RILEY V. CALIFORNIA AND THE STICKINESS PRINCIPLE

STEVEN I. FRIEDLAND†

ABSTRACT

In Fourth Amendment decisions, different concepts, facts and assumptions about reality are often tethered together by vocabulary and fact, creating a 'Stickiness Principle.' In particular, form and function historically were considered indistinguishable, not as separate factors. For example, "containers" carried things, "watches" told time, and "phones" were used to make voice calls. Advancing technology, though, began to fracture this identity and the broader Stickiness Principle.

In June 2014, Riley v. California and its companion case, United States v. Wurie, offered the Supreme Court an opportunity to begin untethering form and function and dismantling the Stickiness Principle. Riley presented the question of whether cell phone searches incident to a lawful arrest were constitutional. The Court, which had clung to pre-digital concepts such as physical trespass well into the twenty-first century, appeared ready to explore how technology is reshaping historically understood conceptions of privacy. From a broader perspective, the case offers an initial step in reconciling pre-digital rules based on outdated spatial conceptions of physical things with the changing realities of a technology driven world.

INTRODUCTION

"Law is a way of reimagining the real."[1] – Cultural Anthropologist Clifford Geertz

A 'stickiness principle' has shaped Fourth Amendment jurisprudence. According to this principle, different concepts, facts and assumptions about reality often adhere to each other. This stickiness is particularly evident in pre-digital court opinions, and often is revealed in the

---

† The author is a Professor of Law and Senior Scholar at Elon University School of Law. He holds a J.D. from Harvard Law School and LL.M and J.S.D. degrees from Columbia University. He wishes to thank Kelly Holder and Helen Chatt for their stellar research and librarian Lisa Watson for her very helpful assistance. The author also thanks the U. Texas J. on Civ. Lib. & Civ. Rts. for the opportunity to explore the subject matter at an earlier time.

[1] CLIFFORD GEERTZ, LOCAL KNOWLEDGE 14 (1983).

vocabulary used to describe items in the physical world,[2] suggesting items had only a single function.[3] For example, the function of sunglasses was to block the sun. Wrist watches were intended to tell time. Cars provided transportation.

Fourth Amendment privacy mostly dwelt within bright-line boundaries, such as those provided by doors and walls. When questions about digital privacy were at issue, the Supreme Court often struck a similar note, sticking to spatial notions of long-established physical world understandings. In the recent case of *United States v. Jones*,[4] for example, Justice Scalia, writing for the majority, viewed a GPS tracker placed by the police on a private car without permission as a trespass, essentially ignoring the functional capacity of the device to track the auto for weeks at a time.[5] *Jones* and other cases served as evidence of the continuing vitality of the Stickiness Principle, not its demise.

Technological advances, however, are threatening the foundation of the stickiness principle through the creation of powerful new realities that expand the functionality of items. Imbuing traditional appliances and items with new functions have reshaped cultures and understandings. As Jony Ive, the Apple designer behind the iMacs and iPod, has noted:

> 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.[6]

This paper argues that the Supreme Court needs to untether form from function in evaluating Fourth Amendment claims and begin to focus more on the expanding functionality. The functionality of a cellphone as a wireless computer, for example, does not generally implicate the rationales justifying a search incident to a lawful arrest. *Riley v. California*,[7] and its

---

[2] Another illustration is the notion that disclosure of information to a third party is generally a complete waiver of privacy regarding that information.

[3] While these items also provided a layer of fashion, in the legal world they were one-dimensional with respect to form and function.

[4] 132 S. Ct. 945 (2012).

[5] *See id.* at 952 (explaining that because the government "trespassorily inserted the information-gathering device" into the vehicle, it may be distinguished from cases in which parties consented to the presence of a tracking device). Trespass protects the property right to exclude others. It is a cause of action that strongly supports the idea of private property.

[6] Marco della Cava, *The Real Face of Apple*, USA TODAY, Sept. 20, 2013, at 1.

[7] 134 S. Ct. 2473 (2014).

companion case, *United States v. Wurie*,[8] offered the Supreme Court precisely this opportunity—to begin separating form and function in order to discern the "reasonableness" of searches.

Riley and *Wurie* involved challenges to warrantless police searches of cell phones incident to lawful arrests. In *Riley* and *Wurie* the Court's decision required it to categorize the cell phone—was it the equivalent of a container, written records, a corded phone, or something else altogether? A unanimous Supreme Court agreed that a warrantless search incident to a lawful arrest of a suspect's cell phone was not constitutionally justified by the search incident to a lawful arrest exception. The Court's decision reflected its view that the container form of the phone did not define or cabin its extraordinary data functions. In doing so, the Court took a big step forward in accepting new realities and the untethering of form and function in a rapidly changing world of technology. Yet the Court could have gone further in this case to destabilize the stickiness principle. In *Riley*, a "smart" phone was at issue.[9] In *Wurie*, there was no data connection on the wireless phone.[10] Both phones were given the same consideration, again indicating the strength of the stickiness principle by implicitly lumping together form and function.[11]

The paper is divided into four sections. After this introduction, the second section provides background on the advancing realities of technology and outlines the *Riley* decision. The third section advances an untethered conception of the Fourth Amendment as an individual right to autonomy, as well as a collective regulatory check on governmental access, gathering, and analysis of information, using functionality as the baseline for what constitute reasonable Fourth Amendment searches. The paper concludes in its fourth section that the separation of form and function leads to a 21st Century understandings of the Amendment.

