Cellphone Searches After Riley v. California

Will This Landmark Decision Transform Hallowed Fourth and Fifth Amendment Constitutional Law?

By Gregory J. Rolen and Colin T. Murphy

SUMMARY

In a seminal decision, the U.S. Supreme Court held in *Riley v. California* and *United States v. Wurie* that police need a warrant justified by probable cause to search a cellphone seized incident to lawful arrest. However, the legal implications of this case go far beyond criminal procedure. This decision not only challenges the assumptions that underlie the Fourth Amendment "reasonable suspicion" standard for searches on public school campuses, but also the Fifth Amendment issue of forced decryption of cellphone passwords. As technological advances gradually render what was once private as now public, the U.S. Supreme Court will be forced to confront the realities of how technology impacts our daily lives. The *Riley* decision likely will change the way school administrators maintain safety and order on campuses as well as the way we protect our personal privacy.

Gregory J. Rolen, partner, is a member of the public entity, employment and labor, transportation law, and appellate practice groups of Haight Brown & Bonesteel. Mr. Rolen has over 25 years of legal experience serving as the general counsel of a large suburban school district, education law attorney, deputy attorney general, and deputy district attorney. Mr. Rolen is a recognized statewide expert in the Brown Act, Public Records Act, and board governance.

Prior to joining Haight, Mr. Rolen was a state assembly candidate, substance abuse advisory board chairman, JPA board member, DARE speaker, moot court judge, youth football coach, and intercollegiate athlete.

Colin T. Murphy, associate, is a member of the professional liability, risk management and insurance law, and construction law practice groups of Haight Brown & Bonesteel. His experience includes litigation, case evaluation, legal research, discovery, preparing dispositive motions, effective legal negotiation and settlement, counseling clients, and trial preparation.

Prior to joining Haight in 2012 as a law clerk, Mr. Murphy held an internship in the claims department at American Specialty Insurance and played for the San Francisco Seagulls semi-professional baseball team. He presently volunteers his time helping student athletes obtain baseball scholarships from high school and junior college to four-year universities.

On June 25, 2014, the U.S. Supreme Court engaged in what some believe to be an unprecedented act of judicial courage and pragmatism, while others see it as the road to perdition. In April 2014, the justices heard two cases, *Riley v. California*[1] and *United States v. Wurie,*[2] involving the extent to which police can search cellphones obtained incident to lawful arrest. The cases addressed the reasonableness of cellphone searches and whether the increasing capabilities and proliferation of smartphone technology will impact the Fourth Amendment. The court issued a single unanimous decision holding that police need a warrant justified by probable cause to search the cellphones of people they arrest.[3] In so doing, the court paved the way to revisit the venerated "reasonable suspicion" standard articulated in the 1985 case *New Jersey v. TLO.*[4] Based on its rationale, this decision will have a swift and dramatic impact on America's public schools.

A Bold Decision for the Digital Age

Although the Supreme Court has danced around the peripheries of the issue for some time, it could no longer avoid a direct confrontation between technology and privacy. During oral arguments, the court acknowledged the dangers of crafting constitutional laws based on evolving technology. The court prefers universally applicable rules. Justice Anthony M. Kennedy proclaimed that what the court was seeking was "some standard on where we draw the line."[5] However, even Justice Antonin Scalia, arguably the most strict constructionist on the court, recognized, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[6] As such, the court was forced to interpret how Thomas Jefferson and John Hancock might feel about Twitter and Instagram.

Government attorneys argued that long-standing precedent, including *Chimel v. California*,[7] allowed officers to search a person without a warrant "incident to arrest."[8]

[1] *Riley v. California*, 134 S. Ct. 2473 (2014).
[2] *United States v. Wurie*, 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom. Riley*, 134 S. Ct. 2473.
[3] *Riley*, 134 S. Ct. 2473.
[4] *New Jersey v. T.L.O.*, 469 U.S. 325 (1985).
[5] Lyle Denniston, *Argument Analysis: Limiting a Search? Sure, but How?,* SCOTUSblog (Apr. 29, 2014, 2:47 PM), http://www.scotusblog.com/2014/04/argument-analysis-limiting-a-search-sure-but-how/.
[6] *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) (discussing government use of thermal imaging in the context of Fourth Amendment right against unreasonable government search and seizure).
[7] *Chimel v. California*, 395 U.S. 752 (1969).
[8] Transcript of Oral Argument at 33:1-12, *Riley v. California*, 134 S. Ct. 2473 (2014) (No. 13-132), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/13-132_h315.pdf.

