No. 18-10231

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

RICHARD D. JACKSON and LORETTA S. JACKSON, and E.D.J., a minor child, by and through her parents, RICHARD D. JACKSON and LORETTA S. JACKSON

Plaintiff-Appellants,

vs.

DAVID MCCURRY, in his individual and official capacities, and SANDI D. VELIZ, BO OATES, JOSH KEMP, and RYAN SMITH, in their individual capacities,

Defendant-Appellees.

On Appeal from the United States District Court
for the Middle District of Georgia
Case No. 4:17-cv-00017-CDL
The Hon. Clay D. Land

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTIFF-APPELLANTS

Marc Rotenberg
Counsel of Record
Alan Butler
Natasha Babazadeh
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

March 12, 2018

Appeal No. 18-10231
Richard D. Jackson *et al.* v. David McCurry *et al.*

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Amicus Curiae Electronic Privacy Information Center (EPIC) provides the following Certificate of Interested Persons and Corporate Disclosure Statement pursuant to Eleventh Circuit Rules 26.1-1, 28.1(b), and 29-2. In addition to the persons and entities identified in the Certificate of Interested Persons and Corporate Disclosure Statement in the Brief of Appellants and the Brief of Amicus Curiae American Civil Liberties Union Foundation of Georgia, Inc., the following are known to have an interest in the outcome of the case:

1. Babazadeh, Natasha, Counsel for Amicus Curiae
2. Butler, Alan, Counsel for Amicus Curiae
3. Electronic Privacy Information Center (EPIC), Amicus Curiae
4. Rotenberg, Marc, Counsel for Amicus Curiae

EPIC is a District of Columbia corporation with no parent corporation. No publicly held company owns 10 percent or more of EPIC stock. EPIC is not aware of any publicly traded company or corporation that has an interest in the outcome of the case or appeal.

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF AMICUS 1

SUMMARY OF ARGUMENT 3

ARGUMENT 4

I. After *Riley*, searches of students' cell phones require heightened privacy protections 5

A. Cell phones are both data storage devices and a gateway to vast amounts of personal data stored in the cloud. 6

B. Most teenagers today could not survive without a cell phone. 9

II. Courts have recognized that student cell phones are entitled to heightened Fourth Amendment protections. 13

III. After *Riley*, states are adopting stronger privacy standards for the searches of students' cell phones. 14

A. Searches of students' cell phones should be limited to those circumstances where it is strictly necessary. 16

B. In the rare case where it is necessary to search a student's cell phone, the search should be limited in scope and duration to what is strictly required under the circumstances. 18

C. Searches of students' cell phones should only be conducted pursuant to formal school policies that comply with the Fourth Amendment. 23

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULES 28

CERTIFICATE OF SERVICE 29

TABLE OF AUTHORITIES

CASES

Berger v. New York,
388 U.S. 41 (1967).....17, 19, 20, 23

Commonwealth v. White,
475 Mass. 583 (2016) 25

G.C. v. Owensboro Public Schs.,
711 F.3d 623 (6th Cir. 2013)..... 13, 17

Gallimore v. Henrico Cty Sch. Bd.,
38 F. Supp. 3d 721 (E.D. Va. 2014)..... 14

J.W. v. Desoto Cty Sch. Dist., No: 2:09-cv-00155-MPM-DAS,
2010 WL 4394059 (N.D. Miss. Nov. 1, 2010) 13, 23

Klump v. Nazareth Area Sch. Dist.,
425 F. Supp. 2d 622 (E.D. Pa. 2006).....14, 17, 22

Mendoza v. Klein Indep. Sch. Dist., No. H-09-3895,
2011 WL 13254310 (S.D. Texas, Mar. 16, 2011) 22

New Jersey v. T.L.O.,
469 U.S. 325 (1985).....4, 18, 19, 25

Riley v. California,
134 S. Ct. 2473 (2014).....4, 5, 6, 8, 9, 18, 23

Safford Unified School Dist. No. 1 v. Redding,
557 U.S. 364 (2009)..... 21, 22

Tinker v. Des Moines Independent Community School Dist.,
393 U.S. 503 (1969).....4

STATUTES

18 U.S.C. § 2518(4)(c) 23

18 U.S.C. § 2518(5) 23

Cal. Penal Code § 1546.1 (West 2017).....14, 15, 18

Or. Rev. Stat. § 336.840(8) (2017) 15

Wash. Rev. Code § 28A.600.230(2)..... 20

OTHER AUTHORITIES

Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, Pew Research Ctr. (Jan. 12, 2017)..... 12, 13

Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Research Ctr. (Apr. 2015)..... 13

Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After Riley v. California*, 10 Duke J. Const. L. & Pub. Pol'y 83, 90 (2014) 5

Apple, iCloud Drive (2018) 7

Apple, *Use Notifications on iPhone, iPad, and iPod Touch* (2018) 8

Apple, *What Does iCloud Back Up?* (2018) 7

Atlanta Public Schools, *2017/18 Student Handbook* (2017) 15, 16

Blackboard, *Trends in Digital Learning: Empowering Innovative Classroom Models for Learning* (2015) 11