I. BACKGROUND

A. New Realities[12]

The cultural anthropologist, Clifford Geertz, conceptualized law as "reimaging the real."[13] This formulation captures how privacy operates in modern America, particularly regarding the established rules associated

---

[8] *Id.*
[9] *Id.* at 2477.
[10] *Id.*
[11] *See id.*
[12] An example of a new reality is Rene Magritte's painting of a pipe with the statement, "This is not a pipe" below it. RENE MAGRITTE, THE TREACHERY OF IMAGES (1929).
[13] GEERTZ, *supra* note 1, at 14.

with the Fourth Amendment to the U.S. Constitution. These rules are applied and intertwined with evolving understandings of police techniques and reasonable expectations drawn from changing technological, social and cultural norms.

The idea of privacy as a set of personal secrets, whispered in a corner behind physical walls and doors so no one can listen, is fast becoming a quaint anachronism. Instead, "The world isn't run by weapons anymore, or energy, or money, it's run by little ones and zeroes, little bits of data. It's all just electrons."[14]

Advertisers, private companies and the government engage in widespread data collection at the click (or double-click) of a mouse or screen button, and engage in follow-up analysis on a regular basis, using such tools as cell phone location information, Internet tracking data, camera observations, cookies and drones. These tools provide streams of data that can be aggregated and reassembled to create detailed portraits of people.

1. The Information Society

The data produced by everyday things alone indicates that we live in an information-driven society, where technology has created new threads of connection and observation.[15] The quantity, quality, and ease of information gathering, including surveillance and governmental access, continues to grow exponentially.[16]

The metadata from Internet use, cell phone location data and other sources, including hyper-local observations, are fed into computers for complex analysis and then combined with other surveillance information.[17] This information, even when gathered and utilized outside the private space protected by physical walls and doors, may still present a fairly intimate picture of the subject individuals over time. This creates almost a remote key to what is occurring inside a house or building, as well as outside.[18]

---

[14] SNEAKERS (Universal Pictures 1992).

[15] The need for stacks of boxes or file cabinets has largely disappeared, with the replacements quantified in bytes.

[16] *See, e.g.*, Quentin Hardy, *Big Data's Little Brother*, N.Y. TIMES, Nov. 12, 2013, at B1 ("Collecting data from all sorts of odd places and analyzing it much faster than was possible even a couple of years ago has become one of the hottest areas of the technology industry. . . . Now Big Data is evolving, becoming more "hyper" and including all sorts of sources.").

[17] Indeed, the National Security Agency alone gathers 20 billion "record events" per day. James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sep. 29, 2013, at A1.

[18] This off-the-wall versus through-the-wall distinction was advanced in *Kyllo v. United States*, 533 U.S. 27 (2001), where the Court found that the police

The information society has impacted police investigative techniques. From the physical tracking of twenty years ago, to the stationary cameras and informants that are still tools of the trade today, tomorrow's police "might sit in an office or vehicle as their metal agents methodically search for interesting behavior to record and relay."[19] For example, the federal government has developed and begun to implement the Biometric Optical Surveillance System (BOSS),[20] which will have the capability of identifying individuals from distances[21] of up to 100 meters.[22]

To supplement information acquired directly, the government obtains considerable amounts of information through the data already collected by private companies and the consent of third parties.[23] The downstream access of this information by the police often is invisible to the users who provided it.

2. Cell Phone Reality

Riley v. California was decided not only within this information-society context, but also within a cell phone-centric world. As landline telephones recede into the past, the number of cell phone users continues to

---

unconstitutionally used an infrared heat detection device to determine whether heat lamps were being used in the house to grow marijuana. *Id.* at 40.

[19] M. Ryan Calo, *The Drone as Privacy Catalyst,* 64 STAN. L. REV. ONLINE 29, 32 (2011). Americans can visualize and experience this activity as a physical violation of their privacy.

[20] *Privacy Impact Assessment Update for the Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests*, U.S. DEPARTMENT OF HOMELAND SECURITY, (Dec. 17, 2012), https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_st_stidpboss_dec2012.pdf.

[21] The use of such advanced systems does not always mean they will function effectively. For example, it failed to identify the Boston Marathon bombers despite the fact that both faces were in official databases already. *See* Jason Mick, *Homeland Security's BOSS Project Aims Targets Facial ID of Citizens*, DAILY TECH, http://www.dailytech.com/Homeland+Securitys+BOSS+Project+Aims+Targets+Facial+ID+of+Citizens/article33223.htm (last visited Nov. 25, 2015).

