Filed 11/8/17

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

THIRD APPELLATE DISTRICT

(Sacramento)

THE PEOPLE, Plaintiff and Respondent, v. JOSE ALBERTO VALDIVIA, Defendant and Appellant.	C082622 (Super. Ct. No. 16FE012090)

APPEAL from a judgment of the Superior Court of Sacramento County, Bunmi Awoniyi, Judge. Affirmed as modified.

Jyoti Malik, under appointment by the Court of Appeal, for Defendant and Appellant.

Kamala D. Harris and Xavier Becerra, Attorneys General, Gerald A. Engler, Chief Assistant Attorney General, Michael P. Farrell, Assistant Attorney General, Eric L. Christoffersen and Matthew Kearney, Deputy Attorneys General, for Plaintiff and Respondent.

In this domestic abuse case, defendant Jose Alberto Valdivia challenges a condition of his probation authorizing the warrantless search of electronic storage devices, such as cellular phones and computers, under his control.[1] He contends the condition must be stricken because it: (1) "is unreasonable under [*People v.*] *Lent* [(1975) 15 Cal.3d 481], as it bears no relationship to [his] current offense or potential future criminality"; and (2) "is unconstitutional under the Fourth and Fifth Amendments of the United States Constitution because [his] privacy and privilege against self[-] incrimination far outweigh the State's purported and unproven rehabilitation and societal protection interests." He also contends the condition infringes on the privacy interests of third parties.

We find no merit in defendant's arguments that the electronic storage device search condition is unreasonable under *Lent*, nor do we find any merit in his argument that the condition is unconstitutional under the Fifth Amendment. Furthermore, we conclude that his attempt to raise the privacy interests of third parties is barred by forfeiture. We do agree with him, however, that on the facts of this case, the electronic storage device search condition is unconstitutionally overbroad because its potential impact on his Fourth Amendment rights exceeds what is reasonably necessary to serve the government's legitimate interest in ensuring that he complies with the terms of his probation. Accordingly, we will strike the electronic storage device search condition but will also remand the case to the trial court to consider in the first instance whether the condition can be narrowed in a manner that will allow it to pass constitutional muster.

FACTUAL AND PROCEDURAL BACKGROUND

In June 2016, defendant physically assaulted his wife, leaving her with abrasions on her neck, bruises on her cheek, a swollen forearm, and small lacerations on her knee

---

[1] For ease of reference, we will refer to this as the electronic storage device search condition."

and head. He was charged with one count of inflicting corporal injury on a spouse. The case was resolved by a negotiated plea under which defendant pled no contest to the charge in exchange for a grant of probation and 90 days in jail.

On the day of the hearing when defendant changed his plea, the People filed a 23-page boilerplate memorandum of points and authorities, accompanied by a 12-page declaration from a Sacramento County Sheriff's deputy assigned to the Sacramento Valley Hi-Tech Crimes Task Force, in support of the imposition of a probation condition requiring defendant to submit his electronic storage devices, including but not limited to cell phones and computers, to warrantless search and seizure. The boilerplate memorandum explained that the superior court had "developed new language describing search and seizure terms and conditions accompanying grants of probation for certain cases." Essentially, the new language added "electronic storage devices" to the standard condition permitting warrantless probation searches, which already permitted searches of a probationer's "person, place, property, automobile, . . . and any object under [the probationer's] control."[2] According to the memorandum, the probation department was "recommending the imposition of this new language in cases, such as this, where there is a nexus between the grant of probation and the defendant's use of an electronic device." Being a boilerplate document, however, the memorandum did not provide any details relating to this specific case. Instead, the memorandum asserted in a footnote that the new search condition "should be imposed in cases where there has been a demonstrated connection between the type of criminal conduct involved and the use of electronic devices and/or [where the condition] bears a reasonable relation to future criminality,

---

[2] For ease of reference, we will refer to the search condition as a whole as the search condition and will refer to the provision referencing electronic storage devices as the electronic storage device search condition, even though the former is simply a part of the latter.

such as the following: drug sales/transportation; fraud, identity theft, financial crimes; sex offenses; human trafficking, pimping and pandering; *domestic violence*; weapons-related offenses; gang enhancements and gang membership; and any other case where a defendant used an electronic device during the current offense or in a previous crime." (Italics added.)

The accompanying declaration explained how evidence of additional criminal activity (in the officer's training and experience) tended to be found on the electronic devices of those who had engaged in the various types of criminal conduct identified above. With respect to crimes of domestic violence, the officer asserted that the perpetrators of those crimes "often violate restraining orders, protective orders, or no[-] contact orders which ha[ve] been issued post-offense" and "[e]vidence of these violations is often found on electronic devices." The officer explained that such evidence could include actual communications with the protected party "via text, chat, or email," or "[g]eolocation data" that could "provide evidence that the suspect's device was near the victim['s] location in violation of an order." The officer further asserted that "[p]hotographic images, videos, or voice recording communications" could violate such orders, and evidence of those items might be found on the perpetrator's electronic device.

