the use of the beeper did not alter the defendant's expectation of privacy in any way. *Id.* at 282.

police when accomplished incident to a lawful arrest. To some extent, smartphones are containers—they contain hardware circuitry, as well as thousands of documents, photos, and other bits of information. Thus, the transition from the *Robinson* idea of a physical container that could contain contraband or a weapon to the idea of the phone as a data storage device appears to be consistent.

The problem with this approach is that while cell phones are *technically* containers, they are not *functional* containers.[151] That is, they generally are not used by the possessor to contain other physical items, like a backpack or wallet would. While the rhetorical statement is that the device "contains" information—e-mail, documents, videos, photos, etc.—these do not exist in any physical form, but exist via code. Furthermore, while trickery and deception could be applied to disguise a container (or weapon) as a cell phone,[152] the object's overwhelming usage is as a multifunctional, communications tool.

C. Analogue #3: *Chadwick* Footlockers

In *Chadwick*, the Court found:

> Once law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest.[153]

Phones are like *Chadwick* footlockers in that once securely within government possession, they are neither likely to create an imminent danger of harm to the police nor is any evidence in danger of imminent destruction.[154] This concept is also applicable when a cell phone is password protected, fingerprint protected, or otherwise locked.

The problem with this approach is that the analogy only goes so far. The capabilities of a cell phone as a container far outstrip those of a footlocker, and the kinds of activities and contents available on a phone

---

[151] Cell phones "contain" hardware circuitry, boards, SD cards, and a battery within their shells.

[152] Fake phones could, of course, be hollowed out to serve as disguised containers of contraband and other material.

[153] United States v. Chadwick, 433 U.S. 1, 15 (1977), *abrogated in part by* California v. Acevedo, 500 U.S. 565 (1991).

[154] When the primary concern of law enforcement is to preserve evidence, there are alternatives to immediately searching the phone: it can be placed in a Faraday bag or cage, which is "essentially an aluminum-foil wrap . . . which isolates the cell phone from the phone network and from Bluetooth and wireless Internet signals." United States v. Flores-Lopez, 670 F.3d 803, 809 (7th Cir. 2012). In most cases, law enforcement could also simply turn the phone off or remove its battery. So long as one of these measures is taken, the phone is generally safe from being remotely wiped. *See* Transcript of Oral Argument, *supra* note 105, at 47–49.

cover a huge range; that is, a cell phone is both qualitatively and quantitatively different from a conventional storage container.

Further, the cell phone might indeed be a part of the crime for which the suspect was arrested, such as selling drugs; in that circumstance, it should be subject to search. In *People v. Diaz*,[155] for example, the defendant was arrested after driving a car allegedly shepherding buyers of drugs to the seller.[156] The defendant denied any involvement.[157] However, after the police viewed the suspect's phone, they found a message stating, "6 4 80," which they believed was code for a drug sale: "[s]ix pills of Ecstasy for $80."[158] After the police confronted the defendant with this new information, he confessed.[159]

D. Analogue #4: Automobiles

When one looks for advancing technology that transforms Fourth Amendment analysis, one need look no further than the automobile, which also transformed much of society during its development. That is, like cell phones, innovations relating to automobiles directly involved connectivity and changed how the masses travel.[160] The innovations also extended to mass production techniques,[161] as well as efficiencies and styling,[162] so that it became a staple for the twentieth century American family.[163] Particularly in the area of criminal procedure and Fourth Amendment analysis, the automobile has played a large role in twentieth century development of the search and seizures incident to arrest doctrine. Since so many initial contacts and subsequent arrests occur between police and citizens in and relating to automobiles, the doctrine was forced to create structures dealing with what was permissible and what was not within this specific context.

The Supreme Court has created its own case law specific to auto searches addressing topics such as what areas could be searched and what contents within the car could be reached. *Carroll v. United*

---

[155] 244 P.3d 501 (Cal. 2011).

[156] *Id.* at 502.

[157] *Id.* at 502–03 (internal quotation marks omitted).

[158] *Id.*

[159] *Id.*

[160] *See supra* note 20 and accompanying text; *see also Automobiles*, HISTORY (2010), http://www.history.com/topics/automobiles, <http://perma.cc/Y9W4-JRUG> ("The automobile changed the architecture of the typical American dwelling, altered the conception and composition of the urban neighborhood, and freed homemakers from the narrow confines of the home. No other historical force has so revolutionized the way Americans work, live, and play.").