[22] Eddie Keogh, *DHS to Test Facial Recognition Software at Hockey Game*, REUTERS, Sept. 18, 2013, http://rt.com/usa/dhs-hockey-washington-face-033/. This system was scheduled for testing at a public hockey game in the State of Washington in 2013.

[23] Another way the government obtains information is through warrants and requests under the Foreign Intelligence Surveillance Act. 50 U.S.C. §§ 1801-1885 (2010).

grow rapidly around the world.[24] In June 2010, for example, there were 292.8 million cell phone users in the United States alone.[25]

While the cell phone was initially and primarily used to make telephone calls, it has been transformed into a multi-functional tool that is more accurately labeled a pocket super-computer. Specifically, the smart phones have Internet access, through which they can access numerous applications, from scanning bar codes, to getting directions through a GPS system, to keeping appointments in a calendar, and more.[26] The smart phone devices continue to advance, extending their world-wide impact.[27] Of particular significance is their storage capacity; these devices can store and disseminate huge amounts of data, photos, financial records, emails, instant messages, notes and other information.[28]

Among the massive amounts of information that can be stored, the smart phones can hold very personal information for long periods of time,[29] ranging from information relating to personal health, family matters, intimate photos, and critical decisions relating to autonomy (e.g., abortion, illness, doctors, and even personal hygiene).[30] When viewed in the aggregate, including apps, notes, emails, text messages, and a calendar

---

[24] *Smartphone Users Worldwide Will Total 1.75 Billion in 2014*, EMARKETER.COM (Jan. 16, 2014), http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536.

[25] *Id.*

[26] 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 (3d ed. 2011).

[27] Clara Tsao, *Six Ways Mobile Technology Has Transformed the World's Poor*, THE HUFFINGTON POST (Jan. 24, 2014, 6:58 PM), http://www.huffingtonpost.com/clara-tsao/6-ways-mobile-techology-h_b_4054076.html.

[28] *See, e.g.*, Jake Laperruque, *CDT Asks Supreme Court to Bar Warrantless Search of Cell Phones*, CTR. FOR DEMOCRACY & TECH. (Sept. 5, 2013), https://cdt.org/blog/cdt-asks-supreme-court-to-bar-warrantless-search-of-cell-phones/.

[29] *See, e.g.*, Orin Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y. 403 (2013). ("Much of the information stored in a person's cellular phone is deeply personal. The information can include photographs, text messages, e-mails, personal notes, records of visited websites, and many other kinds of personal information.").

[30] *See, e.g.*, State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (explaining 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).

listing all professional and personal appointments, the data stored can create a picture of a person's private world.[31] This picture might be more complete than even that which is known by close friends and business colleagues.

3. Separation of Form and Function

Today's born-digital generation has grown up with mobile cell phones as a rooted part of culture and society; the anachronistic landline has been absent from many households for both economic and surplusage reasons.[32] The mobility and elasticity of information used and stored in cell phones provide other important distinctions from the singular use 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 in-and-out information makes these phones portals, through which information can be aggregated and evaluated by Big Data, computers specially programmed to assess bytes of information.[33] These aggregations are often invisible to the human eye.[34] Thus, phones are no longer merely phones, but important communication centers, data centers, and perhaps most significantly, loci for the digital culture.

If a phone is not just a phone anymore, its multifunctional nature still requires it to be categorized for purposes of the law, especially the Fourth Amendment and searches incident to a lawful arrest. With its breadth of purpose and use, categorization will become increasingly difficult. This is especially true as its Internet and Cloud interconnectivity continue to expand. It is not simply the expanding functionality that obfuscates the phone's nature, but rather its impact on the larger culture and society.[35]

---

[31] *See, e.g.*, Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

[32] Stephen J. Blumberg et al., *Wireless Substitution: State-level Estimates from the National Health Interview Survey, 2012*, 70 NATIONAL HEALTH STATISTICS REPORTS 1 (Dec. 18, 2013), http://www.cdc.gov/nchs/data/nhsr/nhsr070.pdf.

[33] *Big Data*, IBM, http://www.ibm.com/big-data/us/en/ (last visited Nov. 25, 2015).

[34] In fact, the F.B.I. Director, Robert Mueller, recently conceded during Senate Testimony that drones indeed have been used for some "very minimal" domestic surveillance operations. Phil Mattingly, *FBI Uses Drones in Domestic Surveillance*, BLOOMBERG NEWS (June 19, 2013), http://www.bloomberg.com/news/2013-06-19/fbi-uses-drones-in-domestic-sureillance-mueller-says.html.

[35] James Manyika et al., *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy* 2–3 (2013), http://www.mckinsey.com/insights/business_technology/disruptive_technologies (last visited Dec. 27, 2015). These technologies are transformative because they contribute to social change, where new ways of doing things supplant the status

These phones thus can be a data storage container, a broad communication device; or even more broadly construed as a portal or link to information past, present, and future; or, some combination of these and other analogues.[36] In short, a cell phone is a repository of information and activities.

