No. S230923

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

THE PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff and Respondent,
v.
RICARDO P.
Defendant and Appellant,

APPLICATION FOR LEAVE TO FILE *AMICI* BRIEF AND PROPOSED BRIEF OF *AMICI CURIAE* ACLU OF NORTHERN CALIFORNIA, ACLU OF SOUTHERN CALIFORNIA, ACLU OF SAN DIEGO AND IMPERIAL COUNTIES, ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT AND APPELLANT RICARDO P.

AFTER A DECISION BY THE COURT OF APPEAL
FIRST APPELLATE DISTRICT, DIVISION ONE, CASE NO. A144149

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
Nicole A. Ozer (228643)
Matthew T. Cagle (286101)
Christopher J. Conley (290747)
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493
Facsimile: (415) 225-1478
Email: nozer@aclunc.org

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SAN DIEGO & IMPERIAL COUNTIES, INC.
David Loy (SBN 229235)
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121
Facsimile: (415) 436-9993
Email: davidloy@aclusandiego.org

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA, INC.
Peter Bibring (223981)
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500
Facsimile: (213) 977-5299
Email: pbibring@aclusocal.org

ELECTRONIC FRONTIER FOUNDATION
Lee Tien (148216)
Jennifer Lynch (240701)
Jamie Williams (279046)
815 Eddy Street
San Francisco, CA 93707
Phone: (415) 436-9333
Facsimile: (415) 436-9993
Email: tien@eff.org

Attorneys for *Amici Curiae*

No. S230923

IN THE SUPREME COURT OF THE STATE OF CALIFORNIA

THE PEOPLE OF THE STATE OF CALIFORNIA,
Plaintiff and Respondent,
v.
RICARDO P.
Defendant and Appellant,

APPLICATION FOR LEAVE TO FILE *AMICI* BRIEF AND PROPOSED BRIEF OF *AMICI CURIAE* ACLU OF NORTHERN CALIFORNIA, ACLU OF SOUTHERN CALIFORNIA, ACLU OF SAN DIEGO AND IMPERIAL COUNTIES, ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT AND APPELLANT RICARDO P.

AFTER A DECISION BY THE COURT OF APPEAL
FIRST APPELLATE DISTRICT, DIVISION ONE, CASE NO. A144149

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.
Nicole A. Ozer (228643)
Matthew T. Cagle (286101)
Christopher J. Conley (290747)
39 Drumm Street
San Francisco, CA 94111
Phone: (415) 621-2493
Facsimile: (415) 225-1478
Email: nozer@aclunc.org

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SAN DIEGO & IMPERIAL COUNTIES, INC.
David Loy (SBN 229235)
2750 5th Avenue #300
San Diego, CA 92101
Phone: (619) 232-2121
Facsimile: (415) 436-9993
Email: davidloy@aclusandiego.org

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF SOUTHERN CALIFORNIA, INC.
Peter Bibring (223981)
1313 West 8th Street
Los Angeles, CA 90017
Phone: (213) 977-9500
Facsimile: (213) 977-5299
Email: pbibring@aclusocal.org

ELECTRONIC FRONTIER FOUNDATION
Lee Tien (148216)
Jennifer Lynch (240701)
Jamie Williams (279046)
815 Eddy Street
San Francisco, CA 93707
Phone: (415) 436-9333
Facsimile: (415) 436-9993
Email: tien@eff.org

Attorneys for *Amici Curiae*

APPLICATION TO FILE AMICUS CURIAE BRIEF

Pursuant to California Rule of Court 8.520(f), the ACLU of Northern California, the ACLU of Southern California, the ACLU of San Diego/Imperial County, and the Electronic Frontier Foundation respectfully request leave to file a brief as amici curiae in support of Defendant-Appellant Ricardo P.[1]

The American Civil Liberties Union (ACLU) is a national, nonprofit, nonpartisan civil liberties organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in both the United States and California constitutions and our nation's civil rights law. It has three California affiliates: the ACLU of Northern California, the ACLU of Southern California, and the ACLU of San Diego & Imperial Counties. The California ACLU affiliates have a statewide Technology and Civil Liberties Project, founded in 2004, which works specifically on legal and policy issues at the intersection of new technology and privacy, free speech, and other civil liberties and civil rights.

---

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than amici ACLU of Northern California, ACLU of Southern California, ACLU of San Diego/Imperial County, and Electronic Frontier Foundation contributed money intended to fund preparing or submitting this brief.

The Electronic Frontier Foundation (EFF) is a San Francisco-based, member-supported, nonprofit civil liberties organization working to protect and promote fundamental liberties in the digital world. With more than 26,000 active donors and dues-paying members, EFF represents the interests of technology users in both court cases and broader policy debates surrounding the application of law in the digital age. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support privacy, civil liberties, free expression, and transparency in the information society.

Potential amici believe in—and have long advocated for—personal privacy and free expression, both of which are expressly protected by our state constitution, in the context of emerging technologies like the electronic devices and digital communications at issue in this case. Amici have advocated for privacy under Article I, Section 1 of the California Constitution in cases including *Sheehan v. San Francisco 49ers, Ltd.*, 45 Cal. 4th 992 (2009); *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1 (1994); *Brown v. Shasta Union High Sch. Dist.*, C061972, 2010 WL 3442147 (Cal. Ct. App. Sept. 2, 2010). Amici have also advocated for privacy under the federal constitution in *Riley v. California*, 134 S.Ct. 2473 (2014) and *United States v. Jones*, 132 S.Ct. 945 (2012). Amici have been involved in numerous cases regarding the appropriate scope of government

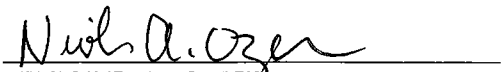
authority to conduct searches and challenging the validity of searches, including *Haskell v. Harris*, 745 F.3d 1269 (9th Cir. 2014) (en banc) (challenge to California statute requiring all felony arrestees to provide DNA samples) and *Offer Westort v. City and County of San Francisco* (S.F. Sup. Ct. No. CGC 13529730) (challenge to searches of arrestees' cell phones). Amici also co-sponsored the California Electronic Communications Privacy Act (CalECPA), Penal Code § 1564 *et seq.*, which requires California government entities to obtain a warrant before searching electronic devices or compelling access to electronic information.

Because this case concerns important questions regarding the scope of government authority, individuals' rights to be free from unreasonable searches, and the appropriate balance between the two, proper resolution of the matter is of significant concern to amici and their members. Amici believe their experience in these issues will make this brief of service to the Court. Potential amici therefore respectfully request that this Court grant them leave to submit the accompanying brief. *See* Rule of Ct. 8.520(f).

Respectfully submitted,

Dated: October 19, 2016

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.

By: 
NICOLE A. OZER

ELECTRONIC FRONTIER FOUNDATION

By: _____
LEE TIEN

Attorneys for *Amici Curiae* ACLU of Northern California, ACLU of Southern California, ACLU of San Diego and Imperial Counties, and Electronic Frontier Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Publications and Scholarly Articles

Electronic Media

Other Authorities

I. INTRODUCTION

The price of any youthful transgression cannot be that the government has an all-access, long-term pass to your private life that chills access to the supportive communities and rehabilitative services that will help you build a healthy and productive future. But that is precisely what the government is asking for with the expansive electronic search condition at issue in this case.

This Court should hold that such a condition fails the third prong of the *Lent* test and is therefore invalid. Amici agree with Appellant that the probation condition fails the third prong of *Lent* because no nexus exists between electronics usage and the underlying offense or future criminality. But the purpose of this brief is to focus this Court's attention on two additional reasons why the electronic search condition is not "reasonably" related to future criminality and must fail the *Lent* test.

First, the search condition here is unreasonable because it authorizes overly broad access to deeply personal information, including communications content. By allowing the government access to a young person's electronic devices, remotely stored digital information, and account passwords, the condition effectively gives the government unlimited access to "the sum" of a young person's life, including highly sensitive and constitutionally protected information about topics such as her sexual orientation. The search condition extends far beyond the scope of

traditional physical searches, making it functionally equivalent to a wiretap, which would be unprecedented as a probation condition.