In a section applicable generally to all of the previously identified categories of crimes, the officer also purported to explain the need to examine the "[e]ntire [c]ontents of [e]lectronic devices." (Bold text omitted.) According to the officer, "it is necessary to search all the content contained on the device in some shape or form in order to identify ownership, possession, and activity related to the specific offense."

The same day the People filed the boilerplate memorandum and accompanying declaration supporting imposition of the electronic storage device search condition, defense counsel filed a boilerplate memorandum objecting to the imposition of that condition. Defense counsel's memorandum asserted that a condition allowing the search of electronic storage devices was too intrusive to be imposed, and even if it was not, such

a condition would be constitutionally overbroad. The memorandum also asserted that compelling someone to reveal the password for their computer would violate the Fifth Amendment.

At the hearing, after defense counsel stipulated to the factual basis for defendant's no contest plea, counsel objected to the proposed electronic storage device search condition "as without a nexus to the particular facts of this case, as well as being overbroad." Defense counsel further asserted that if the court was going to "impose a search condition on cell phones," "that condition should be limited only to material on that phone which would have a nexus to the charge."

The prosecutor responded that the People were seeking imposition of the electronic storage device search condition "particularly because this is a domestic violence case." The prosecutor pointed out that a protective order was going to be issued in the case and then argued (consistent with the declaration from the sheriff's deputy) that evidence of the violation of such orders is often found on electronic devices.

The court imposed the condition "as stated," i.e., without modification. Thus, the probation conditions imposed on defendant included the following: "Defendant shall submit his/her person, place, property, automobile, electronic storage devices, and any object under his/her control, including but not limited to cell phones and computers, to search and seizure by any law enforcement officer or probation officer, any time of the day or night, with or without a warrant, with or without his/her presence or further consent. [¶] . . . [¶] Defendant shall provide access to any electronic storage devices and data contained there, including disclosing and providing any and all information necessary to conduct a search." Defendant was also ordered as a condition of probation to "[o]bey all laws applicable to [him]." And the court ordered, as a condition of probation, that defendant have only peaceful contact with the victim (his wife). To that end, the court issued a criminal protective order, effective during the probationary period, that did not prohibit defendant from having contact with his wife but did prohibit him

from (among other things) harassing, striking, threatening, assaulting, following, stalking, and molesting her.

Defendant timely appealed from the order granting probation.

DISCUSSION

On appeal, defendant offers four arguments as to why the electronic storage device search condition is unlawful. First, he contends the condition violates the test set forth in *Lent*. Second, he contends the condition is overbroad in violation of his constitutional rights under the Fourth Amendment. Third, he contends the condition infringes on the privacy interests of third parties. And fourth, he contends the condition violates his privilege against self-incrimination under the Fifth Amendment. We address each argument in turn, albeit in a different order than presented by defendant.

I

The Lent Test

" 'Probation is generally reserved for convicted criminals whose conditional release into society poses minimal risk to public safety and promotes rehabilitation. [Citations.] The sentencing court has broad discretion to determine whether an eligible defendant is suitable for probation and, if so, under what conditions. [Citations.] The primary goal of probation is to ensure "[t]he safety of the public . . . through the enforcement of court-ordered conditions of probation." [Citation.]' [Citation.] Accordingly, the Legislature has empowered the court, in making a probation determination, to impose any 'reasonable conditions, as it may determine are fitting and proper to the end that justice may be done, that amends may be made to society for the breach of the law, for any injury done to any person resulting from that breach, and generally and specifically for the reformation and rehabilitation of the probationer. . . .' [Citation.] Although the trial court's discretion is broad in this regard, we have held that a condition of probation must serve a purpose specified in Penal Code section 1203.1. [Citations.] If a defendant believes the conditions of probation are more onerous than the

potential sentence, he or she may refuse probation and choose to serve the sentence." (*People v. Olguin* (2008) 45 Cal.4th 375, 379 (*Olguin*).)

Like the Supreme Court, "[w]e review conditions of probation for abuse of discretion." (*Olguin*, *supra*, 45 Cal.4th at p. 379.) Under the test from *Lent*, "[g]enerally, '[a] condition of probation will not be held invalid 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. . . ." [Citation.]' [Citation.] This test is conjunctive -- all three prongs must be satisfied before a reviewing court will invalidate a probation term. [Citations.] As such, even if a condition of probation has no relationship to the crime of which a defendant was convicted and involves conduct that is not itself criminal, the condition is valid as long as the condition is reasonably related to preventing future criminality." (*Olguin*, at pp. 379-380, quoting *People v. Lent*, *supra*, 15 Cal.3d at p. 486.)