Christine L. Borgman, *New Models of Privacy for the University* in *Privacy In the Modern Age* (Marc Rotenberg et al. eds., 2015) 12

danah boyd & Alice E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies*, Oxford Internet Inst. (2011) 12

danah boyd, *It's Complicated: The Social Lives of Networked Teens* (2015) 10

danah boyd, *The Truth About Teens and Privacy*, Wired (Dec. 23 2014) 11

David Kravets, *Legislation Allowing Warrantless Student Phone Searches Dies for Now*, ArsTechnica (Apr. 13, 2017) 15

Douglas Cnty. Sch. Sys., *Douglas County School System Policies and Procedures: High School* 2017-2018 (2017) 21

Dr. Pablo G. Molina, *Protecting Privacy in Education* in *Privacy in Modern Age* (Marc Rotenberg et al. eds., 2015) 12

eMarketer, *Teens' Ownership of Smartphones Has Surged* (July 5, 2016) 10

Florida Dep't of Education, *Guidelines for Investigations* 18

Joseph P. Lilly & Nicole A. Donatich, *'Reasonable Suspicion' Must Precede Cellphone Search*, N.Y.S. Sch. Bds. Ass'n (Oct. 9, 2017) 22

Leslie Brody, *Cellphone Ban in NYC Schools to End*, Wall St. J. (Jan. 6, 2015) 11

Linda Matchan, *Schools Seek Balance for Cellphones in Class*, Boston Globe (June 2015) 10

Memorandum of Understanding Between the Montgomery County Public Schools and Montgomery County Department of Police and Montgomery County Sheriff's Office and Rockville City Police Department and Gaithersburg City Police Department and Takoma Park Police Department and Montgomery County State's Attorney's Office: School Resource Officer Program and Other Law Enforcement Responses to School-Based Incidents (Memorandum of Understanding) (2017) 20, 21

Michelle Coulombe, *New Survey Finds 85 Percent of Educational Institutions Allow BYOD Despite Security Concerns*, Bradford Networks (May 2013) 11

Peggy Anne Salz & Jennifer Moranz, *The Everything Guide to Mobile Apps* (2013) 8

Pew Research Ctr., *Mobile Fact Sheet* (Feb. 2018) 9

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1]

EPIC routinely participates as *amicus curiae* before the United States Supreme Court and other courts in cases concerning emerging privacy issues, new technologies, and constitutional interests. EPIC has authored several briefs specifically concerning searches of cell phones and personal data generated by cell phones. *See*, *e.g.*, Brief of *Amici Curiae* EPIC et. al, *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2016), *cert. granted* 137 S. Ct. 2211 (2017) (No. 16-402) (arguing that the Fourth Amendment protects the right against warrantless seizure and search of location data); Brief of *Amicus Curiae* EPIC, *Commonwealth v. White*, 475 Mass. 586 (2016) (arguing that a warrant is required before a school may turn over a student's cell phone to the police); Brief of *Amici Curiae* EPIC et. al, *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that warrantless search of a cell phone incident to an arrest is impermissible).

[1] All parties consent to the filing of EPIC's *amicus* brief. In accordance with Fed. R. App. P. 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

EPIC also works to protect student privacy. EPIC has proposed a Student Privacy Bill of Rights to safeguard student data and security, EPIC, *Student Privacy Bill of Rights* (2015),[2] has obtained documents regarding the misuse of education records through the Freedom of Information Act, EPIC, *EPIC Uncovers Complaints from Education Department about Misuse of Education Records* (July 18, 2014),[3] and has challenged Department of Education regulations that diminish student privacy safeguards under the Family Educational Rights and Privacy Act. *EPIC v. U.S. Dep't of Educ.*, 48 F. Supp. 1 (D.D.C. 2014).

[2] https://epic.org/privacy/student/bill-of-rights.html.
[3] https://epic.org/2014/07/epic-uncovers-complaints-from.html.

SUMMARY OF ARGUMENT

This case concerns an issue of central importance to families across the country: whether school administrators may gain unfettered access to the contents of a student's cell phone. *TLO v. New. Jersey* established that students have a reasonable expectation of privacy in their belongings. And the Supreme Court's recent decision in *Riley v. California* makes clear that the search of a cell phone requires a warrant.

Under the principles established in *T.L.O.* and *Riley*, teachers may not search a student's cell phone unless they have followed an explicit school policy that complies with Fourth Amendment requirements. The school policy should make clear that teachers should have reasonable suspicion of a threat to life or property, or a clear violation of a school policy, before a student's phone is seized. The search of a student's phone implicates additional constitutional interests. School policies should make clear (1) the circumstances when a cell phone may be seized, (2) that a cell phone may only be searched when strictly necessary , (4) who in the school is authorized to undertake a search, (5) the procedures for limiting the scope of the search, (6) the procedures for notifying the student's parents or guardian regarding the search, (7) that a warrant is required before any evidence obtained may be disclosed to the police, and (8) the procedure for reporting to district officials all incidents involving searches of student cell phones.