Second, the condition undermines, rather than supports, the rehabilitative purpose of probation by chilling young people's access to digital services and programs to support rehabilitation and by disincentivizing third parties from providing a supportive, rehabilitative environment. Young people, particularly young people from vulnerable communities who are disproportionately represented in the juvenile justice system, rely on electronic devices and communication to access critical information, to build essential connections, and to obtain important support and services, all of which further the rehabilitative purpose of probation. The condition here is unreasonable because it is likely to discourage precisely these beneficial activities.

If the Court of Appeal's misinterpretation of the *Lent* test were left to stand, there would be no meaningful limitation on the government's ability to conduct invasive electronic probation searches. Tens of thousands of California's young people are placed on probation every year. More and more of these young people would likely find themselves subject to a broad electronic search condition, regardless of how minor their transgressions or how attenuated these transgressions are to the use of electronic devices or digital communications. They would be forced to choose between using modern technology to connect and seek needed support for rehabilitation on

one hand, and safeguarding their private lives and free expression on the other. This cannot be right.

Instead, this Court should recognize, as the United States Supreme Court did in *Riley v. California*, that properly safeguarding constitutional rights requires taking into account the quantitative and qualitative impact of modern technology, rather than "mechanical[ly]" applying pre-digital legal rules to electronic searches. 134 S. Ct. 2473, 2484 (2014). Following that guidance, this Court should analyze the condition at issue in the full context of the expansive nature of electronic searches, the robust California constitutional rights to privacy and free expression, and the core rehabilitative goals of juvenile probation. After doing so, this Court should find that the electronic search condition is unreasonable, that it fails the third prong of the *Lent* test, and that the juvenile court erred in imposing it on Appellant.

II. ARGUMENT

Under the *Lent* test established by this Court, a probation condition is valid unless it "(1) has no relationship to the crime of which the offender was convicted, (2) relates to conduct which is not in itself criminal, and (3) requires or forbids conduct which is not reasonably related to future criminality." *People v. Lent*, 15 Cal. 3d 481, 486 (1975) (quoting *People v. Dominguez*, 256 Cal. App. 2d 623, 627 (1967)). In the present case, the question before this Court is whether the electronic search condition is "reasonably related to future criminality" and passes muster under the third prong of *Lent*. It fails this test.

Juvenile courts are only authorized to impose "reasonable" conditions of probation. Cal. Welf. & Inst. Code § 730(b); *see People v. Olguin*, 45 Cal. 4th 375, 383 (2008) (when evaluating a probation condition, "the relevant test is *reasonableness*. . . .") (citations omitted). This reasonableness should be determined in light of the purpose of juvenile probation, which is rehabilitation. *See* Cal. Welf. & Inst. Code § 730(b) (probation conditions must be "fitting and proper to the end that . . . the reformation and rehabilitation of the ward [is] enhanced."); *Olguin*, 45 Cal. 4th at 380 (conditions of probation, including those that promote supervision, should "assure that the probation serves as a period of genuine rehabilitation") (citation omitted). This requires considering the secondary effects of a sweeping probationary search on these rehabilitative goals. *See People v.*

Robles, 23 Cal. 4th 789, 799 (2000) (allowing police to effectuate warrantless searches on cohabitants of probationers might cause "many law-abiding citizens . . . not to open their homes to probationers," leading to "higher recidivism rates and a corresponding decrease in public safety."); *In re Jaime P.*, 40 Cal. 4th 128, 138 (2006) (lack of restrictions on the search would "invite repeated harassment and arbitrary searches"). Particular scrutiny is appropriate for "[a] probation condition that imposes limitations on a person's constitutional rights." *In re Sheena K.*, 40 Cal. 4th 875, 890 (Cal. 2007); *cf. Olguin*, 45 Cal. 4th at 384 ("We do not apply such close scrutiny in the absence of a showing that the probation condition infringes upon a constitutional right.").

Evaluating the reasonableness of the electronic search condition at issue in this case requires recognizing the vast quantity of personal information that the condition could impact or expose. For this reason, courts, including the U.S. Supreme Court, have recognized the need for particular diligence to protect the significant privacy and speech interests in electronic devices and the communications and information stored on or accessible through these devices, even in contexts like probation where an individual's general expectation of privacy may be reduced.

In the present case, the lack of a nexus between the electronic search condition and the offense or future criminality is sufficient to invalidate the condition under *Lent*. However, there are two additional reasons that the

condition at issue is unreasonable. First, the condition's scope is unreasonably broad, allowing access to deeply personal information, including communications content.[2] In fact, the searches it authorizes have much more in common with wiretaps than traditional physical searches. And second, the condition does not merely fail to reasonably advance the rehabilitative purpose of juvenile probation, it actually undermines that purpose: it both deters the young person from forming relationships and seeking rehabilitative support or services through his electronic devices and discourages others from connecting with the young person and providing a supportive rehabilitative environment.

A. Young people, especially those from vulnerable populations, rely on electronic devices to access essential services and rehabilitative support.

Electronic devices and information are indispensable to modern life. As the U.S. Supreme Court recognized, "[n]ow it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Riley*, 134 S. Ct. at 2490. The proliferation of electronic devices has gone hand in hand with an increase in the use of digital communication and online

---

[2] The condition imposed by the juvenile court allows the government to search electronic devices, access data stored remotely, and demand device and account passwords. *In re Ricardo P.*, 241 Cal.App.4th 676, 681 & n. 6. The appeals court suggested the juvenile court formulate a slightly narrower condition, but that suggestion still contemplated access to "text and voicemail messages, photographs, e-mails, and social media accounts." *Id.* at 692–93.

accounts. These devices and services allow young people, especially those in vulnerable communities, to access information and find the resources they need to build supportive environments and transition out of the juvenile justice system.

Young people are particularly likely to use mobile devices and online services to connect and seek information. Over 88% of American teenagers have access to a cell phone, 73% of teenagers have access to a "smartphone," and 58% of teenagers have access to a tablet.[3] Texting has become the dominant daily mode of communication for young people.[4] Ninety percent of young adults in the United States use social media websites to connect with others and communicate online.[5] Cell phones and other mobile devices have become a primary driver of teen Internet use: 91% of teenagers go online from mobile devices, and 94% of these "mobile teens" go online daily or more often.[6]

---

[3] Amanda Lenhart, *A Majority of American Teens Report Access to a Computer, Game Console, Smartphone and a Tablet*, Pew Research Center (Apr. 9, 2015), http://www.pewinternet.org/2015/04/09/a-majority-of-american-teens-report-access-to-a-computer-game-console-smartphone-and-a-tablet.

[4] Monica Anderson, *How Having Smartphones (or not) Shapes the Way Teens* Communicate, Pew Research Center (Aug. 20, 2016), http://www.pewresearch.org/fact-tank/2015/08/20/how-having-smartphones-or-not-shapes-the-way-teens-communicate/.

[5] Andrew Perrin, *Social Media Usage: 2005-2015*, Pew Research Center, 2–3 (2015), http://www.pewinternet.org/files/2015/10/PI_2015-10-08_Social-Networking-Usage-2005-2015_FINAL.pdf.

[6] Amanda Lenhart, *Teens, Social Media, & Technology Overview 2015*,

Young people from vulnerable communities, who are overrepresented in the juvenile justice system,[7] are often particularly reliant on electronic devices and online information. For example, mobile phones are the only means of Internet access for many poor youth.[8] African American youth, who comprise 13% of California's youth population but 32% of juveniles on probation,[9] use smartphones to seek help with homework more often than white students.[10] Over 80% of LGBTQ youth, who comprise between 13 and 15% of young people in the juvenile justice system, [11] search the

---

Pew Research Center, 2 (2015), http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf.