Pursuant to the foregoing, the initial question here under *Lent* is whether the electronic storage device search condition is reasonably related to preventing future criminality by defendant. Defendant asserts it is not. He contends that to the extent the prosecutor argued the condition was justified because evidence of the violation of no-contact protective orders is often found on electronic storage devices, "[t]he entire basis for allowing a warrantless search of all electronic devices under [his] control is nonexistent" because the trial court did not issue any such order in this case, but instead issued only a "peaceful contact" protective order. According to defendant, "[p]robation conditions are to be tailored on a case specific basis, and the search condition in light of the facts of this case is completely illogical." To that same end, he contends that because "there is nothing in the record regarding the current offense or [his] social history that connects his use of electronic devices or social media to domestic violence," "the record is wholly silent about [his] usage of electronic devices or social media," and "nothing in [his] current offense or his personal history demonstrates a predisposition to utilize

electronic devices or social media in connection with criminal activity," "there is no reason to believe that the current probation condition will serve a rehabilitative function as precluding [him] from any future criminal acts of violence against his wife."

We are not persuaded. The principle underlying defendant's argument is that for a probation condition to be reasonably related to preventing future criminality, that condition must have a specific connection to the facts of the defendant's offense of conviction or other past criminal conduct and must have a tendency to preclude the defendant from engaging in similar criminal conduct in the future. Case law from our Supreme Court does not support that principle, however. Not that long ago, in *Olguin*, a majority of the Supreme Court held that a condition of probation is reasonably related to future criminality if it "enables a probation officer to supervise his or her charges effectively." (*Olguin, supra*, 45 Cal.4th at pp. 380-381.) While the specific condition at issue in *Olguin* was one "requiring notification of the presence of pets" (*id.* at p. 381), the *Olguin* majority pointed out, as an example, that "probation conditions authorizing searches 'aid in deterring further offenses . . . and in monitoring compliance with the terms of probation. [Citations.] By allowing close supervision of probationers, probation search conditions serve to promote rehabilitation and reduce recidivism while helping to protect the community from potential harm by probationers.' " (*Id.* at p. 380, quoting *People v. Robles* (2000) 23 Cal.4th 789, 795.) The Supreme Court also cited with approval the decision in *People v. Balestra* (1999) 76 Cal.App.4th 57 (see *Olguin*, at p. 381), where the appellate court held that "a warrantless search condition is intended to ensure that the subject thereof is obeying the fundamental condition of all grants of probation, that is, the usual requirement . . . that a probationer 'obey all laws.' Thus, warrantless search conditions serve a valid rehabilitative purpose, and . . . such a search condition is necessarily justified by its rehabilitative purpose." (*Balestra*, at p. 67.) And as long ago as 1971, our Supreme Court explained that the "acknowledged purposes" of a search condition are "to deter further offenses by the probationer and to ascertain whether

he is complying with the terms of his probation. . . . 'The purpose of an unexpected, unprovoked search of [the] defendant is to ascertain whether he is complying with the terms of probation; to determine not only whether he disobeys the law, but also whether he obeys the law. Information obtained under such circumstances would afford a valuable measure of the effectiveness of the supervision given the defendant and his amenability to rehabilitation.' " (*People v. Mason* (1971) 5 Cal.3d 759, 763-764, disapproved on other grounds in *People v. Lent*, *supra*, 15 Cal.3d at p. 486, fn. 1, quoting *People v. Kern* (1968) 264 Cal.App.2d 962, 965.)

Like most, if not all, probationers, defendant here was ordered as a condition of probation to "[o]bey all laws applicable to [him]." Given this condition, the fact that defendant may not have shown any predisposition to use an electronic storage device like a cell phone or computer for purposes of criminal activity, including but not limited to crimes of domestic violence, does not render the electronic storage device search condition unreasonable under *Lent*. The electronic storage device search condition -- like the rest of the search conditions (to which defendant did not object) -- serves to enable defendant's probation officer to supervise him effectively by helping the probation officer ensure that defendant is complying with the conditions of his probation by obeying *all* laws, not just the law he previously disobeyed when he assaulted his wife. Because the electronic storage device search condition serves this valid rehabilitative purpose, it is reasonably related to future criminality and thus satisfies the *Lent* test.[3]

II

Privacy Rights Of Third Parties

Defendant contends that because the electronic storage device search condition "allow[s] for searches outside of [his] immediate control (i.e., computers or electronic

---

[3] A similar question is pending review before the Supreme Court in *In re Ricardo P.* (2015) 241 Cal.App.4th 676, review granted February 17, 2016, S230923.

devices he may leave at work or with a friend or relative, or computers or devices he might share with coworkers, family members, or roommates)," because his wife and her children "continue to reside in the same home as [defendant], and potentially use the same electronic storage devices as him," and because "as a parent, he technically has control over his minor children's electronic storage devices," the condition here "is overbroad and infringes on not only [his] but his entire family's privacy rights" and thus "must be stricken."