ARGUMENT

Students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." *Tinker v. Des Moines Independent Community School Dist.*, 393 U.S. 503, 506 (1969). Nor do they shed their reasonable expectation of privacy. *New Jersey v. T.L.O.*, 469 U.S. 325, 326 (1985). The Court has emphasized that "[s]choolchildren have legitimate expectations of privacy. They may find it necessary to carry with them a variety of legitimate, noncontraband items, and there is no reason to conclude that they have necessarily waived all rights to privacy in such items by bringing them onto school grounds." *Id.*

The Court has also recognized that cell phones contain uniquely sensitive records that demand special protection. As the Court outlined in *Riley v. California*, 134 S. Ct. 2473 (2014), cell phones "place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search" that the Court previously allowed in the search incident to arrest context. 134 S. Ct. at 2485. Cell phones have become integral to social, professional, educational, and personal activities—especially for young students. The Court's conclusion in *Riley* that cell phones require greater Fourth Amendment protections than physical items applies equally to searches and seizures by school administrators. Therefore, under

Riley and *T.L.O.*, school administrators must strictly limit searches of cell phones and ensure that special protections are in place.

I. After *Riley*, searches of students' cell phones require heightened privacy protections

Modern cell phones contain detailed, sensitive personal information and should not be seized and searched by school administrators without consent or due process. The Court made clear in *Riley* that searches of cell phones by government officials pose unique threats to privacy and must be strictly limited under the Fourth Amendment. "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Riley*, 134 S. Ct. at 2494–95 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). The Court found that cell phones are different in "both a quantitative and a qualitative sense from other objects." *Id*. at 2489. Their storage capacity, functionality, and unique role as an essential tool for modern life "fundamentally alters the privacy interests at stake." Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After Riley v. California*, 10 Duke J. Const. L. & Pub. Pol'y 83, 90 (2014).

The Court in *Riley* provided a simple answer to the "question of what a police officer must do before searching a cell phone seized incident to arrest . . . get a warrant." 134 S. Ct. at 2495. It is clear that search of a cell phone is more intrusive than the search of such physical possessions, as purse or gym bag. Cell

phone searches therefore require greater protections than a search of physical items in the student's possession. "Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Riley*, 134 S. Ct. at 2488–89. Cell phones store troves of personal information and are a "pervasive and insistent part of daily life." *Id.* at 2484. This is particularly true for teenagers, the vast majority of whom are rarely untethered from their cell phones.

A. Cell phones are both data storage devices and a gateway to vast amounts of personal data.

A majority of cell phone users now own smartphones equipped with mobile applications that connect, synchronize, and deliver data stored and processed on remote servers. *Riley*, 134 S. Ct. at 2491. Many of these mobile "apps" allow users to access content across multiple platforms—on their phones, computers, and tablets. Modern phones not only provide access to files, messages, photos, and music, but they also act as the keys that unlock a users' online identities. *Id.* These devices provide access to remote repositories that contain private financial, medical, and location information. *Id.* at 2490.

Users access e-mail messages, calendars, photographs, files, notes, and other personal data on all their devices – phones, computers, and tablets – via mobile apps. For example:

> With iCloud Drive, you can safely store all your presentations, spreadsheets, PDFs, images and any other kinds of files in iCloud – and access them from your iPhone, iPad, iPod touch, Mac, or PC. And now you can invite people to work on the same file with you – no creating copies, sending attachments, or managing versions. …the new Files app gives you one easy place to find, organize, and share [your files].

Apple, iCloud Drive (2018).[4] The iCloud Backup also stores vast troves of personal data across different platforms, including:

> App data, Apple Watch backups, call history, device settings, HomeKit configuration, Home screen and app organization, iMessage, text (SMS), and MMS messages, photos and videos on your iPhone, iPad, and iPod touch, purchase history from Apple services, like your music, movies, TV shows, apps, and books, ringtones, and Visual Voicemail password.

Apple, *What Does iCloud Back Up?* (2018).[5] Therefore, given iCloud services, access to a phone provides significantly more data than that which the phone itself produced throughout the duration of its use.

Many mobile apps display a mix of locally stored and remotely synchronized content on the user's device. When a user opens an app, "[c]ontent such as pictures or video is [downloaded] over the Internet via a mobile data connection ([or] Wi-Fi), and once the content is embedded in the device (your smartphone), the data connection can be closed and the content viewed offline

[4] https://www.apple.com/icloud/icloud-drive/.
[5] https://support.apple.com/en-us/HT207428.

(when you are not connected to the Internet)." Peggy Anne Salz & Jennifer Moranz, *The Everything Guide to Mobile Apps* 15 (2013).