[7] *See generally* Tamar R. Birckhead, *Delinquent by Reason of Poverty*, 38 Wash. U.J.L. & Policy, 53 (2012); *Disproportionate Minority Contact*, Nat'l Conf. of St. Leg., 1, 3 (2010), http://www.ncsl.org/documents/cj/jjguidebook-dmc.pdf (Sixty-nine percent of youth detained by law enforcement are minority youth, who comprise only 41% of the overall youth population).

[8] *See* Victoria Rideout & Vikki Katz, *Opportunity for All? Technology and Learning in Lower-Income Families*, The Joan Ganz Cooney Center at Sesame Workshop, 1, 5 (2016), http://digitalequityforlearning.org/wp-content/uploads/2015/12/jgcc_opportunityforall.pdf. ("One quarter (23%) of families below the median income level and one third (33%) of those below the poverty level rely on mobile-only Internet access.").

[9] *Disproportionate Minority Contact*, *supra* note 7, at 3.

[10] *Young Teens in U.S. Use Mobile Devices for Homework*, Reuters (Nov. 28, 2012), http://www.reuters.com/article/us-technology-tweens-mobiles-homework-idUSBRE8AR1DC20121128 ("Smartphones were used by . . . 42 percent of African-Americans and 36 percent of whites. . . .").

[11] *LGBTQ Youths in the Juvenile Justice System*, Office of Juvenile Justice and Delinquency Prevention, Literature Review, 1, 2 (2014), http://www.ojjdp.gov/mpg/litreviews/LGBTQYouthsintheJuvenileJusticeSystem.pdf.

Internet for health-related information and support services.[12] And many survivors of sexual assault, who make up 56% of all girls in the California juvenile justice system,[13] find support in online communities.[14]

The rehabilitative and support services that young people access through electronic devices are an important part of helping them to lead healthy and productive lives. Text messaging programs have successfully encouraged low-income young people to stay in school[15] and access needed health information and clinical and social services.[16] Other online services help young people cope with mental health issues, including suicide and

---

[12] *Out Online: The Experiences of Lesbian, Gay, Bisexual, and Transgender Youth,* GLSEN (July 10, 2013), http://www.glsen.org/press/study-finds-lgbt-youth-face-greater-harassment-online.

[13] Malika Saada Saar et al., *The Sexual Abuse to Prison Pipeline: The Girls' Story*, Rights4Girls, 1, 5 (2015), http://rights4girls.org/wp-content/uploads/r4g/2015/02/2015_COP_sexual-abuse_layout_web-1.pdf.

[14] *See, e.g.*, *After Silence Home Page*, http://www.aftersilence.org/ (last visited Oct. 16, 2016) ("Our mission is to support, empower, validate, and educate survivors [of sexual assault] as well as their families and supporters. The core of our organization is a support group . . . where victims and survivors come together online in a mutually supportive and safe environment.").

[15] *See e.g.*, Benjamin L. Castleman & Lindsay C. Page, *Summer Nudging: Can Personalized Text Messages and Peer Mentor Outreach Increase College Going Among Low-Income High School Graduates?*, Ctr. on Educ. Policy and Workforce Competitiveness, 1, 2 (2013), http://curry.virginia.edu/uploads/resourceLibrary/9_Castleman_SummerTextMessages.pdf.

[16] *See e.g.*, Deb Levine, *Using New Media to Promote Adolescent Sexual Health: Examples from the Field*, ACT for Youth Center of Excellence (2009), http://www.actforyouth.net/resources/pm/pm_media_1009.pdf.

depression.[17] Online support communities also provide an important place for LGBTQ teens to discuss their sexuality and seek support for experiences with harassment and discrimination.[18] Text messaging interventions developed by the University of California, Los Angeles help young people stay off drugs, reducing relapse by as much as half as compared to standard aftercare.[19] The Court Messaging Project, developed at Stanford University, uses text messages to help young people navigate the juvenile justice system and stay out of trouble.[20]

---

[17] Crisis Text Line, for example, provides free, anytime crisis support. Crisis Text Line, http://www.crisistextline.org/faq/ (last visited Oct. 4, 2016). More than 18.5 million messages have been exchanged since August 2013, with 80% of texters reporting being under age 25. Ina Fried, *Crisis Text Line Gets $23.8 Million from Tech A-Listers*, Recode (June 23, 2016), http://www.recode.net/2016/6/15/11950608/crisis-text-line-23-million-funding. Another service, IM Hear offers "an online teen chat service which provides confidential peer support . . . to teens who are struggling with feelings of depression, loneliness, and stress." IM Hear, Samaritans, http://samaritanshope.org/im-hear/ (last visited Oct. 16, 2016).

[18] *See* LGBTeens, Reddit (last visited Oct. 4, 2016), http://www.reddit.com/r/lgbteens ("A place where LGBT teens and their surrounding peoples can find support and love!"); *LGBT Youth Help and Support – Jovenes LGBT Ayuda y Apoyo*, Facebook (last visited Oct. 4, 2016), https://www.facebook.com/groups/LGTBPEOPLE/. *See also Out Online*, *supra* note 12 ("Over 50% of LGBT individuals use the Internet to meet new friends and relate to people like them.").

[19] *Text Messaging Aftercare Intervention Cuts Youths' Risk for Relapse*, Nat'l Inst. on Drug Abuse (June 30, 2015), https://www.drugabuse.gov/news-events/nida-notes/2015/06/text-messaging-aftercare-intervention-cuts-youths-risk-relapse.

[20] *The COURT MESSAGING Project*, Legal Design Lab, http://www.legaltechdesign.com/CourtMessagingProject/ (last visited Oct. 16, 2016).

Electronic devices also help young people foster social connections that help them integrate into society. For example, young people who communicate digitally are more likely to engage in civic activities,[21] which has been shown to have a positive impact on reducing recidivism.[22]

B. Electronic devices store and allow access to enormous amounts of personal information.

Modern electronic devices have "immense storage capacity" and may contain a staggering amount of sensitive personal information. *Riley v.* 134 S. Ct. at 2489. The *smallest* storage capacity available on a new iPhone is 16 gigabytes ("GB") (16 billion bytes),[23] enough for nearly 4,000 digital

---

[21] Wenjin Xie, *Social Network Site Use, Mobile Personal Talk and Social Capital Among Teenagers*, 41 Comput. In Hum. Behav. 228, 232 (2014), https://www.researchgate.net/publication/267159988_Social_network_site_use_mobile_personal_talk_and_social_capital_among_teenagers (last visited Oct. 16, 2016) ("[R]esults indicate that SNS adoption and mobile personal talk can not only increase teenagers' close ties with friends, but also jointly promote teenagers' civic engagement").

[22] *Do Interactions with the Criminal Justice System Have Civic Effects?*, CIRCLE, (2011), http://civicyouth.org/wp-content/uploads/2011/06/v8.i2.5.pdf ("[C]ivic participation can be a preventive force against arrest and interaction with the criminal justice system. . . . offending among YouthBuild graduates decreased and educational outcomes increased").

[23] The iPhone SE is the only current model available with as little as 16 GB of storage; all other current iPhone models come with at least 32 GB of storage. *See Compare iPhone Models*, Apple, http://www.apple.com/iphone/compare/ (last visited Oct. 16, 2016). The iPhone 5, which was released in 2012, also came with a minimum of 16 GB of storage. *See iPhone 5,* Wikipedia, https://en.wikipedia.org/wiki/IPhone_5 (last visited Oct. 4, 2016).

pictures,[24] over 260,000 private voicemails,[25] hundreds of home videos,[26] or 800 million words of text[27]—well over a football field's length of books.[28] Even "feature phones"[29] can hold a variety of information, including months or even years of text messages, thousands of contacts, calendars, "to do" lists, call history, photographs, and more. *See Riley*, 134 S. Ct. at 2489. And laptop and desktop computers may have far larger storage capacities, with companies now offering ten terabyte (ten trillion

---

[24] Assuming each photo is taken at the native 12 megapixel resolution, a 16 GB device could hold roughly 3,814 photos. *Number of Pictures That Can Be Stored on a Memory Device*, SanDisk, http://perma.cc/J7JW-7AC7 (last visited Oct. 4, 2016).

