COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT
NO. SJC-11917

COMMONWEALTH OF MASSACHUSETTS
Appellant

v.

ONYX WHITE
Defendant-Appellee

ON APPEAL FROM A JUDGMENT OF THE SUFFOLK SUPERIOR COURT

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANT

Marc Rotenberg
BBO# 55048
Caitriona Fitzgerald
BBO# 673324
Alan Butler
John Tran
Electronic Privacy
Information Center
(EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

November 23, 2015

CORPORATE DISCLOSURE STATEMENT

Pursuant to S.J.C. Rule 1:21 *amicus curiae* Electronic Privacy Information Center ("EPIC") states that it is a District of Columbia corporation with no parent corporation or publicly-held company with a 10 percent or greater ownership interest. EPIC is a non-profit, non-partisan corporation, organized under section 501(c)(3) of the Internal Revenue Code.

TABLE OF CONTENTS

TABLE OF CONTENTS..... ii

TABLE OF AUTHORITIES..... iii

INTEREST OF THE AMICUS CURIAE..... 1

SUMMARY OF THE ARGUMENT..... 3

ARGUMENT..... 5

I. Digital is different: The *New Jersey v. T.L.O.* standard for school searches does not apply to cell phones..... 5

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

B. Cell phones are nearly universal and teenagers, the generation most exposed to new technologies, are particularly dependent on cell phones. 10

II. The adoption of reasonable cell phone use policies by schools does not grant law enforcement officers the authority to deprive students of their personal property without a warrant. 15

CONCLUSION..... 18

TABLE OF AUTHORITIES

Cases

Commonwealth v. Damian D., 434 Mass. 725 (2001).. 3, 5, 17
Commonwealth v. Snyder, 413 Mass. 521 (1992)..... 3
New Jersey v. T.L.O., 469 U.S. 325 (1985). 5, 6, 16, 17
Riley v. California, 134 S. Ct. 2473 (2014)..... passim
Tinker v. Des Moines Independent Community School Dist., 393 U.S. 503 (1969) 3

Other Authorities

Anderson, Technology Device Ownership: 2015, Pew Research Center (Oct. 2015) 11
Apple, About Notifications on iPhone, iPad, and iPod Touch (2015) 9
Borgman, New Models of Privacy for the University, 32 (Marc Rotenberg et al. eds.), 2015) 13
boyd and Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies (2011) 13, 14
Brody, Cell phone ban in NYC Schools to End, Wall Street Journal (Jan. 6, 2015) 13
Fullbright, Ph.D., Cell Phones in the Classroom: What's Your Policy?, Faculty Focus (Apr. 15, 2013) 16
Google, Android Quick Start Guide (2013)..... 8
Habib, What Parents Need to Know About Changing Cell Phone Policies in Schools, Tulsa World (Nov. 17, 2015) 16
Johnson, How to Manage Cell Phones in the Classroom, Edutopia (June 17, 2015) 15
Kaplan, Opt-Out: Protect Children..... 14
Lenhart, Teen, Social Media and Technology Overview 2015, Pew Research Center (Apr. 2015) 12
Matchan, Schools Seeking Balance for Cell Phones in Class, Boston Globe (June 16, 2015) 15
Molina, Protecting Data Privacy in Education, 138 (Marc Rotenberg et al. eds., 2015) 13
Project Tomorrow and Blackboard, Trends in Digital Learning: Empowering Innovative Classroom Models for Learning (June 2015) 13

Salz & Moranz, The Everything Guide to Mobile Apps (2013) 8
Smith, U.S. Smartphone Use in 2015, Pew Research Center (Apr. 2015) 11, 12

INTEREST OF THE *AMICUS CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. The EPIC State Policy Project is based in Cambridge, Massachusetts. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other democratic values. The EPIC Advisory Board includes renowned legal scholars and technology experts. EPIC maintains one of the top privacy sites in the world, www.epic.org. EPIC frequently participates as *amicus curiae* in the United States Supreme Court, other appellate courts, and this Court in cases concerning emerging privacy issues. *See, e.g.*, *Commonwealth v. Connolly,* 454 Mass. 808 (2009) (use of a GPS tracking device); *Riley v. California*, 134 S. Ct. 2473 (2014) (search of a cell phone incident to an arrest); *Florida v. Harris*, 133 S. Ct. 1050 (2013) (use of drug detection dog at the entry to a home); *Maryland v. King*, 133 S. Ct. 1 (2013) (collection of DNA incident to an arrest).

[1] EPIC Appellate Advocacy Fellow Aimee Thomson assisted in the preparation of this brief.