This model of computing is sometimes described as "cloud computing."[6] From the user's perspective, the data that is stored on the phone and the data that is stored in the cloud and available on the phone are often indistinguishable. App data is continuously updated in order to ensure that the data is synchronized across all the users' devices. In fact, many apps now provide updates even when the user does not have them. *See* Apple, *Use Notifications on iPhone, iPad, and iPod Touch* (2018).[7] By default, Apple devices allow these notifications to be viewed even when the phone is locked. *Id.*

This cloud-based model allows the user to obtain their messages, files, and records from several different devices. As a consequence, the seizure of a cell phone provides access not only to files stored on the phone itself but also to personal information stored elsewhere. For example, a user's bank account information may be readily accessible with an app on the phone. With cloud computing, the phone also provides access to the data stored on the user's other mobile devices and home computers. *See Riley*, 134 S. Ct. at 2473. With the growing use of Internet-enabled home services, such as thermostats, lighting and

---

[6] For a brief description of cloud services, see Eric Griffith, *What Is Cloud Computing?*, PC Magazine (May 3, 2016), https://www.pcmag.com/article2/0,2817,2372163,00.asp.

[7] https://support.apple.com/en-us/HT201925.

door locks, possession of the cell phone could even provide intimate information to administrators about the activities of an individual within their home, without ever receiving consent or a warrant to search the home. Cell phones provide access to detailed, sensitive personal information that should not be subject to inspection with consent or reasonable precautions.

B. Most teenagers today could not survive without a cell phone.

In *Riley*, the Supreme Court emphasized the importance of cell phones in Americans' lives, finding that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484. Cell phones are ubiquitous in the United States. More than 95 percent of American adults own a cell phone. Pew Research Ctr., *Mobile Fact Sheet* (Feb. 2018).[8] Seventy-seven percent of U.S. adults have a smartphone, up from 35 percent in 2011. *Id.* Smartphone ownership is nearing the saturation point with some groups: 94 percent of those ages 18-29 have a smartphone, as do 89 percent of those ages 30 to 49. *Id.*

Teenagers, in particular, are dependent on cell phones. It is difficult to overstate in 2018 the role that mobile devices play in teenagers' lives. Approximately 87 percent of teenagers between the ages of 14 and 18 said they

[8] http://www.pewinternet.org/fact-sheet/mobile/.

owned or used a smartphone. eMarketer, *Teens' Ownership of Smartphones Has Surged* (July 5, 2016).[9] Also, 92 percent of teens report going online daily. Linda Matchan, *Schools Seek Balance for Cellphones in Class*, Boston Globe (June 2015).[10] Teens use phones to access the Internet "to connect to people in their community. Their online participation is not eccentric; it is entirely normal, even expected." danah boyd, *It's Complicated: The Social Lives of Networked Teens* 4 (2015). Mobile devices are not just a current fad to teenagers. They have become the modern way of life:

> What the drive-in was to teens in the 1950s and the mall in the 1980s, Facebook, texting, Twitter, instant messaging, and other social media are to teens now. Teens flock to them knowing they can socialize with friends and become better acquainted with classmates and peers they don't know as well. They embrace social media for roughly the same reasons earlier generations of teens attended sock hops, congregated in parking lots, colonized people's front stoops, or tied up the phone lines for hours on end. Teens want to gossip, flirt, complain, compare notes, share passions, emote, and joke around. They want to be able to talk among themselves—even if that means going online.

Id. at 20. For teenagers, cell phones are not only a means of communication, but also a gateway to their social persona and identity. And as technology continues to develop, teens only become more dependent on their personal devices to keep up with the status quo.

---

[9] https://www.emarketer.com/Article/Teens-Ownership-of-Smartphones-Has-Surged/1014161.

[10] https://www.bostonglobe.com/lifestyle/style/2015/06/15/cellphones-school-teaching-tool-distraction/OzHjXyL7VVIXV1AEkeYTiJ/story.html.

Schools have recognized the vital role cell phones play in the everyday lives of teenagers and their families. As a result of this change, there has been a shift in school policies away from banning cell phones on school property. In 2011, over 50 percent of school administrators prohibited students from using their own mobile devices at school; in 2014, that percentage dropped by more than half. Blackboard, *Trends in Digital Learning: Empowering Innovative Classroom Models for Learning* (2015).[11] In 2015, New York City ended its decade long ban on cell phones in schools, citing the need for parents to keep in touch with their children. Leslie Brody, *Cellphone Ban in NYC Schools to End*, Wall St. J. (Jan. 6, 2015).[12] As of 2013, more than 85 percent of educational institutions allow students to bring and use their own personal devices on institutional networks. Michelle Coulombe, *New Survey Finds 85 Percent of Educational Institutions Allow BYOD Despite Security Concerns*, Bradford Networks (May 2013).[13]

There is also a misconception that teens do not care about privacy. Leading privacy researchers have found that teens have a strong sense of privacy and that, though individual behaviors vary, teens treat privacy as a social norm. danah boyd, *The Truth About Teens and Privacy*, Wired (Dec. 23 2014);[14] danah boyd & Alice

---

[11] http://www.tomorrow.org/speakup/2015_ClassroomModels.html.
[12] https://www.wsj.com/articles/cellphone-ban-in-nyc-schools-to-end-1420602754.
[13] https://www.bradfordnetworks.com/new-survey-finds-85-percent-of-educational-institutions-allow-byod-despite-security-concerns/.
[14] https://www.wired.com/2014/12/the-truth-about-teens-and-privacy/.