They argued that a cellphone is no different than a wallet, address book, personal papers, or other items that have been subject to examination by police if found on an individual who is lawfully arrested.[9] By contrast, opposing counsel argued that cellphones are analytically and qualitatively distinguishable not only because of their ubiquity, but also due to the vast amount of data capable of being stored on such a device.[10] Accordingly, they are more analogous to personal effects in a locked desk, office, or safe.[11] This allowed privacy advocates to argue a direct correlation to the plain wording of the Fourth Amendment, which protects "[t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[12]

Government attorneys were faced with an uphill battle because of a growing line of cases examining the increased expectation of privacy for cellphones. The Ohio Supreme Court held the search of a lawfully arrested person's cellphone as unreasonable due to the device's unique characteristics.[13] The U.S. District Court for the Northern District of California held that cellphones carry a higher expectation of privacy because of the vast amounts of private information capable of being stored on them.[14] Lastly, in *United States v. Burgess*, the court reflected *in dicta* that cellphones could deserve a preferred status due to "their unique ability to hold vast amounts of diverse personal information."[15] Consequently, prior to the court's opinion, there already was a judicial trend toward giving a person's cellphone preferred privacy protection.

Chief Justice John Roberts, writing for the court, wholeheartedly adopted the lower courts' reasoning. Simply put, cellphones are now treated differently than other items carried on an arrested individual. Roberts addressed the issue of cellphone ubiquity with humor in writing that cellphones are "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[16] Roberts was more direct in addressing the potential privacy intrusion. He explained that the multiple functions of the cellphone—such as camera, video recorder, address book, calendar, library, diary, newspaper, and Internet access—give them the distinct characteristic of having an immense amount of information in a centralized location.[17] In fact, he wrote that searching a cellphone could provide more information about your life than searching your home.[18]

Finally, Roberts added some constitutional context to the technological rationale by what can best be described as a "tip of the hat" to the Founding Fathers in quoting a statement by John Adams about the colonists' hatred of generalized warrants that led to the Fourth Amendment and, ultimately, the creation of a new nation.[19] The decision was an uncompromising proclamation that there are increased privacy protections for cellphones.

The Impact on Virtually All Aspects of American Life, None More Than Public Schools

The decision can be fairly read to stand for the proposition that computer searches are different from physical searches. This likely will change the law pertaining to laptop searches, cloud searches, and whether the collection and inspection of aggregated data constitutes a search under certain circumstances. But the most immediate impact will be experienced in America's public schools.

The Supreme Court's rationale, its uncharacteristic unanimity, and the unequivocal language will inevitably alter Fourth Amendment standards related to cellphones in public schools. In 1985, when the court decided *TLO*, cellphones were a luxury and quite rare in schools. Living in the now bygone era of backpacks, purses, and other tangible personal items, the court determined that students had a reduced expectation of privacy at school. Now, approximately 90 percent of all Americans own cellphones,[20] many with the capability of storing more data than the Library of Congress. The pervasiveness of cellphones in schools[21] and the Supreme Court's recognition of the increased expectation of privacy for cellphones demand not only a reevaluation of the *TLO* reasonable suspicion standard, but also preparation for how to maintain safe school environments within a new paradigm.

In *TLO*, the court balanced the students' reasonable expectation of privacy against the necessity of maintaining order at school.[22] With these competing interests in mind, the court abrogated the traditional probable cause standard for a lessened reasonable suspicion standard.[23] The court established a multipronged test for school officials' searches of students.[24] First, the search must be "justified at its inception," meaning that the official needs reasonable grounds for suspecting the search will reveal evidence of a violation of school rules or criminal conduct.[25] Second, the search must be "reasonably related in scope to the circumstances which justified the interference."[26] Finally, the search must not be "excessively intrusive in light of the age and sex of the student and the nature of the infraction."[27] In light of the *Riley* decision, each prong of the test now becomes particularly problematic.