[25] Assuming each voicemail lasts 30 seconds and is recorded at a bit rate of 16 kbps, a 16 GB device could hold over 266,666 voicemails.

[26] Assuming each home video is thirty seconds long, recorded at standard definition, 16 GB could store 480 such videos. *See* Derek Fung, *What Storage Should I Get in My Camcorder?,* CNET Australia (Sept. 23, 2009), http://perma.cc/QHX9-KNQ6.

[27] *See* Ryan, *The Amazing History of Information Storage: How Small Has Become Beautiful, Statistical Trends & Numbers*, Statistical Trends & Numbers, (Aug. 30, 2012), http://www.numbersleuth.org/trends/the-amazing-history-of-information-storage-how-small-has-become-beautiful/ (noting that the complete 2010 Encyclopedia Britannica, which contains 32 volumes, weighs 129 pounds in physical form, and contains 50 million words, could fit in a single gigabyte of data).

[28] An American football field, including end zones, is 120 yards long. Since "1 Gigabyte could hold the contents of about 10 yards of books on a shelf," 16 GB would correspond to about 160 yards of books. *Megabytes, Gigabytes, Terabytes . . . What Are They?*, What's a Byte, http://perma.cc/8AAW-MVZQ (last visited Oct. 18, 2016).

[29] Feature phones usually contain "a fixed set of functions beyond voice calling and text messaging, but [are] not as extensive as a smartphone." *Definition of: Feature Phone*, PC Magazine Encyclopedia, http://www.pcmag.com/encyclopedia/term/62894/feature-phone (last visited Oct. 18, 2016).

byte) hard drives capable of storing nearly 600 times as much data as a 16 GB iPhone.[30]

Electronic devices can store a wide range of additional types of data, such as location information, that can reveal sensitive details about their users. Modern mobile devices often use Global Positioning System ("GPS") data or other mechanisms to determine their location whenever the device is turned on,[31] and then retain an archive of that data, providing a detailed record of the individual's movements.[32] And many electronic devices, including smartphones,[33] can also generate and store numerous

---

[30] *See* Brooke Crothers, *New 10 TB Hard Drive Will Take You Forever to Fill*, Fox News Tech, (July 21, 2016), http://www.foxnews.com/tech/2016/07/21/new-10-tb-hard-drive-will-take-forever-to-fill.html.

[31] Location information is used in many common phone applications, including map or ridesharing applications. *See e.g.*, *User Privacy Statement*, Uber, https://www.uber.com/legal/privacy/users/en/ (last visited Oct. 16, 2016) ("Location Information: When you use the Services for transportation or delivery, we collect precise location data about the trip from the Uber app used by the Driver.").

[32] *See* Charles Arthur, *iPhone keeps record of everywhere you go*, The Guardian (Apr. 20, 2011), https://perma.cc/Y2GA-8FBA. Moreover, cell phone companies also store location data for extended periods, often years. *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, (2010), http://perma.cc/J2R7-9N6B.

[33] *See Riley*, 134 S. Ct. at 2489 ("The term 'cell phone' is itself misleading shorthand [for] minicomputers that also happen to have the capacity to be used as a telephone").

other kinds of information created by various "apps," including medical information[34] and financial information.[35]

Electronic devices also often provide a direct path to data generated or stored remotely, including data associated with online accounts.[36] Web-based email accounts can contain a rich archive of personal communications extending years or even decades into the past.[37] Social media services, such as Facebook, Twitter, or Instagram, can expose extensive information about activities and reveal personal thoughts, concerns, and communications, whether via private "direct" user-to-user messages or via posts on private message boards. Indeed, for many, social

---

[34] *See, e.g.*, *Apple Health*, Apple, (last visited Oct. 5, 2016), https://www.apple.com/sg/ios/health/ ("The Health app . . . makes it easy to keep tabs on a wide array of data that matters to you — from measurements of your blood pressure and blood glucose to records of your weight and reproductive health."); Fitbit App Home Page, https://www.fitbit.com/app (last visited Oct. 5, 2016) (describing how the app enables users to "[v]iew progress towards your daily goals for steps, distance, calories burned and active minutes, and see your trends over time").

[35] Jill Duffy, *Best Mobile Finance Apps*, PC Magazine, (Apr. 20, 2016), https://perma.cc/Y96T-Q3QM.

[36] All parties have agreed that the condition imposed by the juvenile court was intended to encompass online account access as well as access to information stored directly on the electronic device. *In re Ricardo P.*, 241 Cal.App.4th at 682.

[37] For example, Google offers 15 GB of storage across its various services including Gmail for free. Assuming an average of 75 kilobytes/email, 15 GB of storage would hold 200,000 emails. *See Bringing It All together: 15 GB now shared between Drive, Gmail, and Google+ Photos*, Google Drive Blog, (Oct. 4, 2016), https://drive.googleblog.com/2013/05/bringing-it-all-together-15-gb-now.html.

media accounts function as a modern-day diary.[38] Applications can also link to other sources of information, such as a live video feed from a third party[39] or even a home security camera.[40] In many cases, these services are accessible from a young person's electronic device with just a click of a mouse or a tap on a screen.

In total, electronic devices can store "not only [] many sensitive records previously found in the home [but also] a broad array of private information never found in a home in any form—unless the [device] is." *Riley*, 134 S. Ct. at 2491.

---

[38] Jess Zimmerman, *Social Media Is Our Modern Diary. Why Do Tech Companies Own All The Keys?*, The Guardian, (Oct. 21, 2014), https://www.theguardian.com/commentisfree/2014/oct/21/social-media-tech-companies-user-privacy; *cf.* Diary, *Merriam-Webster*, (2016) http://www.merriam-webster.com/dictionary/diary (defining "diary" as "a record of events, transactions, or observations kept daily or at frequent intervals").

[39] For example, the popular video sharing app Periscope allows users to create a private broadcast to a select list of followers. *How Do I Make My Broadcast Private?*, https://help.periscope.tv/customer/portal/articles/2016181-how-do-i-make-my-broadcast-private- (last visited Oct. 13, 2016).

[40] *See, e.g.*, *Meet Nest Cam Indoor*, Nest, https://nest.com/camera/meet-nest-cam/ (last visited Oct. 16, 2016) (describing the Nest Cam Indoor security camera and its accompanying app, which enables users to remotely view a high definition live video stream from their camera and "look after [their] home and family – even when . . . away.")

C. The electronic search condition is unreasonable because it allows unlimited access to vast amounts of sensitive personal information.

The electronics search condition at issue is unreasonable under the *Lent* test because it gives the government unfettered access to a young person's electronic information and online accounts. It dramatically infringes on the constitutional rights of a young person by authorizing the government to search communications without limits on the scope or manner. The scope of a search under the condition at issue is far greater than that of any physical search, allowing access to a vast trove of communications, activity logs, and more. The potential for comprehensive, even real-time, search under the probation condition is functionally equivalent to a wiretap, yet we know of no case that has upheld suspicionless telephonic wiretaps of probationers, adult or juvenile. The invasiveness of searches permitted by the condition weighs heavily in favor of finding the condition unreasonable and thus invalid.[41]

---

[41] In addition, it is doubtful that this defect can be remedied by placing simple limits on an otherwise-unreasonable electronic search condition. For instance, simply disconnecting the device from the Internet (e.g. by placing a mobile device in "airplane mode") may not effectively protect third parties' sensitive information from probation searches. *See In re Malik J.*, 240 Cal. App. 4th 896, 903 (2015). In fact, many devices and applications (including Facebook and other social networking services) automatically download information precisely so that the information is available even if the device is disconnected from the Internet. *Cf. Riley*, 134 S. Ct. at 2491 ("Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.") (internal citations omitted).

1. The condition infringes on a young person's right to privacy by authorizing searches far broader and more invasive than any physical search.