[161] *Id.* ("Committed to large-volume production of the Model T, Ford innovated modern mass production techniques at his new Highland Park, Michigan, plant, which opened in 1910.").

[162] *Id.* (General Motors "innovated planned obsolescence" and introduced a "largely cosmetic annual model change").

[163] *Id.* While the automobile was developed in both Europe and the United States in the late 1800s, the vehicle developed for the *masses* in the United States. *Id.*

States,[164] decided in 1925, was one of the first cases to note the distinction between a search of a house and a search of an automobile for contraband.[165] The Court observed that the Fourth Amendment prohibits only unreasonable searches and that a search of a car, if probable cause exists, could be reasonable even without a warrant.[166]

The special development of case law in the Supreme Court occurred with searches of vehicles incident to arrest, starting with *Belton* and leading to *Gant*. Some suggest that cell phones are a transformative technology akin to automobiles and should be treated similarly.[167] The approach taken by the Supreme Court to automobiles generally—requiring reasonable suspicion to stop and probable cause to search—and to searches incident to the arrest of persons in automobiles, provides a framework for use in the detention and search of cell phones.[168]

Professor Orin Kerr aptly suggests that the Supreme Court adjust its doctrine to changing facts in order to moderate the balance of power between the government and the individual; for that reason, he argues, automobile-specific rules were made to fit existing Fourth Amendment doctrine.[169] Automobiles were transformational not only because they provided a new and upgraded form of transportation, but also because

---

[164] 267 U.S. 132 (1925).

[165] *Id.* at 147.

[166] *Id.* at 149.

[167] While some commentators might object to fact-specific rules under the Fourth Amendment, Professor Orin Kerr has offered a thoughtful rebuttal:

> How can we justify one rule for physical evidence and another rule for digital evidence? I have two answers. The first is that technology-specific rules can be appropriate when technologies create recurring facts. Within Fourth Amendment law, the automobile provides the obvious example. A large chunk of Fourth Amendment doctrine concerns automobile-specific rules. Examples include the automobile exception to the warrant requirement, rules on when automobiles can be stopped, when passengers can be ordered out of the car, and when cars can be searched incident to a driver's arrest. . . . Second, whether technology-specific rules appear natural or awkward depends on [where] along the technology timeline you look.

Kerr, *supra* note 6, at 407.

[168] Professor Kerr provides a provocative and thoughtful comparison:

> In my view, sensible guidance for new rules governing the search of digital storage devices incident to arrest is provided by existing doctrine on searching automobiles in those circumstances. Like cell phones, cars are mobile. And like cell phones, cars can store a great deal of personal information. As the Court recognized in *Arizona v. Gant*, allowing a complete search of a car as a routine matter whenever the driver has been arrested permits a search far beyond the rationales of the exception. Under *Gant*, officers can search the car only in two circumstances: first, "when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search," and second, when "it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle."

Kerr, *supra* note 6, at 406.

[169] Orin S. Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480, 506 (2011) (asserting that *Carroll v. United States*, for example, was "all about equilibrium-adjustment," which he describes as "a judicial response to changing technology and social practice [when] new tools and new practices threaten to expand or contract police power in a significant way.").

they served as advantageous transport tools for criminals, thereby facilitating crime.[170] This was especially true during Prohibition, when cars provided the primary means of transport for illicit alcohol.[171] Consequently, cars lost some of the privacy that had previously enveloped them.[172]

The problem with this approach is that there are important differences between automobiles and cell phones. Cell phones are not used to commit crimes or to transport contraband in as central a manner as automobiles were in the past, although phone calls and text messaging are indeed sometimes used to *facilitate* crimes, such as drug deals.[173] Rather, cell phones are better viewed as multifunctional tools, doing many more things than the automobile, which is still primarily used for transportation purposes. Further, the automobile is a more conventional storage container, with a trunk and glove box specifically designed for the storage of physical things. While the rationale of *Gant* can be readily transferred to cell phone searches incident to a lawful arrest, it does not mean that phones are just like automobiles and should be treated similarly.[174]

E. Analogue #5: Houses

The search of cell phones can be analogized with searches of individual homes in that phones are used to shelter important possessions (information) from the rest of the world, have different rooms or icons, and contain applications and folders with multiple functions. Smartphones are also set up to support the user's daily life, such as locating food, housing, and jobs. In addition, a phone can paint an intimate picture of the phone's owner if an interloper is permitted to rummage through it.[175] A phone may reveal who the owner's associates are, what items are on his calendar, what doctors he is seeing, what medications he is taking, and what social media he is on.