It must be noted that the puzzling question of cellphone privacy has gone through a similar evolution in school law as it has in criminal law. Emboldened by the abridged Fourth

[9] *Id.* at 38:12-18.
[10] *Id*. at 9:25-10:7.
[11] *Id*. at 3:10-20.
[12] *See Id*.; U.S. Const. amend. IV.
[13] *State v. Smith*, 124 Ohio St. 3d 163, 2009-Ohio-6426, 920 N.E.2d 949.
[14] *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007).
[15] *United States v. Burgess*, 576 F.3d 1078, 1090 (10th Cir. 2009).
[16] *Riley v. California*, 134 S. Ct. 2473, 2484 (2014).
[17] *Id*. at 2490.
[18] *Id*. at 2491.
[19] *Id*. at 2494.
[20] Lee Rainine, *Cell Phone Ownership Hits 91% of Adults,* Pew Research Center (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.
[21] Mary Madden, et al., *Teens and Technology 2013*, Pew Research Center (Mar. 13, 2013), http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_TeensandTechnology2013.pdf.
[22] *New Jersey v. T.L.O*., 469 U.S. 235,at 326.
[23] *Id*. at 353 (Powell & O'Connor, JJ. concurring).
[24] *Id*. at 341.
[25] *Id*. at 341-42 (quoting *Terry v. Ohio*, 392 U.S. 1, 20 (1968) (internal quotation mark omitted).
[26] *Id*. at 342 (quoting *Terry*, 392 U.S. at 20).
[27] *Id*.

Amendment protections in the past, schools responded to the very real phenomena of gang violence, drug abuse, and cyberbullying by adopting policies that increasingly encroached on students' personal privacy. However, in *G.C. v. Owensboro Public Schools,* the court held that an assistant principal did not have reasonable suspicion to search the cellphone of a student caught texting in class.[28] The court wrote, "Using a cellphone on school grounds does not automatically trigger an essentially unlimited right enabling a school official to search any content stored on the phone that is not related either substantively or temporally to the infraction."[29] On Feb. 26, 2014, in *State v. Granville*, a Texas appellate court ruled in favor of a student who was convicted based on evidence found by a school resource officer who heard that the student had taken an unauthorized photo of another classmate in a bathroom.[30] The court stated, "Searching a person's cellphone is like searching his home desk, computer, bank vault, and medicine cabinet all at once."[31] Much like in the criminal law context, courts are beginning to recognize an increased expectation of privacy for students' cellphones, which may set the stage to overturn *TLO*.

The TLO Balancing Test Has Suddenly Become Obsolete for Cellphone Searches

By articulating an elevated expectation of privacy for cellphones, the Supreme Court completely eviscerates the basic assumptions underlying *TLO*. First, *TLO* addressed tangible items such as a purse, handbag, or locker. Justice White even gave examples of highly personal items such as letters, diaries, and "the necessaries of personal hygiene and grooming."[32] Cellphones can no longer be considered analogous to tangible items. Cellphones have a storage capacity that dwarfs the purses or handbags of the mid-'80s. They can contain voluminous personal information about an individual's medical history, finances, sexual orientation, political affiliations, and family issues. When the Burger Court crafted a limited expectation of privacy in tangible items, it could not have comprehended the immense amount of information students would be able to carry with them. Consequently, the court carved out a lessened reasonable suspicion standard that provided school officials access to considerably less personal and private information than they otherwise would have access to today through a student's cellphone.

The court's second assumption was that school officials reasonably could limit their searches to tangible locations related to the initial justification for the search. The ever-increasing capabilities of cellphones make it nearly impossible for school officials to reasonably limit their searches. In 1985, a conscientious school official may have been able to sift through students' belongings and intentionally limit their searches. The Supreme Court now recognizes that assumption as untenable. Reasonable suspicion conceivably can justify a search into any application including, but not limited to, social media, text messages, instant messages, telephone numbers, address books, calendars, and search histories. Combined with typical school officials' relative lack of sophistication in navigating new electronic devices, this capacity could transform a limited search into a "fishing expedition."

Finally, social norms and the manner in which students now use cellphones make it exceedingly more difficult to adhere to the often ignored element of the *TLO* test—that the search must not be "excessively intrusive in light of the age and sex of the student and the nature of the infraction."[33] In 1985, the court added this limitation to avoid unreasonable searches that may shock the conscience. For example, in *Safford Unified School District v. Redding*, the court ruled that the district's strip-search of a student to find over-the-counter pain medication violated the Fourth Amendment.[34] Today, students' cellphones carry much more personal and sensitive material than the tangible items of the past. Cellphones are now capable of storing high-resolution photos and audio and video files. They can contain information about personal proclivities, interests, and habits. Moreover, students' cellphones are now an indispensable instrument of romance. Not only are intimate conversations retained on cellphones, but also students frequently engage in "sexting."