The Fourth Amendment requires this Court to take into account the sensitivity as well as the sheer volume of information laid bare by the condition to fully assess if it is reasonable. *See* generally *Riley*, 134 S. Ct. at 2489. By allowing government access to both a wide range of communication channels and a broad array of very sensitive information, the condition unreasonably burdens the "substantial" privacy interest that probationers retain in their electronic devices and information. *United States v. Lara*, 815 F.3d 605, 612 (9th Cir. 2016).

Federal courts, including the U.S. Supreme Court, have increasingly recognized that electronic searches may be unreasonable, and thus unconstitutional, even if they seem to satisfy pre-existing doctrine allowing for warrantless searches, because of the qualitatively different privacy interest at stake in a digital search. In *Riley v. California*, the U.S. Supreme Court unanimously held that the warrantless search of a cell phone found in an arrestee's possession violated the Fourth Amendment. 134 S. Ct. at 2495. In doing so, the Court conducted a thorough analysis of the unique nature of digital devices and the privacy interests associated with their contents. It concluded that the capacity to hold vast quantities of different types of highly personal information makes them "quantitative[ly] *and*

qualitative[ly]" different from their physical counterparts.[42] *Id.* at 2489 (emphasis added).

Similarly, in *United States v. Jones*, five Justices recognized that the collection of extensive location records through technological means implicates the Fourth Amendment and could constitute an unreasonable search even where traditional visual observation by officers would not. 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment); *id.* at 955–56 (Sotomayor, J., concurring). As Justice Alito noted, "[s]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring in the judgment).

In addition, the Sixth Circuit, the only Court of Appeals to consider the issue, held that searching an online email account without a warrant violated the Fourth Amendment. *See United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The court's decision turned on the invasive nature of a search of an online account: "'[A]ccount' is an apt word for the conglomeration of stored messages that comprises an email account, as it

---

[42] In fact, the U.S. Supreme Court chided the government for its claim that a search of a cell phone was "materially indistinguishable" from a traditional search incident to arrest: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 134 S. Ct. at 2488–89.

provides an account of its owner's life." *Id.* at 284. The *Warshak* court recognized that constitutional protections "must keep pace with the inexorable march of technological progress, or [their] guarantees will wither and perish." *Id.* at 285.

Two courts that have applied *Riley* to the probation context have also recognized that the unique attributes of digital devices and information require a careful analysis of the invasiveness of an electronic search rather than mechanical acceptance that "standard" search conditions may encompass electronic devices. In *United States v. Lara*, the Ninth Circuit rejected the government's contention that a warrantless search of a probationer's cell phone was justified by a general search condition and a claim that "drug traffickers commonly use cell phones to arrange narcotics sales." 815 F.3d at 607–08, 612. Instead, the court held that the defendant's "substantial" privacy interest in his cell phone and the information it contained, although "somewhat diminished" by his status as a probationer, nonetheless outweighed the government's interest in enforcing a probation condition generally applicable to physical property and containers. *Id.* at 611–612. And in *People v. Appleton*, the Sixth Appellate District invalidated an electronic search condition that "would allow for searches of vast amounts of personal information unrelated to defendant's criminal conduct or his potential for future criminality." 245 Cal. App. 4th 717, 727 (2016). The *Appleton* court, following *Riley*, observed how the "scope of a

digital search is extremely wide," sweeping more broadly than the "standard" condition allowing for searches of persons, vehicles, and homes. *Id.* at 726. As a result, the condition would "potentially expose . . . medical records, financial records, personal diaries, and intimate correspondence with family and friends," much of which may be unrelated to the offense or future criminality. *Id.* at 725. The First District has likewise held that electronic search conditions must be carefully evaluated under the reasoning in *Riley*. *In re Malik*, 240 Cal. App. 4th 896, 902 (2015) ("In view of these significant privacy implications [highlighted by *Riley*], the electronics search condition must be modified . . . .").

The electronic search condition here allows access to the same scope and detail of records that led the *Riley* court and others to find electronic searches unreasonable. It authorizes access to a vast trove of information, including both direct communications like email and text messages and indirect information sharing on social networks and forums. *See supra* Part II.B. Moreover, the search condition encompasses many types of sensitive private information: location records that can "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building" and thus expose "'a wealth of detail about her familial, political, professional, religious, and sexual associations'"; web browsing history that could reveal "a search for certain symptoms of disease"; and application data that "can form a revealing montage of the

user's life," from how she "plan[s] [her] budget" to the fact that she is "tracking pregnancy symptoms." *Riley*, 134 S. Ct. at 2490 (quoting *Jones*, 132 S.Ct. at 955 (Sotomayor, J. concurring)).

In sum, the condition at issue would authorize searches that

> would typically expose to the government far *more* than the most exhaustive search of a house: [An electronic device] not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the [device] is.

Id. at 2491. This places a severe burden on the substantial privacy interest that a young person on probation retains in his electronic devices and information.

2. The condition allows access to information that is protected by the California Constitution.

Electronic searches also directly implicate the motivating factors behind California's protections for privacy, which this Court has long construed to afford even greater protection than the Fourth Amendment.[43] The Privacy

---

[43] *See People v. Brisendine*, 13 Cal. 3d 528, 548-552 (1975) (rejecting *United States v. Robinson*, 414 U.S. 218 (1973) and holding that California citizens are entitled to greater protection under Article I § 13 of the California Constitution against unreasonable searches and seizures than that required by the United States Constitution). Although 1983 California constitutional amendment Proposition 8 eliminated exclusionary rule as remedy for violations of this provision, its "substantive scope ... remains unaffected" by that initiative. *In re Lance W.*, 37 Cal.3d 873, 886-87 (1985). *Brisendine* and its progeny therefore remain good law except to the extent they require exclusion of evidence. *See also People v. Mayoff*, 42 Cal. 3d 1302, 1313 (1986) (rejecting *California v. Ciraolo*, 476 U.S. 207

Amendment to Article 1, Section 1 of the California Constitution, which protects the privacy rights of "all people," was passed in response to the "modern threat to personal privacy" posed by then-emerging data collection technology. *White v. Davis*, 13 Cal. 3d 757, 774 (1975). This Court has consistently held that the constitutional protection applies rigorously to collections that comprise a "virtual current biography." *People v. Blair*, 25 Cal. 3d 645, 652 (Cal. 1979). Information accessible via electronic devices has an "element of pervasiveness" that directly implicates the same concerns: it comprises "a digital record of nearly every aspect of [possessors'] lives—from the mundane to the intimate." *Riley*, 134 S. Ct. at 2490.

Courts, including this Court, have specifically held that the right to privacy in the California Constitution protects communications information that can reveal sensitive information about Californians' private lives. In *People v. Blair*, this Court held that the state constitution requires that police obtain a warrant to access a defendant's phone records, rejecting the

---

(1986) and *Dow Chemical v. United States*, 476 U.S. 227 (1986) to find expectation of privacy in backyard visible via aerial surveillance); *People v. Krivda*, 5 Cal. 3d 357 (1971) (finding expectation of privacy in trash left for collection under state constitution even though *California v. Greenwood*, 486 U.S. 35 (1988), found no expectation of privacy under Fourth Amendment); *Burrows v. Superior Court*, 13 Cal. 3d 238 (1974) (expectation of privacy in bank records under California constitution even though *United States v. Miller*, 425 U.S. 435 (1976), found none under Fourth Amendment).

federal "third party doctrine" that placed such records outside the scope of the Fourth Amendment. 25 Cal. 3d at 653, 655; *see Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a telephone subscriber does not have a Fourth Amendment interest in telephone records held by the phone company). And in *People v. Chapman*, this Court extended that reasoning to a telephone customer's contact information. 36 Cal. 3d 98, 108 (Cal. 1984). More recently, a federal court recognized that this protection most logically extends to cell phone location information. *In Re: Application for Telephone Information Needed for a Criminal Investigation Case*, No. 15–XR–90304–HRL–1(LHK) (N.D. Cal. July 29, 2015) ("There is little doubt that the California Supreme Court's holding [in *Blair*] applies with full force to the government's application here, which seeks historical CSLI generated by a target cell phone's every call, text, or data connection, in addition to any telephone numbers dialed or texted.").