4. Phones In Other Forms: the Internet of Things

The unraveling of the stickiness principle from the separation of form and function can be seen in the development of "smart" multifunctional things.[37] There is now a commercially produced "smart" watch,[38] in which Dick Tracy's cartoon watch is now a reality.[39] The watch tells time, possesses computing functions, and has the capability of making phone calls as well.[40] While it might be worn as a watch, such an item is functionally less a watch than a general inter-connective technology device. "Smart" glasses have been developed as well. For example, Google has created Google Glass, worn like a pair of eyeglasses, but calling it that

---

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.

[36] Weak analogues obfuscate predictable rules, particularly with advancing technology issues.

[37] The Supreme Court eventually will need to address the question of watch and glasses searches, as well as the search of other devices that are part of the Internet of Things—data driven "smart" devices that allow for remote operation and adjustment to context. In this way, the Supreme Court will have to deal less with form than with function.

[38] 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?ref=discovery (last visited Nov. 25, 2015).

[39] The advertisement for a "Pebble" smart watch indicates its versatility:

> Pebble is the first watch built for the 21st century. It's infinitely customizable, with beautiful downloadable watch faces and useful internet-connected apps. Pebble connects to iPhone and Android smart phones using Bluetooth, alerting you with a silent vibration to incoming calls, emails and messages. While designing Pebble, we strove to create a minimalist yet fashionable product that seamlessly blends into everyday life.

PEBBLE, http://getpebble.com (last visited Oct. 2, 2013). The Web Site indicated there were "85,000 users and counting." *Id*.

[40] *See, e.g.*, *Apple Watch*, APPLE, http://www.apple.com/watch/?cid=wwa-us-kwg-watch-com (last visited Nov. 25, 2015).

would be a misnomer, given it is so much more of a multifunctional device than a monochromatic tool. Google Glass can record what the wearer sees, send a message, share what is seen, and produce directions on the glass.[41]

Cell phone technology does not stand still, either. For example, Near-Field Communication (NFC) allows direct cell phone-to-cell phone communication.[42] Other expanding technologies include a Bluetooth health-device protocol that connects a phone to heart monitors and cardio equipment,[43] and smart skin phones that take any digital image and display it across the skin of the phone.[44] There is also a combination phone, laptop tablet and digital camera.[45]

5. Phones and Privacy

The storage of important data requires protection. Phones contain methods for protecting stored data, including the remote tracing or wiping of information, and a 'kill switch' function, although newer methods for wiping are also being developed as well. Newer phones have an activation lock that requires a password for reactivation, and a custom message displayed even after a remote erase.[46] This feature is designed to deter theft

---

[41] *What is Google Glass? All you need to know about the state-of-the-art -wearable tech*, MIRROR.COM, http://www.mirror.co.uk/news/technology-science/technology/what-google-glass-how-look-3513110 (last visited Dec. 27, 2015).

[42] This technology permits cell phones to communicate directly with each other. The phones are held back-to-back and the phones can swap information, such as browser pages. A significant use is to allow one device to read another to make a commercial transaction. Companies such as McDonald's and Walgreens have adopted some NFC-equipped terminals for use with this technology. John Brandon, *8 Groundbreaking Mobile Tech Advancements for 2012*, POPULAR MECHANICS (Jan. 28, 2013), www.popularmechanics.com/technology/gadgets/news/8-groundbreaking-mobile-tech-advancements-for-2012#slide-1.

[43] *See, e.g.*, *Runtastic Heart Rate Combo Monitor,* RUNTASTIC, https://www.runtastic.com/shop/en/runtastic-bluetooth-smart-combo-heart-rate-monitor?utm_source=runtastic.com&utm_medium=link&utm_campaign=shop.runbt1&utm_content=static/show.products_page (last visited Nov. 25, 2015).

[44] Samsung is developing and has sought a patent for this technology, described as a "smart device-skin." *Samsung Patent Intros a Wild Concept for Smart Device-Skins*, SAMSUNG UPDATES, http://samsung-updates.com/news-samsung-patent-intros-a-wild-concept-for-smart-device-skins/ (last visited Nov. 25, 2015)

[45] For example, the Fujitsu Lifebook includes these capabilities. See *Fujitsu Lifebook U904 Review*, TECHRADAR.PRO, http://www.techradar.com/us/reviews/pc-mac/laptops-portable-pcs/laptops-and-netbooks/fujitsu-lifebook-u904-1243320/review.