Some of these practices necessarily involve the transmission of sexually charged photographs. In 2008, 19 percent of teenagers had sent a nude or seminude image via text message or email, and 31 percent had received such an image.[35] More shockingly, 29 percent reported that they have sexted an image shared with them knowing the material was private.[36] As such, maintaining intimate photographs or conversations either on a cellphone or in a social media account retained on the cellphone is now commonplace. Therefore, even the most well-intentioned official easily could happen upon photographs or information that would render the intrusion into the cellphone shocking to the conscience.

The Decision Will Beget Greater Privacy Protections for Students

The question will become how to protect student privacy rights and at the same time protect student safety. Although it will initially be seen by some as sacrilege, the only feasible alternative is to institute the probable cause standard for cellphone searches. It is not a giant leap from the amorphous reasonable suspicion standard to the more disciplined probable cause standard. They are similar notions on the spectrum of reasonableness. Whereas reasonable suspicion requires grounds to believe that there has been a violation of rules or law, probable cause requires specific articulable facts and circumstances based on reasonably trustworthy information that the cellphone contains evidence of a violation of rules or law.[37] It requires more than a hunch and less than proof beyond a reasonable doubt.

Furthermore, requiring an official to articulate specific

[28] *G.C. v. Owensboro Pub. Sch*., 711 F.3d 623, 626 (6th Cir. 2013).
[29] *Id*. at 633.
[30] *State v. Granville*, 423 S.W.3d 399, 402 (Tex. Crim. App. 2014).
[31] *Id*. at 415.
[32] *T.L.O.*, 469 U.S. at 339.
[33] *Id.* at 342.
[34] *Safford Unified Sch. Dist. v. Redding*, 557 U.S. 364 (2009).
[35] *Sex and Tech: Results from a Survey of Teens and Young Adults*, Nat'l Campaign 11 (Dec. 2008), http://thenationalcampaign.org/sites/default/files/resource-primary-download/sex_and_tech_summary.pdf.
[36] *Id*.
[37] *See generally Terry v. Ohio*, 392 U.S. 1 (1968).*Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

facts to justify the search necessarily would limit the search's scope. For example, if a student reports that a classmate is distributing compromising photographs throughout the school, it would justify a limited search of the photos maintained on the classmate's cellphone. However, it would not justify the search of another student's cellphone the administrator only believes to be involved. School officials still would be able to address the safety concerns; however, it would involve more deference to student privacy.

This adjustment clearly will require training and reeducation. It must be understood that school officials are not police officers; they presumably went into the education field to teach. Few, if any, chose education to become pseudo law enforcement officers. However, schools historically have adjusted to societal changes. School officials have had to deal with social phenomena such as war, bussing, desegregation, gender equity, and bilingual education. This is no difference. It simply requires school officials to practice what they preach to their students, maintaining a commitment to learning, growing, and becoming more complete citizens.

Password Protection Adds a Layer of Constitutional Complexity for Law Enforcement and Schools

The court now has opined unequivocally that law enforcement must have a warrant substantiated by probable cause to search a cellphone. This begets the question, how will police agencies and school officials access a password-protected cellphone? Law enforcement agencies and school officials have very different responsibilities and practicalities; however, in all likelihood, they will be subject to the same constitutional analysis. Although the *Riley* court was unable to address the issue of forced decryption, it did provide considerable guidance to the lower courts concerning how to address this critical and foreboding issue.

The *Riley* court balanced privacy concerns against the government's need to obtain evidence. Roberts recognized that, because cellphones basically are "minicomputers"[38] that contain details about "the privacies of life,"[39] they require greater privacy protection. In so doing, the Supreme Court essentially returned the personal privacy that the new technologies eroded and the outdated *Chimel* standard threatened. However, the court did not extend the privacy protections so far as to say that cellphones were immune from search and seizure. Instead, once the government has probable cause to believe a cellphone contains evidence that "'will aid in a particular apprehension or conviction' for a particular offense," privacy rights are lessened and the government's right to search takes precedence.[40] Although *Riley* is a Fourth Amendment case, courts will engage in the same balancing act as it relates to forced decryption of password protected devices. Courts will be loath to disturb the delicate balance between privacy and public safety by rendering cellphones impenetrable to search and seizure.