The problem with this analogy is that for all of the similarities to a

---

[170] *Id.* at 503–04.

[171] *Id.* at 504.

[172] *Id.* at 507.

[173] *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 804 (7th Cir. 2012) (illicit drug sale conspiracy); United States v. Barret, 10-CR-809 (S-4) KAM, 2012 WL 171321, at *1 (E.D.N.Y. 2012) (marijuana trafficking conspiracy); United States v. Gomez, 807 F. Supp. 2d 1134, 1139 (S.D. Fla. 2011) (conspiracy to import cocaine).

[174] The Court in *Gant* explained, "circumstances unique to the automobile context justify a search incident to a lawful arrest when it is reasonable to believe that evidence of the offense might be found in the vehicle." 556 U.S. 332, 335 (2009).

[175] Case law suggests that using this analogue would restrict warrantless searches incident to arrest to prevent such privacy encroachments. *See, e.g.*, Payton v. New York, 445 U.S. 573, 590 (1980) ("[T]he Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant."); *see also supra* note 10 and accompanying text.

house, people do not live in their phones and phones are just as likely to be accessed on a crowded plane as in a private location with a closed door. While our "head-down" society shows that people in many ways are completely preoccupied with their phones, phones are not a home-substitute.

V. USING FUNCTION OVER FORM TO EVALUATE FOURTH AMENDMENT SEARCH OF A CELL PHONE INCIDENT TO A LAWFUL ARREST

"[L]aw [is a] . . . distinctive manner of imagining the real."[176]

Factual changes ought to be embraced by the law, particularly the pluralism created by regular technological advances.[177] This pluralism—or multiple realities—can in turn create local structures or frameworks that focus on a specific applicable context, and thereby delineate how people behave based on actual facts.[178] Trying to fit the existence of smartphones into an earlier reality that focuses on form provides for a bad fit and, generally, bad results. The analogues above illustrate how the continued reliance on outdated facts diminishes and eviscerates the parallels. Yet, an alternative protocol exists that embraces local structures.

A. Defining Multifunctionality

Multifunctional evaluation recognizes the need for legal analyses to assess the facts created and distorted by advancing technologies and the new local structures they create. These structures include local cultures, such as video games and their followers, people who use Instagram and Twitter, and those who have online relationships. A legal framework of local structures embraces a "new realities principle." That is, instead of attempting to utilize a unified legal theory such as trespass or proximity, a legal framework using local structure looks at factors, such as: police discretion and intent; the nature, scope, and aggregation of the enhancement of physical perception; and the degree and nature of

---

[176] Clifford Geertz, *Fact and Law in Comparative Perspective*, *in* LOCAL KNOWLEDGE: FURTHER ESSAYS IN INTERPRETIVE ANTHROPOLOGY 167, 173 (3rd ed. 2000) ("[T]he 'law' side of things is not a bounded set of norms, rules, principles, values, or whatever from which jural responses to distilled events can be drawn, but part of a distinctive manner of imagining the real.").

[177] Pluralism is "a theory that there are more than one or more than two kinds of ultimate reality." MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/pluralism, <http://perma.cc/KY34-VGMD>.

[178] As opposed to *universalist* structures, which are based on a one-size-fits-all approach and ignore specific facts.

intrusiveness.

B. Applying a Multifunctional Test

To apply multifunctionality in the context of searches of cell phones incident to lawful arrest, focusing on the various facts associated with the arrest will be important, including: what the police accessed; the type of cell phone; the intent and discretion exercised by the police; and the nature and degree to which the police enhanced their physical perception by accessing the cell phone.

Justice Scalia's description of the bright-line rule for automobile searches incident to lawful arrest mirrors the current debate over cell phone searches:

> [I]n our search for clarity, we have now abandoned our constitutional moorings and floated to a place where the law approves of purely exploratory searches of vehicles during which officers with no definite objective or reason for the search are allowed to rummage around in a car to see what they might find.[179]

Several cases provide a glimpse of how this issue can be aptly handled through the use of a multifunctional evaluation and local structures.