E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies*, Oxford Internet Inst. 1–2 (2011);[15] *see also* Christine L. Borgman, *New Models of Privacy for the University* in *Privacy In the Modern Age* 32, 33 (Marc Rotenberg et al. eds., 2015) ("[P]rivacy underpins an ethical and respectful environment for the entire university community."); Dr. Pablo G. Molina, *Protecting Privacy in Education* in *Privacy in Modern Age* 138, 143 (Marc Rotenberg et al. eds., 2015) ("Among the vulnerable are students with disabilities or special needs, who would like to control the disclosure of this information.").

Cell phones are an increasingly important part of Americans' daily lives. Pew Research found that 12 percent of Americans own a smartphone but do not have broadband at home. Aaron Smith, *Record Shares of Americans Now Own Smartphones, Have Home Broadband*, Pew Research Ctr. (Jan. 12, 2017) [hereinafter Smith, *Smartphones and Broadband*].[16] Also, students who have not graduated from high school are almost three times less likely than college graduates to have home broadband service (34% vs. 91%). *Id.* Americans no longer use their phones solely for calling each other but also to browse online and navigate important life activities. As of 2015, Americans use cell phones to send text messages (97 percent), read e-mail (88 percent), look up information about health conditions (62 percent), do online banking (57 percent), get job information

[15] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.
[16] http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

(43 percent), look up government services or information (40 percent) and take a class or get educational content (30 percent). Aaron Smith, *U.S. Smartphone Use in 2015*, Pew Research Ctr. (Apr. 2015).[17] Social media has also become very popular among teenagers, with 86 percent of individuals between the age of 18 and 29 being social media users. Smith, *Smartphones and Broadband*, *supra*.

Given the central role that cell phones play in the lives of modern teens, there can be no greater privacy interest for a student than the protection of their cell phone from unauthorized search and seizure. In the rare cases where it is strictly necessary for school administrators to seize and search a student's cell phone, special protections are required to ensure Fourth Amendment privacy interests.

II. Courts have recognized that student cell phones are entitled to heightened Fourth Amendment protections.

Even before *Riley,* courts recognized the need for greater protections against school administrators from searching students' cell phones. For example, the Sixth Circuit held that blanket permission to search phones after an intentional violation of school policy on cell phone use was unreasonable and that the school did not have reasonable suspicion to search the phone. *G.C. v. Owensboro Public Schs.*, 711 F.3d 623 (6th Cir. 2013); *but see J.W. v. Desoto Cty Sch. Dist.*, No: 2:09-cv-00155-MPM-DAS, 2010 WL 4394059 (N.D. Miss. Nov. 1, 2010) (finding that searches of phones are reasonable when a student intentionally violates school

[17] http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

policies on cell phone use). One court has excluded records obtained from the search of a student's cell phone by school officials looking for evidence of illegal drug use. *Gallimore v. Henrico Cty Sch. Bd.*, 38 F. Supp. 3d 721 (E.D. Va. 2014). The court in *Gallimore* held that searching the student's phone exceeded the scope of a reasonable search to find drugs because the phone could not have contained drugs. *Id.* Another court found that searching a student's phone was unreasonable because there was no basis for believing the phone's owner had committed the alleged misconduct. *Klump v. Nazareth Area Sch. Dist.*, 425 F. Supp. 2d 622 (E.D. Pa. 2006).

Most of the lower courts that have considered related issues have found that searching the student's cell phone was unreasonably intrusive despite the underlying circumstances prompting the search and the *T.L.O.* reasonableness standard.

III. After *Riley*, states are adopting stronger privacy standards for the searches of students' cell phones.

Since the *Riley* decision, several states have established new standards to limit the scope of searches of student cell phones. For example, California codified special protections for cell phones under the California Electronic Communications Privacy Act ("CalECPA"). *Schools may not search a cell phone without permission except with a search warrant or in the case of an emergency*. Cal. Penal Code § 1546.1 (West 2017). An emergency constitutes "danger of death or

serious physical injury to any person [that] requires access to the electronic device information." *Id.* § 1546.1(c)(6). A recent attempt by state lawmakers to exempt student cell phone searches from the CalECPA rules was blocked and the bill (AB165) did not pass. David Kravets, *Legislation Allowing Warrantless Student Phone Searches Dies for Now*, ArsTechnica (Apr. 13, 2017).[18]