EPIC seeks to ensure the application of Constitutional safeguards as new policing practices emerge. As Justice Sandra Day O'Connor explained, "[w]ith the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities." *Arizona v. Evans*, 514 U.S. 1, 17–18 (1995) (O'Connor, J., concurring). EPIC has focused in particular on the need to safeguard the sensitive personal information that is routinely stored on a cell phone, a concern that the U.S. Supreme Court addressed favorably last term. *Riley v. California*, 134 S. Ct. 2473 (2014).

EPIC also works to protect student privacy. EPIC has proposed a Student Privacy Bill of Rights to safeguard student data and security,[2] obtained documents regarding the misuse of education records through the Freedom of Information Act,[3] and sued the Department of Education regarding changes in an agency regulation that diminished the safeguards set out in

[2] EPIC, Student Privacy Bill of Rights (2015), https://epic.org/privacy/student/bill-of-rights.html.
[3] EPIC, EPIC Uncovers Complaints from Education Department about Misuse of Education Records. (July 18, 2014), https://epic.org/2014/07/epic-uncovers-complaints-from.html.

the Family Educational Rights and Privacy Act, a federal student privacy law.[4]

SUMMARY OF THE ARGUMENT

This case concerns an issue of central importance to students across the country: whether schools may turn over to the police a student's cell phone without a warrant. The answer is simply "no." Cell phones provide access to detailed, sensitive personal information and should not be seized by the police without a warrant. If the police need to obtain a cell phone, the U.S. Supreme Court has made clear the answer: "get a warrant." *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

As the Supreme Court stated in *Tinker v. Des Moines Independent Community School Dist.*, students do not "shed their constitutional rights to freedom of speech or expression at the schoolhouse gate." 393 U.S. 503, 506 (1969). Nor do they shed their reasonable expectation of privacy. *See Commonwealth v. Damian D.*, 434 Mass. 725 (2001); *Commonwealth v. Snyder*, 413 Mass. 521 (1992). No court has granted blanket authority for law enforcement officers to

[4] *EPIC v. U.S. Dep't of Educ.*, 48 F.Supp. 1 (D.D.C 2014).

warrantlessly seize student property during the course of an ordinary criminal investigation, and this Court should not do so in this case for two reasons.

First, the Supreme Court has held that cell phones deserve enhanced protection under the Fourth Amendment, and should not be subject to the warrantless searches that have been allowed for physical objects found on a person. As the Supreme Court explained, "[c]ell phones, however, 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 considered in [*United States v.] Robinson* [414 U.S. 218 (1973)]." *Riley*, 134 S. Ct. at 2485. Cell phones are also now an integral part of social, professional, educational, and personal activities — particularly for students. The Supreme Court's rule in *Riley* that a warrant is required for the search of a cell phone extends to the cell phones carried by students in school. Therefore, if law enforcement needs to seize a student's cell phone in the temporary possession of school officials, a warrant must be obtained first.

Second, the adoption of school policies to regulate the reasonable use of electronic devices on campuses should not be construed to deprive students of their constitutional rights. School officials are understandably concerned with student education, safety, and order in the classroom. However, the seizure of valuable personal objects involves a long-term and permanent interference with an individual's use and enjoyment of their property. School policies cannot justify the conversion of student property and subsequent warrantless seizure by law enforcement without probable cause. Seizures conducted as part of a criminal investigation must be subject to judicial oversight through the warrant process.

ARGUMENT

I. Digital is different: The *New Jersey v. T.L.O.* standard for school searches does not apply to cell phones.

In *New Jersey v. T.L.O.*, the Supreme Court sought to "strike [a] balance between the schoolchild's legitimate expectations of privacy and the school's equally legitimate need to maintain an environment in which learning can take place." 469 U.S. 325, 340 (1985). *See also Damian D.*, 434 Mass. at 725. As a consequence, school officials need not seek a warrant

or have a level of suspicion that rises to probable cause prior to searching a student believed to be in possession of contraband. *T.L.O.*, 469 U.S. at 339-340. "Rather, the legality of a search of a student should depend simply on the reasonableness, under all the circumstances, of the search." *Id.* at 341.

The search in *T.L.O.* involved drug paraphernalia found in a student's pocketbook. While many personal items may be held in a pocketbook, the scope of that search simply does not compare with potential intrusion on privacy that results from the search and seizure of a cell phone. "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 2488-2489. Cell phones store massive amounts 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 stored in "the cloud."

In *Riley v. California*, the Supreme Court held that the traditional rule permitting searches of

physical items on a suspect incident to arrest could not be extended to searches of digital devices. *Id.* at 2494–2495. In reaching that conclusion, the Court focused on the unique nature of electronic devices and digital data and concluded that the intrusiveness of a search of digital data was significantly different from searches of physical objects. *Id.* at 2489. 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. *Id.* 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:

> [Apple's] iCloud Drive lets you access all your files from any device. With Family Sharing, all your photos, videos, music, and iTunes purchases can be shared easily with your family across multiple Apple devices. And iCloud Photo Library keeps every photo and video you take all in one place, and you can access them from your iPhone, iPad, iPod touch, Mac, or PC and on iCloud.com.