The California Constitution also includes an express right to freedom of expression that is "in some ways is broader than [] the comparable provision of the federal Constitution's First Amendment." Cal. Const. Art. 1, § 2; *Beeman v. Anthem Prescription Management, LLC*, 58 Cal. 4th 329, 341 (Cal. 2013) (quoting *Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 959 (Cal. 2002)). As this Court observed in *White v. Davis*, government monitoring may "run afoul of the constitutional guarantee [to free speech] if the effect of such activity is to chill constitutionally protected activity." 13 Cal. 3d at

767 (holding the government's covert surveillance threatened a "substantial inhibition" of free speech and thus presumptively violated the federal and state Constitutions).

California has further safeguarded the robust privacy and free speech rights guaranteed to all people by placing specific limits on government access to electronic information and communications. The California Reader Privacy Act, which went into effect on January 1, 2012, generally prohibits any provider from knowingly disclosing or being compelled to disclose a broad range of personal information without a court finding that there is probable cause to believe the personal information is relevant to the investigation of an offense. Cal. Civ. Code § 1798.90 *et seq*. And the California Electronic Communications Privacy Act ("CalECPA"), which went into effect on January 1, 2016, generally requires a government entity to obtain a warrant to access or obtain any "electronic device information" from an electronic device or to compel the disclosure of "electronic communication information" from a provider. Cal. Pen. Code § 1546 *et seq*. The definition of electronic device information in CalECPA is "comprehensively broad" and "include[s] any information that exists on any electronic device" including information held by service providers.[44]

---

[44] *State and Local Agency Access to Customer Information from Communication Service Providers (2015 Legislation and Next Steps)*, Cal. Law Rev. Comm'n, 7, (Nov. 25, 2015), http://www.clrc.ca.gov/pub/2015/MM15-51.pdf.

California's privacy protections, both constitutional and statutory, follow the same reasoning as *Riley*: the invasiveness of government access to detailed and sensitive records about a person's life is a key factor in determining when such access should be permitted, or whether it should be permitted at all. There can be no question that the protections extend to information held on electronic devices, since searches of these devices provide the government with precisely the sort of all-encompassing, "cradle-to-grave" records that Article 1, Section 1 was specifically designed to protect. *White v. Davis*, 13 Cal. 3d at 774 (quoting 1972 voter pamphlet). Indeed, the search condition allows the government to access information about "personal matters" like reproductive healthcare, family life, and sexuality which are "protected by the constitution from unwarranted government intrusion." *Thorne v. El Segundo*, 726 F.2d 459, 468 (9th Cir. 1983) (the right to informational privacy under the Constitution includes "the individual interest in avoiding disclosure of personal matters . . . .") (quoting *Whalen v. Roe*, 429 U.S. 589, 599 (1977)). The right to privacy applies equally to young people, and it has been recognized in a diverse set of circumstances. *See C.N. v. Wolf,* 410 F.Supp.2d 894, 903 (C.D. Cal 2005) (constitutional right to privacy limits school official's ability to disclose a student's sexual orientation to parents, even if student is openly gay at school); *Videckis v. Pepperdine Univ.*, 100 F.Supp.3d 927, 934 (C.D.

Cal 2015) (students had reasonable expectation of privacy with respect to their sexual orientation and intimate activities).

In the present case, the burden on Appellant's privacy rights far outweighs any justification for the condition, allowing unfettered access to a "virtual current biography" detailing nearly every aspect of a young person's life. That renders the condition unreasonable.

3. The condition authorizes an invasive search akin to a wiretap.

An electronic search condition that requires the young person to provide access, including passwords, to online accounts means that probation officers are able to and expected to access social networks, email and messaging services, and various online accounts "regardless of whether . . . the probationer is present when the search is conducted." *In re Ricardo P.*, 241 Cal.App.4th at 691 (citation omitted). This is the functional equivalent of a wiretap, allowing probation officers to "listen in" on electronic communications in real time. But wiretaps are only permitted where there is a special justification and procedural safeguards, and with good reason, as "few threats to liberty exist which are greater than that posed by the use of [interception] devices." *Berger v. New York*, 388 U.S. 41, 63 (1967). We know of no case that has upheld suspicionless wiretaps of probationers, adult or juvenile. Nor should this Court authorize the equivalent here.

Because of its scope and invasiveness, the use of a wiretap or other means of communication interception requires enhanced judicial oversight and procedural safeguards. In *Berger v. New York*, the U.S. Supreme Court held that a New York statute that authorized issuance of judicial orders for eavesdropping by means of a recording device was facially invalid under the Fourth Amendment. *Id.* at 55. The statute's defect was not a lack of a probable cause requirement, *id.* ("we need not pursue that question further because . . . the statute is deficient on its face in other respects"), but its lack of a particularity requirement sufficient to narrow the scope of the search, which the Court found necessary given the intrusiveness of eavesdropping. *Id.* ("The need for particularity and evidence of reliability [] required when judicial authorization of a search is sought is especially great in the case of eavesdropping. By its very nature eavesdropping involves an intrusion on privacy that is broad in scope"). Because the statute authorized what amounted to a "roving commission" that "le[ft] too much to the discretion of the officer executing the order," the Court held it facially unconstitutional. *Id.* at 59. The reasoning in *Berger* influenced the drafting of the federal Wiretap Act, which imposes a range of limitations and procedural safeguards on the use of wiretaps. 18 U.S.C. §§ 2510–20; *see United States v. Martinez*, 498 F.2d 464, 468 (6th Cir. 1974) ("It is clear that Congress gave careful consideration to [cases including *Berger*] in drafting [the Wiretap Act].").

Federal courts have not limited the *Berger* reasoning to wiretapping and oral interceptions. The Seventh Circuit applied the reasoning in *Berger* in holding that a warrant for video surveillance that "did not satisfy the four provisions of Title III [of the Wiretap Act]" violated the Fourth Amendment. *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984). The court noted that, in contrast to a "conventional search" where "the police go through a home or an office looking for contraband or evidence of a crime, and they either find what they are looking for or not, and then they leave," television surveillance "is identical in its indiscriminate character to wiretapping and bugging." *Id.* at 884-85. Video surveillance, like wiretapping, "pick[s] up anything within [its] electronic reach, however irrelevant to the investigation." *Id.* at 885.

The probation condition at issue in this case, like the statute found unconstitutional in *Berger* or the video surveillance held unconstitutional in *Torres*, has no limiting factor to mitigate its impact on privacy. The search condition does not describe with particularity the types of communications to be intercepted, nor does it provide for minimization of irrelevant communications. Like the statute in *Berger*, the electronic search condition is expressly designed to give probation officers a "roving commission" to rummage through all of a young person's electronic "communications, conversations or discussions." *Berger*, 388 U.S. at 59. As a result, "the conversations of any and all persons" that are accessible through a

probationer's electronic device—including not only those in which the young person is a participant but also those to which he is merely an observer—may "be seized indiscriminately." *Id.* at 69. The result is that probation officers are left with unfettered discretion to seize and use many forms of communications by the young person on probation and anyone with whom he interacts. *See id.*

In many ways, the electronics search condition sweeps even more broadly than the surveillance contemplated in *Berger* and its progeny. First, the condition allows surveillance of devices that include multiple mediums of communication above and beyond a single audio stream (*Berger*) or television feed (*Torres*). Indeed, the search condition at issue in this case potentially allows access to both video and audio communications through services like Skype, text and multimedia messages, e-mails, social media content, and more. Second, the condition allows for remote access to the young person's online accounts, which enables the surreptitious collection of private communications whenever an officer is able to access the Internet. Finally, the search condition lacks temporal limits: it allows access to digitally stored information created from before the imposition of probation to the present moment, far beyond the duration in *Berger*, where the eavesdropping was limited to two physical business offices for sixty days. *See* 388 *id.* at 41, 45. Like in *Berger*, the condition provides a

"blanket grant of permission to eavesdrop" on the young person and those with whom he communicates. *Id.* at 60. It is therefore unreasonable.