Other states have addressed more generally the rights of students to use cell phones at school, while clarifying that the school is not entitled to unfettered access to private student data. For example, Oregon has adopted policies regarding use of personal devices in school, and explicitly acknowledges that these policies do not authorize schools "to request, require or compel access to a student's electronic mail or personal online accounts." Or. Rev. Stat. § 336.840(8) (2017). The Atlanta School District has a policy permitting possession of "mobile telephones and other personal electronic devices (PEDs) with the expressed, written consent of their parents/guardians" but prohibiting use of those devices "[u]nless otherwise directed by school administration or school staff . . . at all times during the instructional day." Atlanta Public Schools, *2017/18 Student Handbook* 47 (2017).[19] The policy provides that "[a]ll staff members have the right to confiscate mobile phones when used in violation" of the school policy and

[18] https://arstechnica.com/tech-policy/2017/04/legislation-allowing-warrantless-student-phone-searches-dies-for-now/.
[19] https://www.atlantapublicschools.us/cms/lib/GA01000924/Centricity/Domain/94/2web_ENG%202017-18%20APS%20Student%20Handbook_July%202017.pdf.

implementing regulations. *Id*. But confiscating a phone used during school hours is not the same as searching the contents of the phone, which the Atlanta policy does not authorize.

In the context of school searches of students' cell phones, strict limitations on the scope and circumstances of the search should be imposed, similar to the limits on audio and video surveillance imposed by the Courts and Congress under *Berger*. These searches should be subject to three types of limitations. First, a school should not be permitted to search a student's cell phone without consent in any disciplinary matters that do not concern data stored on the phone. If a disciplinary investigation does warrant searching a phone without consent, that search should only be conducted after all other reasonable methods of obtaining the information have been exhausted. Second, in the rare instance where it is necessary to search a student's phone, the search should be limited in time and scope to what is strictly necessary to address the disciplinary matter. And third, retention of any data collected on the phone should be limited in time and any subsequent use or dissemination of student data outside the context of the disciplinary matter should be prohibited.

A. Searches of students' cell phones should be limited to those circumstances where it is strictly necessary.

Under *Riley* and other cases that address the unique problems of searching communications, school cell phone searches should be "carefully circumscribed"

and conducted in connection with an inquiry into a "particular offense" that justifies such an extreme invasion of privacy. This means that cell phones should only be subject to search when their contents are at issue in a disciplinary proceeding. Mere confiscation of a cell phone cannot justify a search of that phone. Furthermore, a device should not be searched unless there are no less intrusive means of obtaining the necessary information. For example, teachers may be able to resolve a dispute by further discussions with students, rather than seizing and examining the contents of a particular student's cell phone

Limiting the circumstances in which it is permissible for a school to search a student's phone serves the core Fourth Amendment purpose of preventing "general searches" and "the seizure of one thing under a warrant describing another." *Berger v. New York*, 388 U.S. 41, 58 (1967). For example, violation of a school policy that prohibits possession or use of a cell phone in the classroom might justify temporary confiscation, but it would not justify the search of the contents of the phone. *See G.C. v. Owensboro Public Schs.*, 711 F.3d 623 (6th Cir. 2013). Similarly, a disciplinary inquiry into possession of some physical contraband would not justify a search of a student's cell phone. *See Klump v. Nazareth Area School Dist.*, 425 F. Supp. 2d 622, 640–41 (E.D. Pa. 2006).

Searches of student cell phones should also be limited to those circumstances where all other methods of obtaining the information have failed,

which would ensure that such searches only occur in exceptional circumstances and as a last resort. As noted above, the State of California already prohibits all non-consensual and warrantless cell phone searches, including searches in schools, except in emergency circumstances. Cal. Penal Code § 1546.1.

This exhaustion requirement would also be consistent with existing school policies that outline many other methods of reviewing disciplinary matters, including interviewing witnesses and students involved in the controversy, identifying physical evidence relative to the case, and seeking consent to engage in limited searches. *See, e.g.*, Florida Dep't of Education, *Guidelines for Investigations*.[20] It is only after such efforts have failed that it becomes necessary and therefore "reasonable" to conduct a search of a student's cell phone.

B. In the rare case where it is necessary to search a student's cell phone, the search should be limited in scope and duration to what is strictly required under the circumstances.

The Fourth Amendment requires that "the interests of the students will be invaded no more than is necessary" during a school search "to achieve the legitimate end of preserving order in the schools." *T.L.O.*, 469 U.S. at 343. And the Supreme Court has held that cell phone searches are extremely invasive because of the vast quantity and sensitive nature of the data stored on cell phones. *Riley*, 134 S. Ct. at 2494–95 (noting that cell phone data can reveal "the privacies of life").

[20] http://www.fldoe.org/core/fileparse.php/7725/urlt/0072435-guidelineinvest.pdf.