[46] The iOS9 software offers these features on the iPhone 6s, which has been inherited from earlier versions of the phone and software. *See* Wilson Rothman, *Activation Lock May Be Most Important iOS7*

of the phone for resale.[47] The iPhone 5s and later versions feature a fingerprint-scanning touch identification,[48] although its security value has been questioned because of potential copying and access.[49]

Specific computing functions of the phone have the potential to create huge amounts of data. One example is data related to a phone's location. Cell phone companies routinely track cell phones in order to enhance the signal by pairing the phone with the nearest tower.[50] This tracking provides the phones with the best signal possible. Cell phones can sometimes be tracked within feet of their location, although the efficacy of tracking remains uncertain.[51] The data, known as historical cell phone location information,[52] provides a fairly accurate picture of the movements of the cell phone–and its owner– throughout the day and night. The huge quantities of data that can be stored and accessed from databases provide

---

Feature, TODAY MONEY, (Sept. 18, 2013, 2:31 PM), http://sys03-public.nbcnews.com/today/money/activation-lock-may-be-most-important-ios-7-feature-4B11187477.

[47] *Id*. As several leading prosecutors have noted:

> In the months ahead, it is our hope that Activation Lock will prove to be an effective deterrent to theft, and that the widespread use of this new system will end the victimization of iPhone users, as thieves learn that the devices have no value on the secondary market. We are particularly pleased that—because Activation Lock is a feature associated with Apple's new operating system as opposed to a new device—it will be available to consumers with older phone models who download the free upgrade." Joint Statement by San Francisco District Attorney, George Gascon and New York Attorney General Eric T. Schneiderman. *Id*.

[48] *See, e.g.*, *iPhone 5s Tech Specs*, APPLE, http://www.apple.com/iphone-5s/specs/ (last visited Nov. 25, 2015).

[49] Brandon Griggs, *How Secure is Your iPhone 5S Fingerprint?,* CNN, (Sept. 15, 2014, 9:32 AM), http://www.cnn.com/2013/09/12/tech/mobile/iphone-fingerprint-privacy/.

[50] State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

[51] *See, e.g.*, Donald E. McNeil Jr., *Haiti: Cellphone Tracking Helps Aid Groups Set Up More Effective Aid Distribution, Study Says*, N.Y. TIMES (Sept. 5, 2011), http://www.nytimes.com/2011/09/06/health/06global.html?_r=0; *see also* Justin Fenton, *Police, Privacy Advocates Clash Over Cellphone Tracking*, THE BALTIMORE SUN (Nov. 22, 2014), http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-police-tactic-20141122-story.html#page=1.

[52] *Id*.

new sedimentary layers for historical sleuthing,[53] as well as opportunities to preserve information in perpetuity.[54]

Portable substitutes for towers, such as Stingrays,[55] are utilized to track phones. Stingrays, a form of International Monitor Surveillance Instruments (IMSI), are devices that mimic cell phone towers to collect location data on nearby cell phones.[56] Data from all cell phones within a given range are received, including phones not targeted. Police departments in several states have used IMSI imitator devices in crime interdiction.

B. The Fourth Amendment and *Riley*

1. Fourth Amendment Doctrine

The seminal cases that built current Fourth Amendment doctrine and the Stickiness Principle are based on a tethered view of form and function. The cases mostly occurred in the 20th century and used physical spatial relations as the understandings on which their tests are built.

Katz v. United States[57] continues to provide the baseline test for what constitutes a search under the Fourth Amendment. In the years immediately after its pronouncement, it appeared to offer a progressive test, one not rooted in the physical walls and doors of the prior century. It seemed to sync nicely with the digital era, prohibiting electronic surveillance in a phone booth without consent because that would violate subjective and objective expectations of privacy. Yet, as forward looking as it was, the case still revolved around the physical walls of the now abandoned phone booth, which still offered a bright line and visible barrier of privacy for all others to see. The Court's use of physical notice has been stuck to search issues for decades, remaining in alignment with the Stickiness Principle.

---

[53] The data are equivalent to sedimentary layers of rock, although developing at lightning speed in a more visible fashion.

[54] A person can blast information worldwide almost instantaneously, with the power to change reputations, elections and even governments. The data created can create a trail for others, years and decades later, to follow and refresh.

[55] Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, ABC NEWS 10 (Mar. 6, 2014), http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spying-technology-used-throughout-northern-california/6144949/.

[56] Stingrays track phones within a given range, and obtain information about phones not targeted. Government investigators, including the FBI, have been using stingrays since the 1990s. *See* Declan McCullagh, *FBI Prepares to Defend 'Stingray' Cell Phone Tracking*, CNET NEWS (March 27, 2013), http://news.cnet.com/8301-13578_3-57576690-38/fbi-prepares-to-defend-stingray-cell-phone-tracking/.

[57] 389 U.S. 347 (1967).

The search incident to a lawful arrest exception to the warrant preference owes its existence to *Chimel v. California*.[58] This particular exception allows police to search a person and the area within the person's wingspan contemporaneously with a lawful arrest. Significantly, the search can take place without a warrant or any particularized suspicion. There are two rationales for this exception: one, the potential for the imminent destruction of evidence; and two, the safety of the arresting officer. These rationales justified searches and seizures of contraband as a supplement to the lawful arrest.