We conclude defendant forfeited this argument by failing to raise it in the trial court, and thus we do not address it further. (See, e.g., *People v. Trujillo* (2015) 60 Cal.4th 850, 856.)[4]

III

Fifth Amendment Privilege Against Self-Incrimination

Defendant contends that because the electronic storage device search condition implicitly requires him to "provide needed usernames, passwords, etcetera" to facilitate searches of his devices,[5] "[t]he condition . . . is tantamount to mandating testimony by [him] of his knowledge of the existence and locations of certain personal texts, email and social media accounts, as well as his possession, control, and access to those accounts." In this manner, he contends, the condition requires him "to provide a testimonial or

---

[4] On remand for consideration of whether the condition can be sufficiently narrowed to pass constitutional muster under the Fourth Amendment, defendant may attempt to raise a further challenge to the condition based on the privacy rights of third parties, and we express no opinion on the potential validity of such a challenge, other than to note that defendant may lack standing to assert the privacy rights of persons other than himself. (See *B. C. Cotton, Inc. v. Voss* (1995) 33 Cal.App.4th 929, 947-948 ["courts will not consider issues tendered by a person whose rights and interests are not affected"].)

[5] Actually, the condition *expressly* requires him to "provide access to any electronic storage devices and data contained there, including disclosing and providing any and all information necessary to conduct a search."

communicative act." He further asserts that those acts "could well be accompanied by implied factual statements that could prove to be incriminatory." Because the refusal "to provide personally incriminating and testimonial acts" "would lead to revocation of [his] probation," defendant contends the search condition effectively compels him to provide communicative acts and thus violates his rights under the Fifth Amendment.

The shortest answer to this argument is that even assuming the provision requiring defendant to "disclos[e] and provid[e] any and all information necessary to conduct a search" of electronic storage devices in his control can be reasonably understood as compelling him to incriminate himself in violation of his Fifth Amendment privilege, defendant has offered no authority for the proposition that the provision must be stricken. He places some reliance on the United States Supreme Court's decision in *Minnesota v. Murphy* (1984) 465 U.S. 420 [79 L.Ed.2d 409], but that reliance is misplaced.

In *Minnesota*, the Court addressed "whether a statement made by a probationer to his probation officer without prior [*Miranda*] warnings is admissible in a subsequent criminal proceeding." (*Minnesota v. Murphy*, *supra*, 465 U.S. at p. 425 [79 L.Ed.2d at p. 418].) In the course of answering that question, the Court noted that "if the State, either expressly or by implication, asserts that invocation of the privilege would lead to revocation of probation, . . . the failure to assert the privilege would be excused, and the probationer's answers would be deemed compelled and inadmissible in a criminal prosecution." (*Id.* at p. 435 [79 L. Ed.2d at pp. 424-425].) In an accompanying footnote, the Court further asserted that "a State may validly insist on answers to even incriminating questions and hence sensibly administer its probation system, as long as it recognizes that the required answers may not be used in a criminal proceeding and thus eliminates the threat of incrimination. Under such circumstances, a probationer's 'right to immunity as a result of his compelled testimony would not be at stake,' [citations], and nothing in the Federal Constitution would prevent a State from revoking probation for a refusal to answer that violated an express condition of probation or from using the

probationer's silence as 'one of a number of factors to be considered by a finder of fact' in deciding whether other conditions of probation have been violated." (*Id.* at p. 435, fn. 7 [79 L.Ed.2d at p. 425, fn. 7].)

The foregoing principles from *Minnesota* do *not* support defendant's assertion that the probation condition requiring him to disclose and provide any and all information necessary to conduct a search of electronic storage devices in his control must be stricken as violative of his Fifth Amendment privilege against self-incrimination. Rather, at best, *assuming* (without deciding) that the condition can be reasonably understood as compelling him to incriminate himself in violation of his privilege, and *assuming* (without deciding) that the condition is sufficient by itself to communicate that a refusal to disclose and provide such information will lead to the revocation of probation, all *Minnesota* says is that when (if ever) defendant is asked to disclose and provide such information, he does not have to expressly assert the privilege, the failure to assert the privilege will be excused, and any answers he provides may be deemed compelled and inadmissible in a criminal prosecution. At the same time, however, if defendant *refuses* to disclose and provide such information, he may be in violation of the terms of his probation and the state can revoke his probation on that basis. Nothing in *Minnesota* supports defendant's contention that the mere *existence* of the condition requiring him to disclose and provide any and all information necessary to conduct a search of electronic storage devices in his control *presently* violates his Fifth Amendment privilege against self-incrimination such that the condition cannot lawfully exist and must be stricken. For this reason, defendant's challenge to the condition under the Fifth Amendment is without merit.