1. Using Existing Precedent as a Foundation

a. *Kyllo v. United States*

Kyllo v. United States[180] was the Court's first advancing technology case on the cusp of the digital age. While the Court appeared ready to confront the reality-changing nature of the infrared technology involved, it was not ready to provide an assessment of how much technology enhancement of perception would render police action a search:

> The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage

[179] Thornton v. United States, 541 U.S. 615, 628 (2004) (Scalia, J., concurring) (quoting United States v. McLaughlin, 170 F.3d 889, 894 (9th Cir. 1999) (Trott, J., concurring) (internal quotation marks omitted)).

[180] 533 U.S. 27 (2001).

> point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found "it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened."[181]

Instead, the Court had a familiar locus to wrap its opinion around—government invasiveness of a house:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use.[182]

The Court recognized the power of advancing technology to create new ways to access the interior of a house, regardless of the lack of physical intrusion of the police.[183] Yet, the Court qualified its admonitions by stating that the determination about whether the information is obtained via a "search" is dependent in part on whether the technology is in "general public use."[184] This qualifier has the potential to marginalize the meaning of privacy as it applies to the *use* of technology to conduct searches and to the search *of* technologies such as smartphones and smart watches, which are already widely used in our society.

b. *California v. Carney*

California v. Carney[185] shows how the Court often handles multifunctionality by shifting to unifunctionality whenever it can. In *Carney*, the Court had to decide whether to treat a recreational vehicle (RV)—"a fully mobile 'motor home'"—as an automobile, a home, or as a combination of the two for purposes of a search.[186] The Court considered the advance in technology as part of its analysis,[187] which is exactly what it should do when technology provides new cultural realities and facts. Ultimately, however, the Court chose to focus on the RV's use as a vehicle specifically in classifying it within the automobile

---

[181] *Id.* at 33 (citation omitted).
[182] *Id.* at 34 (citation omitted).
[183] *Id.* at 34–35 (discussing a "directional microphone" and "satellite capable of scanning from many miles away").
[184] *Id.* at 34.
[185] 471 U.S. 386 (1985).
[186] *Id.* at 387, 393.
[187] *See id.* at 393 ("In our increasingly mobile society, many vehicles used for transportation can be and are being used not only for transportation but for shelter, *i.e.*, as a 'home' or 'residence.'").

category.[188]

Carney may provide an appropriate analogy for courts that choose to treat cell phones as simply telephonic evidence on the arrestee's person.[189] Yet, when carried as multifunctional computers, they ought to be protected as a computer.[190] When used in a criminal enterprise—to call customers in a drug ring, for example—and accompanied by the reasonable suspicion they are being used as such, phones should be subject to search incident to lawful arrest. This analysis is similar to the one the Court used in *Gant*, to allow searches when the police have a reasonable suspicion that evidence relating to the arrest will be recovered in the automobile.[191]

c. *United States v. Cotterman*

United States v. Cotterman[192] offered the Ninth Circuit different ways to approach a border search of electronic equipment.[193] While border searches are generally presumptively reasonable and do not require individualized suspicion of criminal activity,[194] the search of electronic equipment could be swallowed up by the border location or be viewed as creating a different test, with the electronic device triggering a

---

[188] However, the Court seemed to provide an exemption for vehicles not "readily capable" of "being used on the highways," and "found stationary" in a place normally "used for residential purposes—temporary or otherwise." *Id.* at 392.

[189] *Id.* at 393–94. The Court in *Carney* explained, "Our application of the vehicle exception has never turned on *the other uses to which a vehicle might be put*." *Id.* at 394 (emphasis added). Other courts have similarly declined to look at all the capabilities of a cell phone, choosing instead to treat them as devices primarily used to make and receive telephone calls. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 809–10 (7th Cir. 2012) (upholding a search of a cell phone for the limited purpose of obtaining the cell phone number, which was used to subpoena call history records); United States v. Fuentes, 368 F. App'x 95, 99 (11th Cir. 2010) (permitting the search of cell phone's contact list to obtain the name and phone number of a co-conspirator); United States v. Murphy, 552 F.3d 405, 407–08, 412 (4th Cir. 2009) (permitting the initial search of a cell phone to retrieve phone numbers of people who could corroborate the defendant's identity).