D. The electronic search condition is unreasonable because it undermines the rehabilitative purpose of probation.

An electronics search condition that lacks a connection to a person's offense or history and that provides the government with an all-access, long term pass to his private life is unreasonable because it undermines rather than promotes the central goal of juvenile probation: rehabilitation. Rather than effectively deterring a young person from backsliding, as the state contends, such a search condition will undermine rehabilitation by deterring him from accessing services and support groups and benefiting from modern support services that promote healthy living and rehabilitation.[45] By invading the privacy of any third party who communicates with, or merely joins the same digital community as, the young person on probation, it also discourages others from offering essential support to the probationer.

---

[45] *See also Cf. Olguin*, 45 Cal. 4th at 387 (Kennard, J., dissenting, with Moreno, J., concurring) ("An overbroad pet notification may itself interfere with achievement of probation's rehabilitative goals because [it] may discourage pet ownership, thereby depriving probationers of the well-documented physical and mental health benefits of animal companionship . . . .")).

1. The condition is likely to weaken a young person's community ties and chill him from seeking support and rehabilitative services online.

A recent comprehensive policy review on reducing recidivism and improving outcomes for youth in the juvenile justice system, conducted by the Council of State Governments Justice Center with support from the United States Department of Justice, found that programs based on "surveillance" and "fear" are not only often ineffective in reducing juvenile recidivism but in some cases actually increase delinquency.[46] By forcing a young person to choose between pursuing needed support and relationships online or protecting sensitive personal information from potential search, an electronic search condition that provides an all-access pass to a young person's digital personal life is likely to undermine, rather than promote, rehabilitation.

Young people on probation may be less likely to seek support, services, and community online if doing so means exposing sensitive information to a potential probation search. Seeking support online can expose a wide range of information to electronic searches, including text messages and

---

[46] *Core Principles for Reducing Recidivism and Improving Other Outcomes for Youth in the Juvenile Justice System*, The Council of State Governments Justice Center (Oct. 4, 2015) 12, 17, https://csgjusticecenter.org/wp-content/uploads/2015/11/Juvenile-Justice-White-Paper-with-Appendices-.pdf. The Office of Juvenile Justice and Delinquency Prevention, U.S. Department of Justice was also a sponsor of and provided guidance on the content of the paper.

voice mails, emails, online posts, and web browser histories. This information can reveal very sensitive personal information, such as membership and communications in personal support groups or social and political activism. It will be readily available through the search of an electronic device[47] or the use of an online account password. *See generally supra* Part II.B.

Online interactions can support the rehabilitation of young people on probation. The Justice Center's policy review found that many of the juvenile rehabilitation programs that demonstrate the most success seek to strengthen "interactions," including connecting youth to other "positive adults, peers, and activities in their schools and community."[48] For young people, especially from vulnerable communities, many of these interactions come through social media and other forms of electronic communication.[49] Privacy may be particularly important to promoting interactions related to intervention and support services.[50]

---

[47] *See Riley*, 134 at 2491 (noting that "cloud-computing" allows a "cell phone [to be] used to access data located elsewhere, at the tap of a screen").
[48] *See Core Principles*, *supra* note 46, at 18.
[49] Amanda Lenhart, *Social Media and Friendships*, Pew Research Center, (2015), http://www.pewinternet.org/2015/08/06/chapter-4-social-media-and-friendships/.
[50] *See* Alisa Haxell, *Cn I jus txt, coz I don wan 2b heard: Mobile Technologies and Youth Counseling*, ascilite Melbourne 405 (2008), http://www.ascilite.org/conferences/melbourne08/procs/haxell.pdf (finding young people preferred texting rather than calling to get further support from counselors because they did not want to be heard).

These interactions may not happen if fear of surveillance discourages the young person from discussing or reaching out for help related to deeply personal issues. A young person on probation seeking to stay off drugs may choose not to use proven-successful interventions to reduce drug-abuse relapse, which rely on "[m]essages . . . [that] can be accessed and responded to privately, when and where youths find it convenient or feel a need for help," if they fear those messages might be subject to search.[51] A young person may not use Crisis Text Line[52] if she is worried that a probation officer might learn about her concerns or mental health struggles. If she is gay, she may not seek support from an LGBTQ Facebook group if she is worried that a probation officer could uncover and possibly expose her sexual orientation by reading private group conversations[53] or simply by discovering her participation in that group. A transgender young person would not be able to self-identify and seek support on a social network without similar concerns. Others, fearing probation officers will learn about the immigration status of family members or disapprove of their political or

---

[51] *See Text Messaging Aftercare supra* note 19.
[52] *See* Fried, *supra* note 17; see *also* Samaritans, *supra* note 17.
[53] *LGBT Youth Help and Support, supra* note 18, (Assuring potential members of the group that since it is a closed Facebook group, posts will not be publicly posted to Facebook walls. "This is a closed group made in order to be ourselves and to help also those who are LGTB [sic], without concern if the posts will appear in [sic] our walls, you can be sure that it'll never happen . . .").

social activism, may avoid becoming involved with groups such as United We Dream[54] or BlackLivesMatter.[55] As a result, rather than supporting rehabilitation, an all-access search condition will weaken the community ties and access to a positive networks, support, and social and civic activities that promote youth success.

Increasing public awareness of surveillance misuse may also increase the chilling effects of an all-access search condition. In recent years, revelations about government surveillance have greatly increased the public's understanding of how often the government exercises its surveillance authority and the wealth of information that digital searches can reveal. This awareness has led many people to change their behavior, including avoiding communicating about or accessing information about sensitive topics.[56] *See Jones*, 132 S.Ct. at 956 (Sotomayor, J., concurring)

---

[54] United We Dream Home Page, http://unitedwedream.org/, (last visited June 8. 2016) ("United We Dream is the largest immigrant youth-led organization in the nation.").

[55] Black Lives Matter Home Page, http://blacklivesmatter.com/, (last visited June 8, 2016) ("Black Lives Matter is a chapter-based national organization working for the validity of Black life.").

[56] *See, e.g.*, Nadia Prupis, *Snowden Revelations Led to 'Chilling Effect' on Pursuit of Knowledge: Study, Common Dreams*, Common Dreams (June 6, 2016), http://www.commondreams.org/news/2016/04/27/snowden-revelations-led-chilling-effect-pursuit-knowledge-study (contending that evidence of curtailing searches for particular terms "shows that people have become scared to learn about 'important policy matters' due to the fear of government surveillance" in the post-Snowden era.); *see also* Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, Pew Research Center: Internet, Science & Tech, (Mar. 16, 2015),

("Awareness that the Government may be watching chills associational and expressive freedoms."). California's voters expressed similar concerns four decades earlier. *See White*, 13 Cal. 3d at 774 (the Privacy Amendment "prevents government . . . from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us").

In providing the government with virtually unlimited access to a young person's digital private life, the expansive search condition here is likely to create fear of surveillance and chill social engagement and access to important support services. In doing so, the condition undermines juvenile probation's central goals of rehabilitation and reformation. That renders it unreasonable.

2. The condition discourages third parties from building relationships with and offering support to young people on probation.

An all-access search condition undermines rehabilitation in another way: it discourages third parties from providing support and services to young people on probation if those third parties are concerned about exposing their own private information to government scrutiny. A young

---

http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ ("25% of those who are aware of the surveillance programs (22% of all adults) say they have changed the patterns of their own use of various technological platforms 'a great deal' or 'somewhat' since the Snowden revelations.").

person's electronic devices not only store and allow access to the intimate details of her life; they also provide access to sensitive personal information about hundreds or even thousands of other people, including those with no direct connection to the young person. These other people use technology for the same purposes as a young person on probation might—and in doing so offer advice, emotional support and close relationships that help the young person build strong connections and lead a healthy and productive life. But third parties may choose not to provide that support if doing so subjects them to surveillance through an all-access search condition imposed on a young probationer.