IV

Overbreadth

Defendant's final challenge to the electronic storage device search condition is that it is overbroad in violation of his constitutional rights under the Fourth Amendment.

Thus, the question we are left with is this: Does an electronic storage device search condition that passes muster under *Lent* because it reasonably relates to future criminality by allowing defendant's probation officer to search such devices within defendant's control to ensure he is obeying all laws also pass muster under the Fourth Amendment? On the facts here, we conclude the answer to that question is "no."

"A probation condition that imposes limitations on a person's constitutional rights must closely tailor those limitations to the purpose of the condition to avoid being invalidated as unconstitutionally overbroad." (*In re Sheena K.* (2007) 40 Cal.4th 875, 890.) "Conditions which infringe on constitutional rights are not automatically invalid. Certain intrusions by government which would be invalid under traditional constitutional concepts may be reasonable at least to the extent that such intrusions are required by legitimate governmental demands." (*In re White* (1979) 97 Cal.App.3d 141, 149-150.) A probation condition "is unconstitutionally overbroad . . . if it (1) 'impinge[s] on constitutional rights,' and (2) is not 'tailored carefully and reasonably related to the compelling state interest in reformation and rehabilitation.' " (*In re E.O.* (2010) 188 Cal.App.4th 1149, 1153, quoting *In re Victor L.* (2010) 182 Cal.App.4th 902, 910.)

There is no doubt that the electronic storage device search condition imposed on defendant here impinges on his constitutional rights under the Fourth Amendment. In *Riley v. California* (2014) ___ U.S. ___ [189 L.Ed.2d 430], the United States Supreme Court held that the police generally may not, without a warrant, search digital information on a cell phone (one type of electronic storage device) incident to an arrest. In reaching that conclusion, the Court explained how "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of" "other objects that might be kept on an arrestee's person," such as "a cigarette pack, a wallet, or a purse." (*Id.*at p. ___ [189 L.Ed.2d at p. 446].) Detailing how the search of a cell phone can impact a person's privacy interests, the Court wrote as follows: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers

that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.

"One of the most notable distinguishing features of modern cell phones is their immense storage capacity. . . .

"[T]he current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. [Citation.] Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. [Citation.] We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

"The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information -- an address, a note, a prescription, a bank statement, a video -- that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

"Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the

person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. [Citation.] A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. [Citation.] But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives -- from the mundane to the intimate. . . .

"Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns -- perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. [Citation.]

"Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase 'there's an app for that' is now part of the popular lexicon. The average smart

phone user has installed 33 apps, which together can form a revealing montage of the user's life. [Citation.]

"In 1926, Learned Hand observed . . . that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.' [Citation.] If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone 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 phone is.

"To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. [Citation.] But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of 'cloud computing.' Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. [Citation.] Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another." (*Riley v. California*, *supra*, ___ U.S. ___, ___ [189 L.Ed.2d at pp. 446-449, fn. omitted.)

From the United States Supreme Court's observations in *Riley*, it is abundantly clear that a probation condition that authorizes the warrantless search of an electronic storage device like a cell phone carries the potential for a significant intrusion into defendant's private affairs -- even more so than the standard condition authorizing the search of defendant's "person, place, property, automobile, . . . and any object under

[defendant's] control." As the appellate court observed in *People v. Appleton* (2016) 245 Cal.App.4th 717 (*Appleton*), "the computer search condition at issue here arguably sweeps more broadly than the standard three-way search condition allowing for searches of probationers' persons, vehicles, and homes. First, by allowing warrantless searches of all of defendant's computers and electronic devices, the condition allows for searches of items outside his home or vehicle, or devices not in his custody -- e.g., computers or devices he may leave at work or with a friend or relative. Second, the scope of a digital search is extremely wide. . . . Thus, a search of defendant's mobile electronic devices could potentially expose a large volume of documents or data, much of which may have nothing to do with illegal activity. These could include, for example, medical records, financial records, personal diaries, and intimate correspondence with family and friends." (*Id.* at p. 725.)

Given the potential for an essentially unprecedented intrusion into private affairs that may -- and likely will -- have nothing to do with illegal activity, the question is whether such an intrusion is nonetheless constitutionally permissible because it is tailored carefully to the government's legitimate interest in defendant's reformation and rehabilitation. We conclude it is not.

It goes without saying that the state has a legitimate and significant interest in ensuring that the purpose of probation -- defendant's rehabilitation -- is achieved here. (See *People v. Wardlow* (1991) 227 Cal.App.3d 360, 365 ["The purpose of probation is rehabilitation"].) Moreover, as we have concluded already in upholding the electronic storage device search condition under *Lent*, a search condition that permits warrantless searches of electronic storage devices under defendant's control for evidence of criminal activity can be understood to serve that purpose by helping to ensure that defendant is obeying all laws, which another condition of his probation requires him to do. But at the same time the electronic storage device search condition serves the state's legitimate interest in monitoring defendant's rehabilitation, it permits unprecedented intrusion into

his private affairs -- and it does so on a record that demonstrates little likelihood, or even possibility, that evidence of illegal activity will be found in the devices the condition subjects to a warrantless search.