[190] *See, e.g.*, State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (drawing an analogy between cell phones and computers—which "are entitled to a higher expectation of privacy"—and holding that because a person has a similarly high expectation of privacy with regards to the contents of a cell phone, a search warrant is required once the cell phone is under the exclusive control of law enforcement).

[191] Arizona v. Gant, 556 U.S. 332, 343 (2009).

[192] 709 F.3d 952 (9th Cir. 2013), *cert. denied*, 134 S. Ct. 899 (2014).

[193] *Id.* at 967 ("International travelers certainly expect that their property will be searched at the border. What they do not expect is that, absent some particularized suspicion, agents will mine every last piece of data on their devices or deprive them of their most personal property.").

[194] *Id.* at 957 ("Although courts have long recognized that border searches constitute a 'historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained,' . . . reasonableness remains the touchstone for a warrantless search. Even at the border, we have rejected an 'anything goes' approach." (quoting United States v. Ramsey, 431 U.S. 606, 621 (1977)). In *Ramsey*, the Court held that international border searches are reasonable "pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." 431 U.S. at 616.

functional analysis.[195]

When Cotterman entered the United States from Mexico, his two laptop computers and digital camera were taken 170 miles away and the contents forensically searched without a warrant; consequently, pornographic pictures of children were found.[196] In a rehearing en banc, the Ninth Circuit found that the warrantless forensic search of Cotterman's electronic devices would have violated his rights under the Fourth Amendment absent "a showing of reasonable suspicion."[197] The court stated, "A person's digital life ought not be hijacked simply by crossing a border" and imposed a reasonable suspicion standard for follow-up searches such as the one that occurred.[198]

The court observed that while a suitcase provided a person with the opportunity to pack a limited amount of belongings, people can now store an extensive amount of their personal information on portable devices like smartphones, laptops, and tablets.[199] Regarding the forensic nature of the search, the court explained, "It is as if a search of a person's suitcase could reveal not only what the bag contained on the current trip, but everything it had ever carried."[200] The court ultimately held that a reasonable suspicion standard for forensic searches protects travelers from a "computer strip search" every time they need to lawfully cross the border.[201] Interestingly, the court found that password protection does not in and of itself give rise to reasonable suspicion, but is relevant in the totality of circumstances analysis.[202]

2. *The Predictability of a Multifunctional Fourth Amendment Analysis*

Given the rapid development of technology, existing precedent provides but a rough guide to future analyses. These analyses, though, can still be predictive and general, while incorporating the understanding that circumstances matter, along with cultural and factual realities. The analyses would simply be based on the existing facts created by the new data sets or technological advances. Judicial evaluations would still be based on essential themes consistent with the text and intent of the Fourth Amendment, namely: (1) the invasiveness, duration, and intent of

---

[195] The *Cotterman* court did, in fact, emphasize that "[i]t is the comprehensive and intrusive nature of a forensic examination—not the location of the examination—that is the key factor triggering the requirement of reasonable suspicion here." 709 F.3d at 962.

[196] *Id.* at 958–59.

[197] *Id.* at 968.

[198] *Id.* at 965–66. The court's analysis rested on the reasonableness of the search, "paying particular heed to the nature of the electronic devices and the attendant expectation of privacy." *Id.* at 964.

[199] *Id.*

[200] *Id.* at 965.

[201] *Id.* at 966, 967–68.

[202] *Id.* at 969.

the government conduct;[203] and (2) the nature, exposure, and impact of the invasion.[204]

The requirement of at least a legitimate and articulable suspicion of criminal wrongdoing to search a cell phone, without any circumstantial suspicion that it would contain evidence relating to the crime, is consistent with *Kyllo*, which, while concerning a house, warned against seemingly innocuous invasions that reveal very personal and private information. This approach is also consistent on a broader scale with the abhorrence of writs of assistance, which are metaphorically viewed as fishing expeditions.[205]

In sum, it is not simply the access to or the aggregation of data by the government that matters, but the way these data sets can be analyzed and then used with no expiration date.[206] Without checks and balances, and a clear distinction between the public and private domains, the private domain will shrink to an incredibly small size.[207]

3. When Searches of Devices Are Justified

Under a multifunctional approach, circumstances will sometimes justify cell phone searches incident to a lawful arrest. For example, stun guns can be disguised as cell phones,[208] and flash mobs are often arranged with the cell phone serving as the organizing lynchpin via text messaging.[209] In addition, criminals can make calls integral to the