In *T.L.O.*, the Court found that the reasonableness of a search depends upon "whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place." 469 U.S. at 341 (internal citations omitted). The Court held that a search is only reasonable "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive." *Id.* The Court emphasized that "[t]o the extent that deeply intrusive searches are ever reasonable [in the school] context, it surely must only be to prevent imminent, and serious harm." *Id.* at 382 n. 25.

In order to ensure that student interests are adequately protected during searches of cell phones, courts should look to the privacy protections that have been applied to another category of highly invasive searches: wiretaps.

When the Supreme Court ruled that a New York statute authorizing the interception of private communications was invalid under the Fourth Amendment, it did so not based on a lack of warrant or probable cause, but based on the lack of "particularization" and the lack of "precise and discriminate" limitations on the search. *Berger*, 388 U.S. at 55, 58. The Court in *Berger* identified several factors that made the interception of privacy communications unreasonable in context: (1) the lack of a requirement that a "particular offense" be identified and that the target conversations be "describe[d] with particularity," (2) the lack of limitation on the scope of the search, which would involve seizing "the conversations of any and all

persons . . . indiscriminately and without regard to their connection" with the offense under investigation, (3) the lack of limitations on the length of the search or requirement that exigent circumstances be shown, and (4) the lack of restrictions on the subsequent "use of seized conversations of innocent as well as guilty parties." *Id*. at 58–59. Congress subsequently codified a set of explicit requirements in the Wiretap Act that track the *Berger* factors.

Several schools already have policies limiting excessively intrusive searches in the physical context based on factors such as age and gender of the student. These limitations and restrictions on physical searches based on age and gender have been adopted on a state-wide basis in Washington. Wash. Rev. Code § 28A.600.230(2). Similar restrictions have been applied through county-wide policies in other states. *See, e.g.*, Memorandum of Understanding Between the Montgomery County Public Schools and Montgomery County Department of Police and Montgomery County Sheriff's Office and Rockville City Police Department and Gaithersburg City Police Department and Takoma Park Police Department and Montgomery County State's Attorney's Office: School Resource Officer Program and Other Law Enforcement Responses to School-Based Incidents (Memorandum of Understanding) 2 (2017) [hereinafter Montgomery MOU];[21] Douglas Cnty. Sch. Sys., *Douglas County School System Policies and*

[21] http://www.montgomeryschoolsmd.org/departments/policy/pdf/jgbra.pdf.

Procedures: High School 2017-2018, at 50 (2017) (detailing search and seizure policies for high schools in Douglas County, Ga.).[22] These limitations directly track the factors that the Supreme Court considered excessively intrusive in *Safford Unified School Dist. No. 1 v. Redding*, 557 U.S. 364 (2009). And some schools have gone even further in limiting unnecessary and excessively intrusive physical searches. For example, Montgomery County prohibits officials from continuing to search students when there is no reasonable possibility that a contraband item could be concealed and the scope of the search is no longer reasonable. Montgomery MOU, *supra*, at 2.

For the same reason that schools have previously limited the scope of physical searches based on *T.L.O.* and *Redding*, schools should now limit the scope of cell phone searches based on *Riley*. For example, the New York State Association of School Attorneys has issued a statement recommending that school administrators limit searches of student phones to situations in which it is "reasonable to believe that the search will yield evidence that the student has violated the law or a school rule," while also limiting the scope of cell phone searches "only to those parts of the phone where the evidence being sought may reasonably be expected to be found." Joseph P. Lilly & Nicole A. Donatich, *'Reasonable Suspicion' Must Precede Cellphone Search*, N.Y.S. Sch. Bds. Ass'n

[22] http://images.pcmac.org/Uploads/DouglasCounty/DouglasCounty/Sites/DocumentsCategories/Documents/2017-2018_HIGH_SCHOOL_HANDBOOK.pdf.

(Oct. 9, 2017).[23] Students may store highly sensitive material on their phones which should be given similar levels of protection as their physical privacy.

For example, the student in *Redding* was humiliated and her privacy was violated when school officials saw her undressed. *Redding*, 557 U.S. at 374–75. In a troublingly similar scenario, the school official in *Mendoza v. Klein Independent School District* subjected a student to humiliation and embarrassment when she saw nude photos of the student while searching her phone. *See Mendoza*, No. H-09-3895, 2011 WL 13254310, at *11 (S.D. Texas, Mar. 16, 2011). The school official in *Mendoza* had confiscated the phone and was searching it to determine whether the student had been "using it during school hours" in violation of the school policy. *Id*. at *9. But even the school official in that case subsequently acknowledged that it was not necessary to read the contents of the student's text messages. *Id.* at *10.

Absent a clear rule imposing limitations on the scope of cell phone searches, school officials have repeatedly searched and used cell phones for purposes far outside the justifiable scope under *T.L.O.* For example, in *Klump*, a teacher confiscated a phone that fell out of a student's pockets in class and subsequently read the student's text messages and used the phone to call other students and even send text messages to the student's younger brother. *Klump*, 425 F. Supp. 2d at

[23] http://www.nyssba.org/news/2017/10/05/on-board-online-october-9-2017/reasonable-suspicion-must-precede-cellphone-search/.