As defendant points out, "the record does not show that electronic devices played any role in the underlying criminal conduct" -- that is, defendant's infliction of corporal injury on his wife. Moreover, there was nothing in the record to demonstrate that defendant "use[d] electronic devices for wrongful purposes in the past." Essentially, the record here showed only that defendant physically assaulted his wife on a single occasion. And it is significant that the People did not seek, nor did the trial court issue, a protective order prohibiting defendant from having contact with his wife. Rather, defendant was subjected only to a *peaceful* contact order -- meaning he can still lawfully reside with his wife and interact with her on a daily basis, as long as he does so peacefully. Under these circumstances, there appears to be no substantial reason for believing that evidence of future criminal activity by defendant is likely to be found on electronic storage devices under his control.

In their attempt to justify imposition of the electronic storage device search condition on defendant, the People first contend that "because [he] has pleaded no contest to a felony and accepted probation in lieu of additional punishment, [defendant] has a diminished expectation of privacy as compared to law-abiding citizens or those subject to searches incident to arrest." This is undoubtedly true, but at the same time defendant did not entirely surrender his rights under the Fourth Amendment by pleading no contest and accepting probation. The fact that the overbreadth doctrine applies at all to probationers like defendant illustrates this point. A probation condition that infringes on the constitutional rights a probationer otherwise enjoys still must be closely tailored to achieve the legitimate purpose or purposes of that condition. The fact that a person convicted of a felony has agreed to subject himself to the supervision of probation does not, by itself, give the government the right to dig through every aspect of that person's

private affairs in search of evidence of criminal activity without any explanation or justification from the government of why such a search has, at the very least, a reasonable possibility of actually *uncovering* such evidence.

In attempting to suggest that such a possibility was shown here, the People argue essentially that the electronic storage device search condition was justified because defendant was convicted of a crime of domestic violence, and the evidence before the trial court (in the form of the stock declaration from the sheriff's deputy) showed that "in domestic violence related crimes, offenders often violate criminal protective orders like the one issued against [defendant] by threatening their victims via various electronic devices."

We find this argument unpersuasive for two reasons. First, the evidence presented to the trial court was not specific to peaceful contact protective orders like the one the court issued here. As we have explained, the sheriff's deputy whose declaration was offered to justify imposition of the electronic storage device search condition attested only generally that the perpetrators of domestic violence crimes "often violate restraining orders, protective orders, or no[-]contact orders which ha[ve] been issued post-offense," and "[e]vidence of these violations is often found on electronic devices" in the form of actual communications with the protected party "via text, chat, or email," or "[g]eolocation data" that could "provide evidence that the suspect's device was near the victim[']s] location in violation of an order." The deputy further asserted that "[p]hotographic images, videos, or voice recording communications" could violate such orders, and evidence of those items might be found on the perpetrator's electronic device.

Whatever the validity of the deputy's observations might be in cases involving *no-contact* protective orders, there appears little, if any, substantial basis for finding a reasonable possibility that evidence of a violation of the *peaceful contact* order imposed here would be found on an electronic storage device under defendant's control. As defendant himself observes, "[a]nything violent or abusive [he] would potentially convey

to the victim through text, Instagram or Snapchat, he could convey much more easily in the flesh." As a matter of pure logic, just because defendant physically assaulted his wife does not make it any more likely that evidence of future behavior toward her in violation of the peaceful contact order would be found on a cell phone or computer under his control. And as a matter of *experience* -- particularly the experience of the sheriff's deputy whose stock declaration was offered in support of the electronic storage device search condition -- there is simply no adequate evidentiary basis for concluding that evidence of a violation of a peaceful contact order is likely to be found on an electronic storage device under defendant's control, especially when the deputy's testimony addressed in an undifferentiated manner *all* types of protective orders, including no-contact orders, and that testimony was not in any way tailored to defendant or his circumstances.

The second reason we reject the People's attempt to justify imposition of the electronic storage device search condition on the basis that evidence of a violation of the peaceful contact order might be found in a search performed pursuant to that condition is that, in any event, the People's justification is too narrow to reasonably justify the breadth of the condition actually imposed. Essentially, the People's position breaks down to this: Because there is a possibility that evidence of contact between defendant and his wife that violates the peaceful contact order -- e.g., contact that amounts to harassing, threatening, following, stalking, or molesting her -- might be found on an electronic storage device under defendant's control, the warrantless search of such devices *without any limitation whatsoever* is justifiable and not overbroad under the Fourth Amendment. On the record before us, however, we cannot agree with that position. As set forth above, *Riley* details the staggering amount of personal information that can be found on a typical cell phone, and *Appleton* reinforces that point. We cannot say that it is reasonable to allow law enforcement officials to cull through *all* such information on defendant's devices, without limitation, because of the remote possibility that *somewhere* in that

information evidence of a nonpeaceful contact between defendant and his wife may be found.