---

[203] *See generally* United States v. Chadwick, 433 U.S. 1 (1977) (holding that if seized property is within exclusive control of law enforcement, warrantless search is impermissible), *abrogated on other grounds by* California v. Acevedo, 500 U.S. 565 (1991); Chimel v. California, 395 U.S. 752 (1969) (finding that dual rationales of officer safety and protection of evidence justify search incident to arrest), *abrogated by* Davis v. United States, 131 S. Ct. 2419 (2011); United States v. Burgard, 675 F.3d 1029, 1033 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 183 (2012) (holding that delayed search will impact owner's possessory rights and may be considered impermissible); United States v. Flores-Lopez, 670 F.3d 803 (7th Cir. 2012) (holding that targeted search is permissible trivial invasion); State v. Smith, 920 N.E.2d 949 (Ohio 2009) (holding that if no *Chimel* exigency exists, warrantless search is impermissible).

[204] *See generally* United States v. Jones, 132 S. Ct. 945 (2012) (noting that cell phones contain exceedingly private and personal information); Kyllo v. United States, 533 U.S. 27 (2001) (reiterating that the interior of one's home is a constitutionally protected space); *Cotterman*, 709 F.3d 952 (requiring that reasonable suspicion threshold must be met); Smallwood v. State, 113 So. 3d 724 (Fla. 2013) (finding that search of a cell phone is akin to giving law enforcement a key to one's home, revealing private and personal details).

[205] *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987) (emphasizing that the purpose of the Fourth Amendment's particularity requirement is to limit searches to "the specific areas and things for which there is probable cause to search," thereby ensuring that "the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

[206] *See supra* notes 21, 49 and accompanying text.

[207] *See supra* note 21 and accompanying text.

[208] *See, e.g.*, *Cell Phone Stun Guns*, HOME SECURITY SUPER STORE, http://www.thehomesecuritysuperstore.com/self-defense-stun-guns-cell-phone-stun-guns-sub=39, <http://perma.cc/BQ87-63AE>.

[209] *See* Sunil Bhave, *Warrantless Cell Phone Searches in the Age of Flash Mobs*, 12 CONN. PUB. INT. L.J. 263, 264–65 (2013) (examining the constitutionality of searching the contents of cell phones

commission of a crime using a cell phone. When these and similar situations arise, there is ample justification to search the phone to protect officer safety, to interdict an ongoing crime, or to preserve evidence.

Even if there is reasonable suspicion that the phone was a tool of criminal activity, local structure analysis provides guidance about the scope of subsequent searches. For example, if a cell phone is believed to have been recently used as part of illicit drug sales, reasonable suspicion should allow a search only so far as the suspicion extends. If the suspicion is that the phone was used to text a drug seller or buyer, then only the text component should be accessed. If it is reasonably believed the phone was used to call a co-conspirator, then only the recent phone call numbers should be accessed, not the texts.

VI. CONCLUSION

Cell phones and other multifunctional devices are helping to reshape realities in the twenty-first century. Unlike the physical world of walls and doors, new smart devices are separating form and function. In *Wurie* and *Riley*, the Supreme Court has the opportunity to reshape and update the Fourth Amendment exception for searches incident to a lawful arrest. Even if the *Katz* test of reasonable expectation of privacy survives these cases, it is unavoidable that a cell phone is no longer just a phone, but rather many things wrapped up in one object. It is not simply waxing poetic to say that a cell phone is a portal into its owner's past, present, and future—a big picture window into intimacies, secrets, and yards of information. Consequently, to properly assess searches of cell phones, the Court should apply a multi-pronged analysis that considers function as well as pre-digital form, including factors such as the nature and extent of the invasiveness of the government's actions, the specific articulable purpose of the government's conduct, and the basis for the arrest. While a search incident to a lawful arrest is firmly based on the dual rationales of safeguarding the arresting officer and protecting against the imminent destruction of evidence, searching a cell phone generally does not raise either rationale unless there is a particular basis for believing one of the rationales is implicated. While specific exceptions exist, the cell phone generally should not be analogized to a *Robinson* container, an *Edwards* paint chip, or a *Chimel* possession. Instead, the Supreme Court should take a position that engages the digital age.

---

incident to lawful arrest within the context of flash mobs and positing that these searches are necessary to protect officer safety because cell phone communications can be used to call for an ambush of law enforcement).