The case of *United States v. Jones*[59] offered the Court an opportunity to directly deal with advancing technology and adapt the *Katz* test to newer technologies. Instead, the Court retreated, utilizing a long-standing physical trespass test from the case of *Olmstead v. United States*[60] to provide the foundation for the ruling. Justice Scalia looked at the placing of the GPS device on the defendant's car by the police without permission and outside the time-frame authorized by a warrant as an unreasonable search. *Olmstead* provided some bright lines and therefore some appealing clarity with its trespass test. The test was associated with longstanding prohibitions derived from eighteenth century trespass law. In *Olmstead's* time, trespasses were visible and understandable within the confluence of the physical boundaries of land and common sense.

Not all of the justices in *United States v. Jones* subscribed to the physical trespass approach used by Justice Scalia, however. Justices Alito and Sotomayor, in their concurrences in *Jones*, observed that at some point electronic surveillance could violate the Fourth Amendment even when tracking in a sustained manner in a public place and without a physical invasion.[61] Pursuant to a "mosaic theory," a privacy violation does not require a physical trespass and might occur from the aggregation of public information.

2. Riley *and* Wurie

Riley[62] builds on well-established precedent to confront remote GPS technology as a case of first impression for the U.S. Supreme Court. In *Riley*, several men standing near Riley's car shot at the car of a rival gang

---

[58] 395 U.S. 752 (1969).

[59] 132 S. Ct. 945 (2012). The case involved the placement of a GPS device on a private individual's car. *Id.* at 948 (majority opinion). Writing for the majority, Justice Scalia found that the installation of the device was a search within the meaning of the Fourth Amendment. *Id.* at 952.

[60] 277 U.S. 438 (1928).

[61] 132 S. Ct. at 956 (2012) (Sotomayor, J., concurring); *id.* at 961 (Alito, J., concurring).

[62] Riley v. California, 134 S. Ct. 2473 (2014).

member. Riley was implicated as one of the shooters.[63] Subsequently, Riley was driving in San Diego, California, where he was stopped for having an expired tag on his car. Riley also was driving with a suspended driver's license. Consequently, Riley was arrested and his car was impounded.[64] An inventory search of the car yielded several loaded handguns that were linked to a prior shooting. Riley was charged with the possession of the handguns.[65]

An officer searched Riley and seized his smartphone from one of his pants pockets. Information accessed by the officer on the phone linked Mr. Riley to gang activity.[66] A different officer who was seeking additional information about gang activity accessed Riley's phone again two hours later. The officer looked at videos captured on the phone and at a picture of Riley in front of a car that had been involved in an earlier shooting.[67]

The appellate court hearing the appeal in Riley's case 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."[68] Because the Court found it was immediately associated with his person, that triggered the search incident to arrest exception regardless of "whether or not an exigency still existed."[69]

In *United States v. Wurie*,[70] *Riley's* companion case before the U.S. Supreme Court, the defendant, Brima Wurie, was arrested for selling drugs and then was taken to the police station, where two cell phones and keys were found on him. On one cell phone, there was an external caller ID screen that flipped open.[71] The phone was not a "smart phone," meaning it did not have Internet connectivity and mini-computer capabilities.[72] The police observed the phone repeatedly receive calls from what appeared on the external screen as a caller labeled "my house."[73] The officers opened

---

[63] *Id*. at 2480.
[64] *Id.*
[65] *Id.*
[66] Specifically, the officer found some words either in the contacts list or text messages that were preceded by the letters 'CK," which apparently meant "Crip Killers," a term used by members of the Bloods gang. *Id*.
[67] *Id*. at 2481.
[68] *Id*. (citing People v. Diaz, 244 P.3d 501, 505 (2011)).
[69] *Id*.
[70] 728 F.3d 1 (1st Cir. 2013).
[71] *Id.* at 2.
[72] The limited nature of the cell phone under consideration perhaps could be important in a case to reach the Supreme Court, since these phones would not have the same level of connectivity, informational storage capacity, or technological capacity.
[73] *Id.*

the phone and saw on the wallpaper a picture of a woman and a child.[74] The officers pressed a button to access the phone's call log in order to see who had just called.[75] The officers typed the phone number into the white pages phone directory and obtained an address for the telephone number. The address happened to be near where the defendant had parked his car.[76] The defendant moved to suppress the evidence resulting from the search of the cell phone. Judge Stahl focused on whether exigent circumstances existed to justify the search.[77] Given the lack of such circumstances, the Court of Appeals reversed the denial of Wurie's motion to suppress and vacated his conviction.[78]

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.[79]

Significantly, the Court viewed the cell phone as a specialized computer,[80] noting the immense storage capacity of Apple's iPhone 5 was equivalent to four million pages of Microsoft Word documents.[81]

---

[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id*. at 13.
[78] *Id.* at 14.
[79] *Id.* at 8.
[80] *Id.* at 8. The Court conceded that the Supreme Court has not distinguished between the types of items found in such searches or "its capacity to store private information" as a litmus test for legitimacy, but said the search of cellular phone devices are qualitatively different:

> In our view, however, what distinguishes a warrantless search of the data within a modern cell phone from the inspection of an arrestee's cigarette pack or the examination of his clothing is not just the nature of the item searched, but the nature and scope of the *search itself*. *Id.* at 9.