A search of a young person's electronic device can provide access to sensitive information about a vast number of other people since such a search may reveal years worth of emails, text messages, and other private communications. *See supra* Part II.B. In addition, electronic devices can allow access to a wide range of third party information beyond direct communications, such as the private information and posts of "friends" (the average teen Facebook user has 300 Facebook friends) as well as their photographs, videos, and other speech.[57] Individuals also join closed communities online whose members can share information with each other

---

[57] *32 Awesome Facebook Statistics by Age*, BrandonGaille.com (Apr. 25, 2015), http://brandongaille.com/32-awesome-facebook-statistics-by-age/.

while keeping that information private from non-members.[58] These communities address sensitive topics including addiction,[59] sexuality and gender,[60] religious, political or ethnic affiliations and activities,[61] mental health concerns,[62] immigration status[63] and more. Young people also reach out to peers on social networks for advice, to form bonds, and to share

---

[58] *See, e.g.,* LGBT Youth Help and Support – Jovenes LGBT Ayuda y Apoyo
Facebook (Oct. 4, 2016),
https://www.facebook.com/groups/LGTBPEOPLE/ ("This is a closed group made in order to be ourselves and to help also those who are LGTB [sic], without concern if the posts will appear in [sic] our walls, you can be sure that it'll never happen…"

[59] *See, e.g., Text Messaging Aftercare, supra* note 19; *Alcoholics Anonymous – Bay Area*, Facebook,
https://www.facebook.com/groups/721773207870650/ (last visited Oct. 18, 2016).

[60] *See, e.g., OutOfTheCloset (Bay Area LGBT!+ Youth Group),* Facebook,
https://www.facebook.com/groups/1005878246173771/# (last visited July 6, 2016); *LGBT Youth Help and Support, supra* note 18.

[61] *See, e.g., Bay Area YOUTH & EM Pastor Fellowship*, Facebook,
https://www.facebook.com/groups/222698774589811/ (last visited Oct. 18, 2016); *Bay Area Youth "BAY" Christian Fellowship*, Facebook,
https://www.facebook.com/groups/222698774589811/#_=_ (last visited July 6, 2016); *SF Bay Area Youth Ministry Network*, Facebook
https://www.facebook.com/groups/513823702041307/#_=_(last visited July 6, 2016).

[62] *See, e.g., Depression and Anxiety Youth Group*, Facebook,
https://www.facebook.com/groups/180736338948203/#_=_(last visited July 6, 2016); *Anxiety & Depression Youth support group*, Facebook,
https://www.facebook.com/groups/515612035283365/#_=_ (last visited July 6, 2016).

[63] *See, e.g., Being Brought to the U.S. as Children Does Not Make Us Criminals!*, Facebook,
https://www.facebook.com/groups/213153242081450/#_=_(last visited July 6, 2016).

sensitive information with each other.[64] Information about very personal matters of others could be exposed in an electronic search.

The scope and invasiveness of the search condition in this case may discourage third parties from communicating with young people on probation or from offering the supportive environments and services those young people need. *See generally supra* Parts II.A. & II.D.1. This expansive search condition could be particularly harmful "in communities where a higher than average number of persons are on probation" and others may be particularly wary of exposing their own lives to government scrutiny. *People v. Hoeninghaus*, 120 Cal. App. 4th 1180, 1197 (2004) (citing *Robles*, 23 Cal. 4th at 800).

This Court has already recognized that the reasonableness of a search must be questioned if it may lead "many law-abiding citizens . . . not to open their homes to probationers" because they fear arbitrary government intrusion into their lives. *Robles*, 23 Cal. 4th at 799. It recognized that expansive searches could lead to "higher recidivism rates and a corresponding decrease in public safety." *Id.* Lower courts evaluating search conditions have considered this impact on third parties even where

---

[64] *See How Teens Use Media*, The Nielson Company 1, 7 (June 2009), http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2009-Reports/How-Teens-Use-Media.pdf ("57% of teen social networkers said they look to their online social network for advice, making them 63% more likely to do this than the typical social networker.").

those persons' privacy rights were not directly at issue. *See In re J.B.*, 242 Cal. App. 4th 749, 759 (2015) (even if probationer did not have standing to assert third party's Fourth Amendment rights, "that is no justification for the court to authorize probation officers to invade the privacy of other innocent parties who participate in the same social media networks as the minor."); *In re Malik J.*, 240 Cal. App. 4th at 902 ("the threat of unfettered searches of Malik's electronic communications significantly encroaches on his and potentially third parties' constitutional rights of privacy and free speech").

The expansive electronic search condition here discourages others from "open[ing] their" online "homes to probationers" to give them a safe place where they can seek the support and services they need. *Robles*, 23 Cal. 4th at 800. As a result, the condition is unreasonable.

CONCLUSION

For the foregoing reasons, Amici urge this Court to find that the electronic search probation condition is unreasonable, that it fails the *Lent* test, and that the juvenile court erred in imposing it on Appellant.

Respectfully submitted,

Dated: October 19, 2016

AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, INC.

By: _____
NICOLE A. OZER

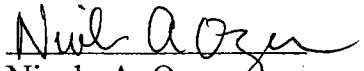
ELECTRONIC FRONTIER FOUNDATION

By: _____
LEE TIEN

Attorneys for *Amici Curiae* ACLU of Northern California, ACLU of Southern California, ACLU of San Diego and Imperial Counties, and Electronic Frontier Foundation

CERTIFICATE OF WORD COUNT

I certify pursuant to California Rules of Court 8.204 and 8.504(d) that this Amicus Brief is proportionally spaced, has a typeface of 13 points or more, contains 9,362 words, excluding the cover, the tables, the signature block, verification, and this Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: October 19, 2016 By: 

Nicole A. Ozer
Counsel for *Amici Curiae*

PROOF OF SERVICE

I, Cecilia Bermudez, declare under penalty of perjury under the laws of the State of California that the following is true and correct:

I am employed in the City of San Francisco, County of San Francisco, California, in the office of a member of the bar of this court, at whose direction the service was made. I am over the age of eighteen (18) years, and not a party to or interested in the within-entitled action. I am an employee of the American Civil Liberties Union Foundation of Northern California, and my business address is 39 Drumm Street, California 94111.

On October 20, 2016, I served the following document(s):

Application of the ACLU of Northern California, ACLU of Southern California, ACLU of San Diego and Imperial Counties, and Electronic Frontier Foundation for leave to file Amici Curiae brief

and

Amici Curiae brief in support of Defendant and Appellant Ricardo P

In the Following Case:
In re Ricardo P
No. S230923

on the parties stated below by the following means of service:

Ronald E. Niver
Office of the Attorney General
455 Golden Gate Avenue,
Suite 11000
San Francisco, CA 94102
Counsel for The People: Plaintiff and Respondent

Megan Hailey-Dunsheath
Attorney at Law
1569 Solano Avenue, #457
Berkeley, CA 94707
Counsel for Ricardo P.: Defendant and Appellant

First Appellate District,
Division One
Court of Appeal of the State of California
350 McAllister Street
San Francisco, CA 94102

Alameda County Superior Court
Att: Hon Leopoldo E. Dorado,
Judge
2060 Fairmont Drive, 1st Fl.
San Leandro, CA 94578

First District Appellate Project
FDAP
Oakland, CA 94612
eservice@fdap.org
via Electronic Mail

Office of the Attorney General
SF San Francisco AG
San Francisco, CA 94102
SFAG Docketing@doj.ca.gov
via Electronic Mail

X__ By U.S. Mail enclosing a true copy in a sealed envelope in a designated area for outgoing mail, addressed with the aforementioned addressees. I am readily familiar with the business practices of the ACLU Foundation of Northern California for collection and processing of correspondence for mailing with the United States Postal Service and correspondence so collected and processed is deposited with the United States Postal Service on the same date in the ordinary course of business.

I declare under penalty of perjury that the foregoing is true and correct. Executed on October 20, 2016 at San Francisco, California.

_____
Cecilia Bermudez, Declarant