Although forced decryption is not an altogether new technological phenomenon, it has yet to be addressed thoroughly by the courts. For some time, law enforcement agencies have had access to data extrication devices.[41] Manufacturers of such devices describe them as "high-end mobile forensics solution[s]" that "extract[], decode[] and analy[ze] actionable data from…smartphones [and] handheld tablets..."[42] Accordingly, police officers can "rip" an entire cellphone's contents within two minutes.[43] However, recently this capability has been compromised by Apple's iPhone 6. The iPhone 6 is capable of encrypting emails, photos, and contacts based on a complex mathematical algorithm that uses a code created by the phone's user and that the phone's creator does not possess.[44] Consequently, traditional subpoenas demanding the contents of a mobile phone will not yield cognizable information. This prompted outrage from Federal Bureau of Investigation (FBI) Director James B. Comey, who proclaimed, "What concerns me about this is companies marketing something expressly to allow people to hold themselves [above] the law."[45] Thus, the stage is set for another constitutional showdown between technology and privacy.

The crux of the issue is whether providing a password constitutes "testimony" protected by the Fifth Amendment's self-incrimination clause. The clause states that "[n]o person… shall be compelled in any criminal case to be a witness against himself."[46] To oversimplify the issue, compelled communications are testimonial if they require substantial mental effort; those requiring little mental effort are not. Consequently, courts have held that providing handwriting or voice samples is not a testimonial act but complying with a voluminous document production is testimonial. The U.S. Circuit Court of Appeals for the 11th Circuit is the only court that has found forced decryption testimonial. The 11th Circuit's analysis was based on a line of Supreme Court *dicta* opining that the production of strongbox keys can be compelled but combinations to a safe cannot.[47] Therefore, courts must decide whether a password is more akin to a key or a combination.[48]

Traditionally, if a law enforcement agency obtained a warrant substantiated by probable cause, it received the information it sought. This capability was not frustrated by either a safe or a password. However, with the advent of not only iPhone 6 encryption technology, but also cellphone specific rules of criminal procedure, the Supreme Court will undoubtedly confront this issue. The Supreme Court has long recognized that the Fourth Amendment and the Fifth Amendment substantially overlap. This overlap is implicit in *Riley* in that it speaks to

[38] *Riley v. California*, 134 S. Ct. at 2489.

[39] *Id.* at 2495.

[40] Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 Nw. U. L. Rev. Online 56, 59 (2014) (quoting *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967)).

[41] Justin Meyers, *Cops Can Hack Your Cell Phone*, Business Insider (Apr. 25, 2011, 9:00 PM), http://www.businessinsider.com/data-pirates-aka-cops-can-hack-your-cell-phone-2011-4.

[42] Cellebrite, https://www.cellebrite.com/corporate/about-cellebrite (last visited Feb. 6, 2015).

[43] Meyers, *supra* note 41.

[44] David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. Times, Sept. 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html?_r=0.

[45] *Id.*

[46] U.S. Const. amend. V.

[47] *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012).

[48] *See generally id.*

the unique nature of cellphones, which are invariably password protected. The court will presumably recognize this when deciding the issue of forced decryption. Requiring government officials to obtain probable cause to search a cellphone incident to lawful arrest arguably restores equilibrium between personal privacy and public safety. This also holds true in a public school context. However, requiring a warrant and holding that forced decryption violates the self-incrimination clause swings the pendulum of criminal procedure jurisprudence too far. Providing either arrestees or students the constitutional right to secrete inculpatory evidence on a common cellphone would disrupt the delicate balance the justices took such great pains to achieve.

Embracing Privacy Rights Is Not an Invitation to Chaos

Some may reflexively recoil at any limitation on school officials' investigatory capabilities, believing it to be capitulation to the criminal forces that torment school children every day. On closer analysis, this is not the case. The Supreme Court did not hold that all cellphone searches are prohibited; instead, they held that police officers must obtain a search warrant before exploring the content of one's cellphone.[49] By the same token, if a probable cause standard is instituted, school officials still can search students' cellphones to maintain an orderly educational environment, only now they need a good reason.

The lesson is that safety and privacy can coexist if everyone commits to preserving these equally sacrosanct values. Giving school officials unfettered access to search students' cellphones sets a questionable example. Unjustified invasions can be particularly troubling during the fragile adolescent years when personal struggles, relationship dynamics, and issues of self-discovery are omnipresent on students' cellphones. Articulating probable cause is only one more step and a little more work. Isn't that what we have always done to protect children?

[49] *Riley v. California,* 134 S. Ct. at 2493.