For both of the foregoing reasons, we conclude that on the record in this case the electronic storage device search condition is unconstitutionally overbroad because its potential impact on defendant's Fourth Amendment rights exceeds what is reasonably necessary to serve the government's legitimate interest in ensuring that he complies with the terms of his probation. Whether the condition can, as a practical matter, be narrowed in a manner that will allow it to pass constitutional muster is a matter we leave for the parties and the trial court to address in the first instance on remand. For now, it is sufficient for us to conclude that the imposition of the condition in its current form cannot be sustained based on the record presently before us.

DISPOSITION

The order granting probation is modified by striking the probation condition requiring defendant to submit his "electronic storage devices, . . . including but not limited to cell phones and computers, to the search and seizure by any law enforcement officer or probation officer, any time of the day or night, with or without warrant, with or without his/her presence or further consent," and to "provide access to any electronic storage devices and data contained there, including disclosing and providing any and all information necessary to conduct a search." As modified, the order is affirmed. The case is remanded to the trial court for further proceedings consistent with this opinion.

/s/
Robie, Acting P. J.

I concur:

/s/
Butz, J.

MURRAY, J., concurring and dissenting.

Regarding electronic search conditions, one size may fit many, but one size does not fit all. Here, the prosecution sought and obtained an overbroad electronic search condition based on a boilerplate presentation to the trial court without regard to the specific circumstances of this case or defendant's history, or any apparent consideration of the privacy interests of the victim or other third parties, or the potential negative impact on defendant's rehabilitation and reformation. One size does not fit all.

I agree with the majority's conclusion that defendant's challenge to the electronic search condition on Fifth Amendment grounds is without merit. And while I disagree with the majority's conclusion that the search condition is justified on the ground that it is *reasonably* related to preventing future criminality without a nexus, I agree with the majority that the search condition is constitutionally overbroad.

I write separately: (1) to emphasize the difference between the home, vehicles, and a probationer's person on the one hand and modern electronic devices on the other as they relate to general probation search conditions; (2) to express my belief that, because of the differences between homes, vehicles and persons, as compared to electronic devices, *People v. Lent* (1975) 15 Cal.3d 481 (*Lent*) and the Fourth Amendment touchstone of reasonableness require a nexus between the present crime, or defendant's past crimes or misconduct, or defendant's background, history or circumstances, and the electronic search condition to be imposed; (3) to express my view that it is for the trial court to determine in the first instance whether the rationale of ensuring that defendant "obey all laws" warrants the imposition of the electronic search condition where this rationale was not considered in the trial court and to further point out that nothing in the majority opinion prevents the trial court from determining on remand that such a condition is *not* warranted to ensure that defendant obey all laws given the circumstances of this case; (4) to express my belief that the third party privacy concerns that are

implicated here, including those of the victim, should be considered in the trial court's overbreadth analysis; and (5) to discuss additional considerations that should be taken into account in crafting an electronic search condition to avoid overbreadth concerns. Thus, I concur in part and dissent in part.

I. Electronic Devices are Different

Today's electronic devices are fundamentally different from homes and other places subject to traditional general search conditions. Indeed, a search of electronic devices bears little resemblance to searches of physical places or property. Accordingly, the Fourth Amendment requirement of reasonableness requires that such devices be treated differently in the context of probation search conditions.

In *Riley v. California* (2014) 573 U.S. ___ [189 L.Ed.2d 430] (*Riley*), the United States Supreme Court addressed how the search incident to arrest exception to the warrant requirement applies to modern cell phones, which are "based on technology nearly inconceivable just a few decades ago," and which have become ubiquitous in our society. (*Id.* at p. 441.) While the circumstances at issue in *Riley* are different than those involved here, the high court's discussion of modern electronics is informative.

As the high court observed in *Riley*, "*a cell phone search would typically expose to the government far more than the most exhaustive search of a house*: A phone 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 phone is." (*Riley, supra,* 189 L.Ed.2d at p. 448, italics added.) A modern mobile phone, tablet, laptop, or personal computer may be capable of storing a far greater volume of data than a person traditionally would have physically stored in his or her entire home. The intrusion on privacy when searching such electronic devices is not physically limited in the same way as in the search of a house, a car, or a person. Moreover, the "gulf between physical practicability and digital capacity will only

continue to widen in the future." (*Id.* at pp. 446-447.) Indeed, technology has made substantial leaps in the brief time since the high court decided *Riley*.