630. School officials in a Mississippi case confiscated a phone for violation of a similar rule and subsequently searched through the student's photos in order to identify "photographs depicting him making gang signs." *J.W. v. Desoto Cnty. Sch. Dist.*, No. 09-cv-155, 2010 WL 4394059, at *14 (N.D. Miss. Nov. 1, 2010). That sort of fishing expedition is precisely the type of unreasonable search that the Court rejected in *Riley*, 134 S. Ct. at 2480–81.

A strict limitation on the scope of school searches of students' cell phones is necessary to ensure that the Fourth Amendment particularity requirement is met. *See, e.g.*, *Berger*, 388 U.S. at 56; 18 U.S.C. §§ 2518(4)(c), 2518(5). In the school context, these limitations safeguard against overly intrusive searches and limit the search to what is strictly necessary. Without restrictions on the scope of these searches, school officials will be able to gain unfettered access to the contents of students' cell phones even in cases where a brief or limited search is all that is necessary to serve the school's legitimate disciplinary purpose.

C. Searches of students' cell phones should only be conducted pursuant to formal school policies that comply with the Fourth Amendment.

Given the highly intrusive nature of cell phone searches and the strong Fourth Amendment protections recognized by the Supreme Court in *Riley*, school officials should not be permitted to search a student's phone except pursuant to a formal policy that complies with the Fourth Amendment. Every school should have such a policy that sets out:

1. The circumstances when a cell phone may be seized;
2. That a cell phone may only be searched when strictly necessary or with the consent of the student;
3. Who in the school is authorized to undertake a search;
4. The procedures for limiting the scope of the search;
5. The procedures for notifying the student's parents or guardian regarding the search;
6. That a warrant is required before any evidence obtained may be disclosed to the police; and
7. The procedure for reporting to district officials all incidents involving searches of student cell phones.

In order to comply with the Fourth Amendment, these policies should impose limits both on when cell phone searches can occur and on the permissible scope of those searches.

First, the school policy should make clear that teachers need to have a reasonable suspicion of a threat to life or property, or a clear violation of a school policy, before seizing a student's cell phone. The policy should also make clear that authority to search a cell phone is necessarily more limited than the authority to confiscate that phone temporarily based on a minor infraction of school rules. In the same way that the arrest of the defendant and resulting seizure of the phone in

Riley did not justify a subsequent search, the confiscation of a student's phone alone cannot justify a subsequent search. Also, a cell phone search should only be conducted when it is strictly "necessary," meaning that all other possible methods for resolving the disciplinary matter have failed.

Second, the school policy should make clear that in the rare circumstances where a search of a student's cell phone is justified, that search must be strictly limited in scope and duration. The search must be "reasonably related to the objectives" and "not excessively intrusive." *T.L.O.*, 469 U.S. at 341. This means limiting the search to the specific communications or applications within the phone where relevant evidence may be reasonably expected to be found, as the school attorneys in New York have recommended.

The school policy should also address potential law enforcement access. After *Riley*, courts have recognized that law enforcement can only search a student's phone with a warrant. For example, the Massachusetts Supreme Judicial Court ruled that the Fourth Amendment prohibits law enforcement from seizing a cell phone from a school based simply on an officer's suspicion that a cell phone may be used in a crime. *Commonwealth v. White*, 475 Mass. 583 (2016). The Court emphasized that "even where there is probable cause to suspect the defendant of a crime, police may not seize or search his or her cellular telephone to look for evidence unless they have information establishing the existence of particularized

evidence likely to be found there." *Id.* at 590–91. Otherwise "it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search." *Id.* at 591. In *White*, the Court also found that retaining the cell phone for 68 days before obtaining a warrant was unreasonable. *Id.* at 595. In other words, secondary use, retention and dissemination were considered unreasonable under the Fourth Amendment without procedural safeguards, like getting a warrant.

* * *

After the Supreme Court's decision in *Riley v. California*, schools should respect the substantial Fourth Amendment limitations on the search of the contents of a student's cell phone. The United States Constitution, and the protections it affords, provide the basis for our form of government. Schools should teach by example.

CONCLUSION

Amicus Curiae respectfully requests this Court to reverse the lower court's decision.

March 12, 2018

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
Alan Butler
Natasha Babazadeh
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Amicus

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULES

This brief complies with the type-volume limitation of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 5,909 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(i). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word for Mac 2011 in 14 point Times New Roman.

Dated: March 12, 2018

/s/ Marc Rotenberg
Marc Rotenberg

CERTIFICATE OF SERVICE

I hereby certify that on March 12, 2018, I electronically filed the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center Support of Petitioner with the Clerk of the United States Court of Appeals for the Eleventh Circuit using the CM/ECF system. All parties are to this case will be served via the CM/ECF system.

Dated: March 12, 2018

/s/ Marc Rotenberg
Marc Rotenberg