Apple, What is iOS 9 (2015).[5] The e-mail apps on Apple iOS and Android, the two most common mobile operating systems, are configured to download new messages whenever the user opens the app. See Apple, iPhone User Guide 58 (2015).[6]

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 (when you aren't connected to

---

[5] http://www.apple.com/ios/what-is/.

[6] *Available at* http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf. *See also* Google, Android Quick Start Guide 36 (2013), available at http://static.googleusercontent.com/media/www.google.com/en/us/help/hc/images/android/android_ug_42/Android-Quick-Start-Guide.pdf.

the Internet)." Salz & Moranz, The Everything Guide to Mobile Apps 15 (2013).

This model of computing is sometimes described as "cloud computing."[7] 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 open. *See* Apple, About Notifications on iPhone, iPad, and iPod Touch (2015).[8] 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

[7] For a brief description of cloud services, see Griffith, *What Is Cloud Computing?,* PC Magazine (Apr. 17, 2015), *available at* http://www.pcmag.com/article2/0,2817,2372163,00.asp.
[8] https://support.apple.com/en-us/HT201925.

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 door locks, possession of the cell phone could even provide intimate information to police about the activities of an individual within their home, without police ever obtaining a warrant to search the home. Cell phones provide access to detailed, sensitive personal information that should not be subject to warrantless police inspection.

B. Cell phones are nearly universal and teenagers, the generation most exposed to new technologies, are particularly dependent on cell phones.

In *Riley*, the Supreme Court also noted 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 they were an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484. Cell phones are ubiquitous in the United States. More than 92 percent of American adults own a

cell phone. Anderson, Technology Device Ownership: 2015, Pew Research Center (Oct. 2015).[9] Sixty-eight 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: 86 percent of those ages 18 to 29 have a smartphone, as do 83 percent of those ages 30 to 49. *Id.*

Cell phones are an increasingly important part of Americans' daily lives. Pew Research found that 10 percent of Americans own a smartphone but do not have broadband at home, and 15 percent own a smartphone but otherwise have a limited number of options for going online. Smith, U.S. Smartphone Use in 2015, Pew Research Center (Apr. 2015).[10] Americans no longer use their phones solely for calling each other but also to browse online and navigate important life activities. 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 (43 percent), look up government services or information

[9] http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015.
[10] http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

(40 percent) and take a class or get educational content (30 percent). *Id.* Forty-six percent of American adults say that their smartphone is something they "couldn't live without." *Id.*

Teenagers, in particular, are dependent on cell phones. In fact, in 2015, it is difficult to overstate the role of cell phones in teenagers' lives. Nearly three-quarters of teens have or have access to a smartphone and 30 percent have a basic phone. Lenhart, Teen, Social Media and Technology Overview 2015, Pew Research Center (Apr. 2015).[11] Just 12 percent of teens ages 13 to 17 say they have no cell phone of any type. *Id.* Fully 91 percent of teens go online using a mobile devices at least occasionally. *Id.* A typical teen sends and receives 30 texts per day. *Id.*

As schools have recognized the vital nature of cell phones to teenagers and their families, 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. Project Tomorrow

[11] http://www.pewinternet.org/files/2015/4/PI_TeensandTech_Update2015_0409151.pdf.

and Blackboard, Trends in Digital Learning: Empowering Innovative Classroom Models for Learning (June 2015).[12] Earlier this year, NYC ended its decade long ban on cell phones in schools, citing the need for parents to keep in touch with their children. Brody, Cell phone ban in NYC Schools to End, Wall Street Journal (Jan. 6, 2015).[13] This shift demonstrates how integral cell phones are in students' lives.

There is also a misconception that in today's world of information sharing on social media, teens do not care about privacy. Researcher danah boyd has found that teens do have a sense of privacy, and though it varies widely, their practices show that teens see privacy as a social norm. boyd and Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies 1-2 (2011).[14] When adults use

---

[12] http://www.tomorrow.org/speakup/2015_ClassroomModels.html.

[13] http://www.wsj.com/articles/cell phone-ban-in-nyc-schools-to-end-1420602754.

[14] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128. See also 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."); Molina, Protecting Data Privacy in Education in Privacy In Modern Age, 138, 143 (Marc Rotenberg et al. eds., 2015) ("Among the vulnerable are students with disabilities or

their power to violate teens' norms, using the accessibility of the information as justification, they "further marginalize young people, reinforcing the notion that they do not have the social status necessary to deserve rights associated with privacy." *Id.*

The modern cell phone provides access to the single greatest concentration of personal information available. For many users, information about their entire lives is accessible from their phones, and they depend on it to perform many day-to-day functions. This reliance means that an individuals' possessory interest in their phone is extremely strong. This is especially true for teenagers, who rely on their mobile devices to obtain information, communicate with family and friends, get a ride, and live their lives. It is not overstatement to suggest that there is no possession of greater value to a student than his or her cell phone.