[81] The Court stated, "Apple's iPhone 5 comes with up to sixty-four gigabytes of storage, which is enough to hold about 'four million pages of Microsoft Word documents.'" *Id*. at 8; *See* Apple, iPhone, Tech Specs, http://www.apple.com/iphone/specs.html (last visited May 16, 2013).

The Court also referred to the origins of the Fourth Amendment and the use of general warrants 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 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.[82]

The critical issue before the Supreme Court was whether the police actions regarding petitioner's cell phone constituted an unreasonable search.[83] Under the Fourth Amendment, some reasonable searches are permitted without a warrant, including the search incident to a lawful arrest. In both *Riley* and *Wurie* the officers engaged in a search.[84] The only issue was whether the searches were reasonable, falling within the incident to arrest exception. The Court found that examining the data contained within a cell phone without permission is an apt illustration of an invasion of privacy society would recognize as unreasonable.[85] Further, people would subjectively expect their cell phones to be private as well.

The unanimity of the ruling of the Supreme Court provides several important inferences. First, the Court comfortably applied the rationales and parameters of the search incident to arrest exception—whether the search was needed to prevent the imminent destruction of evidence or to protect the officers' safety. This analysis reflected the prevailing law and viewed the Fourth Amendment as a regulatory limit on government investigation into criminal activity. Second, the Court had the clarity of experience in describing and analogizing the realm of the cell phone. The justices understood its power and its distinctiveness, especially from other "containers." The Court was able to utilize appropriate metaphors and analogues, the phone as a supercomputer, precisely because it separated form and function. This was in stark contrast to *Jones*, which stuck to the safe, bright lines of physical trespass and did not look to the functionality and intrusiveness of GPS tracking.

---

[82] *Id.* at 9 (citing Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence,* 50 SANTA CLARA L. REV. 183, 211 (2010)).
[83] Riley, 134 S. Ct. at 2482.
[84] Under *Katz v. United States*, a search occurs if the government violates both a subjective and reasonable expectation of privacy. *See* 389 U.S. 347 (1967).
[85] *Id.*

The capacities of the cell phone[86] also offered the specter of indiscriminate searches reminiscent of the general warrants of the British colonial era.[87] This specter, once the cell phone was seen as a portal into the intimate details of a person's life, permitted the justices to line up behind limitations on potential police fishing expeditions occurring within the programs of a single phone.

II. MOVING AWAY FROM THE STICKINESS PRINCIPLE: THE SIGNIFICANCE OF UNTETHERING FORM AND FUNCTION

Riley v. California shows that technology can fit within existing legal parameters, but that those parameters have to adapt to new realities. Even if *Katz* remains the prevailing test, what counts as a "reasonable expectation of privacy"[88] will necessarily change with the untethering of form and function. The expansive functionality of cell phones can be seen as generally failing to implicate either of the dual rationales of the search incident to arrest exception. In essence, tests for warrant exceptions primarily based on functionality—not form—are critical in negotiating these new realities.

A. Why Untethering Is Important

The use of functionality will illuminate the dual nature of the Fourth Amendment. First, it allows the Fourth Amendment to retain its understanding as a "zone of privacy" prohibiting unwarranted government penetration. Second, if government intrusion is warranted, it creates within the Fourth Amendment a regulatory limit on governmental access, collection, storage and analysis of information relating to digital privacy.[89]

If functionality prevails, it is then easier to observe that privacy today is not confined to physical spaces, but is portable.[90] If so, the idea of presumptive government access to information, just because it somehow

---

[86] The cell phone as a super computer indicates its expansive capacity as a gathering, storage and analysis device.

[87] The existence of general warrants in Britain and colonial America was one of the central motivations behind the adoption of the Fourth Amendment.

[88] *See* Katz, 389 U.S. at 347 (1967).

[89] This dual nature of the Fourth Amendment is much like the dual nature of "Shimmer" from the old Saturday Night Live sketch—Shimmer was both a floor wax and a dessert topping. *Saturday Night Live* (NBC television broadcast Jan. 10, 1976).

[90] The portability is aided by new technologies and the changed focus of relationships occurring over devices more and face-to-face less.

becomes public, ignores the new realities and cultures of advancing technology.

B. The Intersubjectivity of Objectively Reasonable Expectations of Privacy

What is "objectively reasonable" depends on the lens through which one looks. Describing the Katz test as "a reasonable expectation of privacy" only starts the analysis of what is reasonable. If reasonableness views human behavior as interdependent and contextualized, then an intersubjective conceptualization will inform what is reasonable in light of advancing technology. American judicial decision-making culture, for example, can depend on different kinds of facts, such as background facts and other environmental information, to weave together a tapestry of what is reasonable, one that adapts to the times. According to one commentator, "The particularities of any one subject—his or her desires, preferences, abilities, fears—are inextricably intertwined with those of the beings encountered throughout the subject's ongoing development."[91] Just like judicial decisions are build on precedent, objectivity is built on context and culture, leading to new realities.

These new realities create a modified set of understandings about reasonableness, which are by necessity contextual.[92] The digital era has created new cultures—and new forms of information, tilting societies in ways never experienced in the past.[93]

Thus, *Riley* might be a product of the Court's culture as well as that of the digital age. The decision perhaps could very well be attributed in some small way to the justices' own comfort with cell phones and their own usage. Specifically, the Justices all have access to or own cell phones.[94] If this change in culture has provided a subtle but clear influence, as the "Gamer"[95] reality becomes more prevalent, the Justices will become more

---

[91] *Id.* at 128.

[92] This contextuality depends upon the facts of the case and the totality of the circumstances, much like *Illinois v. Gates*. The socio-cultural underpinnings of the facts, though, matter as well. Illinois v. Gates, 462 U.S. 213 (1983).

[93] Even Justice Roberts recognized in the decision that much of the information generated and stored in cell phones did not exist before the digital age.

[94] *See* Nina Totenberg, *Rare Unanimity in Supreme Court Term, With Plenty of Fireworks*, NPR (July 6, 2014), http://www.npr.org/2014/07/06/329235293/rare-unanimity-in-supreme-court-term-with-plenty-of-fireworks ("They all have cellphones, so they really understood this," says Clinton administration acting Solicitor General Walter Dellinger. "This is one area where they could be said to have empathy").

[95] The "gamer" generation depicts those playing or comfortable with video games, generally using advanced digital technology.

immersed in new realities that create gigabytes of information—information that will become central to challenges under the Fourth Amendment. The tech cultures that have moved into society's mainstream will become important in how future cases are decided.

Yet, the *Riley* decision also reflects the limitations of the Court. While the Court recognized the functionality of a cell phone, it did not take the opportunity to distinguish different levels of functionality in smart phones and non-smart phones. Although many people could explain offhand the differences in features and functioning of different phones, the Court returned in this sense to the Stickiness Principle, merging form and function. Further, the Court did not explore the cultural implications of a cell phone search decision, implicating inter-subjectivity, particularly when the justices have not incorporated other subcultures and experiences into their own lives. Some commentators have compared this case to warrantless street searches for drugs and found that the reasoning provided a class disparity. That disparity involved what appeared to be diminished protection for those from a lower socioeconomic strata who might carry drugs on the street. One commentator noted, "I think the class dimension of this is pretty obvious."[96]

C. The Waiver of Rights

While *Riley* can be seen as a good start for incorporating digital realities into Fourth Amendment analysis, it is simply a relatively safe start. It is safe because the pervasiveness of the cell phone makes it a technology that transcends cultures and technological boundaries. The growing interfaces between the physical and digital privacy world are still governed by several antiquated cases decided in the bricks and mortar era of the Twentieth Century. For example, in *Smith v. Maryland*,[97] the Court decided that pen registers on telephones did not implicate the Fourth Amendment because the metadata of telephone numbers were voluntarily disclosed to third parties, and not the content of the calls.[98] Similarly, in *United States v. Miller*,[99] the Court found that information disclosed to banks was not subject to a Fourth Amendment search analysis because it was voluntarily disclosed to third parties.[100]

These cases have given rise to an all or nothing approach with respect to disclosures of information and privacy. The old realities that form the basis of these cases need updating, especially when the digital

---

[96] *See* Gates, *supra* note 94.
[97] 442 U.S. 735 (1979).
[98] *Id.* at 745.
[99] 425 U.S. 435 (1976).
[100] *Id*. at 442–43.

culture would auger for a more nuanced approach to the waiver of rights that further recognizes the separation of function and form in the digital world.

IV. CONCLUSION

Riley v. California and *United States v. Wurie* provided the Supreme Court with the opportunity to set a new 21st century benchmark for searches incident to a lawful arrest. For the first time since *Kyllo v. United States,*[101] the Court considered the implications of the advancing technology.[102] The case recognizes that form should not automatically win out over function when police are dealing with an arrestee's container-like super-computer, the cell phone. The dual rationales for search incident to lawful arrest, a search for dangerous weapons or evidence that could be imminently destroyed, are not generally implicated by cell phone searches. Thus, functionality should prevail over form. The separation of form and function is occurring more and more often in the digital era and functionality is proving to be the preferable guidepost for analysis.

While *Riley* is a good first step toward incorporating the digital era into the Court's decisional calculus, it is only a first step and an easy one at that. As the multi-functionality of devices continues to expand, the Court needs to include and further reflect on the new realities brought about by advances in technology to reconcile pre-digital Fourth Amendment jurisprudence with the 21st century. Otherwise, we will keep returning to the stickiness principle, where form and function are tethered together in a limiting fashion.

---

[101] Kyllo v. United States, 533 U.S. 27 (2001).
[102] *Id*.