---

special needs, who would like to control the disclosure of this information."); and Kaplan, Opt-Out: Protect Children, http://www.opt-out-now.info.

If law enforcement needs to seize a student's cell phone in the temporary possession of school officials, a warrant must be required.

II. The adoption of reasonable cell phone use policies by schools does not grant law enforcement officers the authority to deprive students of their personal property without a warrant.

School cell phone policies should not alter Fourth Amendment interests. In exercising a supervisory role, schools sometimes confiscate student personal property. Matchan, Schools Seeking Balance for Cell Phones in Class, Boston Globe (June 16, 2015).[15] *See also* Monfredo, Cell Phone Policy in Our Schools Needs to Be Discussed, GoLocalWorcester (Nov. 7, 2015).[16] As schools move away from outright bans of cell phones on school grounds, they are adopting electronic device policies giving school officials the ability to temporarily confiscate students' cell phones.

Some schools have strict no-use policies, while others take a "don't ask, don't tell" approach.

---

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

[16] http://www.golocalworcester.com/news/monfredo-cell-phone-policy-in-our-schools-needs-to-be-discussed.

Johnson, How to Manage Cell Phones in the Classroom, Edutopia (June 17, 2015).[17] Some teachers even integrate cell phone use into their lesson plans. Habib, What Parents Need to Know About Changing Cell Phone Policies in Schools, Tulsa World (Nov. 17, 2015).[18] But teachers and school administrators also recognize that students deserve fair notice of the restrictions placed on cell phone use and agree that policies should focus on preventing classroom distraction. Fullbright, Ph.D., Cell Phones in the Classroom: What's Your Policy?, Faculty Focus (Apr. 15, 2013).[19]

"It is beyond dispute that the Federal Constitution, by virtue of the Fourteenth Amendment, prohibits unreasonable searches and seizures by state officers." *T.L.O.*, 469 U.S. at 334 (quoting *Elkins v. United States*, 364 U.S. 206, 213 (1960)). *See also Commonwealth v. Considine*, 448 Mass. 295, 298-299

[17] http://www.edutopia.org/blog/how-manage-cell-phones-classroom-ben-johnson.
[18] http://www.tulsaworld.com/news/education/what-parents-need-to-know-about-changing-cell-phone-policies/article_4f848a03-03bd-52e7-9d84-13bcdf56e16f.html.
[19] http://www.facultyfocus.com/articles/effective-classroom-management/cell-phones-in-the-classroom-whats-your-policy/.

(2007). When a school deprives a student of her property and transfers possession to the police, the school exceeds its authority over a student's property. "[N]otwithstanding the legitimate goal of school administrators to maintain a safe learning environment, students continue to have a legitimate expectation of privacy in their persons and the items they bring to school." *Damian D.*, 434 Mass. at 727 (citing *T.L.O.*, 469 U.S. at 338–339). A school's difficult task of maintaining school discipline "is not so dire that students in the schools may claim no legitimate expectation of privacy." *T.L.O.*, 469 U.S. at 338.

When a teacher confiscates contraband based on reasonable suspicion, the police may be called and the evidence turned over. But cell phones are not contraband. A rule that permitted the police to obtain a student's cell phone without a warrant could be applied to all searches of all property involving all students. It would permit generalized searches, almost entirely unbounded.

In some circumstances, it may be appropriate for school administrators to require that a student temporarily turn over a cell phone in accordance with

a school policy, but seizure of the phone by the police is an entirely different matter and still requires a warrant. The Fourth Amendment, the Supreme Court's decision in *Riley*, and common sense make this requirement clear.

CONCLUSION

Amicus Curiae respectfully request this Court to deny Appellant's motion to reverse the decision of the lower court.

Respectfully submitted,

Marc Rotenberg (BBO# 550488)
Caitriona Fitzgerald (BBO# 673324)
Alan Butler
John Tran
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave. NW
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

November 23, 2015

Mass. R. A. P. 16(k) CERTIFICATION

I hereby certify that the above brief complies with the rules of court that pertain to the filing of briefs, including, but not limited to: Mass. R. A. P. 16(a)(6); Mass. R. A. P. 16(e); Mass. R. A. P. 16(f); Mass. R. A. P. 16(h); Mass. R. A. P. 18; and Mass. R. A. P. 20.

/s/
Caitriona M. Fitzgerald
BBO# 673324
Counsel for *amicus curiae* EPIC