Furthermore, "[a]lthough the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." (*Riley*, *supra*, 189 L.Ed.2d at pp. 447-448.) Thus, while much of the data stored on mobile phones or similar electronic devices subject to the electronic search condition could duplicate physical objects that might be found in a search of the home, car, or person of the probationer, such as photographs, documents, and correspondence, electronic devices host an entirely unprecedented collection of data in perhaps greater amounts and divulging details that previously would not have been recorded or kept, let alone subject to collection.

For example, as the high court in *Riley* noted, access to electronic devices can reveal Internet searches and browser history. (*Riley*, *supra*, 189 L.Ed.2d at pp. 447-448.) There is no analogue to this kind of access in searches of physical places. If a person visited the library to perform research on a medical condition and made no record of this activity, that activity would not be found in a search of that person's home. However, where a person performed similar research on his or her mobile phone or computer, law enforcement could quickly and effortlessly discover all material searched for and accessed by the individual in performing the research, as well as when the individual conducted the research. Additionally, as observed in *Riley*, a mobile phone can track and record an individual's movements. (*Id.* at p. 448.) Thus, as *Riley* made clear, data stored

on a mobile phone is both quantitatively *and* qualitatively different from the home, car, and person, which have traditionally been the subject of search conditions. (*Id*. at p. 447.) The same can obviously be said about computers and similar electronic devices. (*People v. Appleton* (2016) 245 Cal.App.4th 717, 724 (*Appleton*) ["Much of the reasoning in *Riley*—which recognized how the immense storage capacity of modern cell phones allows users to carry large volumes of data—would apply to other modern electronic devices covered by the probation condition at issue here"].)

There are additional characteristics of electronic devices that are materially different compared to physical locations such as a home. Data in electronic devices can be deleted, yet it can be forensically retrieved. (See, e.g., *In re Malik J.* (2015) 240 Cal.App.4th 896, 904 (*Malik J.*) [officers "should not be allowed to conduct a forensic examination of the device utilizing specialized equipment that would allow them to retrieve deleted information that is not readily accessible to users of the device without such equipment"].) This is not the case with items that may have once been located in a home. When a person throws out some private item or physically shreds or destroys some document out of concern for his or her privacy, it is unlikely, if not impossible, that it will be retrieved.

"To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself" due to " 'cloud computing,' " which is "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." (*Riley, supra*, 189 L.Ed.2d at p. 448.) Again, the same can be said for computers and tablets. There is no analogue to such storage related to homes, vehicles, and other physical locations that allows such easy access to a person's private information.

We may further consider the nature of home searches and searches of other physical locations to illustrate why searches of electronic devices are different in the probation context. In supervising probationers, probation officers sometimes make visits

to probationers' homes. This is an invasion of privacy of all who reside at the residence, but one that is necessary, understood, and accepted. (See *People v. Woods* (1999) 21 Cal.4th 668, 675 ["For nearly three decades, this court has upheld the legality of searches authorized by probation terms that require probationers to submit to searches of their residences at any time of the day or night by any law enforcement officer with or without a warrant"]; *People v. Trujillo* (2017) 15 Cal.App.5th 574, 588 (*Trujillo*) ["courts routinely uphold probation conditions granting probation officers broad authority to search a probationer's residence without a warrant or reasonable cause"].)

However, as a practical matter, a search executed at a residence during a home visit does not rise to the level of intrusion implicated in searching electronic devices. For example, as a practical matter, in a probation search of a home, law enforcement is not going to look at every document or scrap of paper on the off chance that it *might* reveal evidence of a violation. Law enforcement simply does not have the resources to undertake such fishing expeditions. Nor would it be reasonable to do so. In fact, a search where officers showed up at a home and went through *every piece of paper* looking, for example, for written threats or other non-peaceful communication just to determine whether a probationer *may have* written some such communication without some reason to believe such evidence would be found could be considered arbitrary, capricious, or harassing. (See *People v. Bravo* (1987) 43 Cal.3d 600, 608 (*Bravo*) [probation searches may not be undertaken for harassment or for arbitrary or capricious reasons]; *People v. Cervantes* (2002) 103 Cal.App.4th 1404, 1408 ["A search is a form of harassment when its motivation is a mere whim or caprice"], citing *People v. Reyes* (1998) 19 Cal.4th 743, 754 (*Reyes*); *People v. Bremmer* (1973) 30 Cal.App.3d 1058, 1063 [unrestricted search of a probationer by law enforcement officers at their whim or caprice is a form of harassment].) If it were understood that this is how officers would use the authority granted under general search conditions—to go on extensive fishing expeditions in homes or other places for such information—my belief is that most judges would not so

freely order general search conditions. Yet, the search condition imposed here allows a search of *everything* stored on electronic devices, and in the cloud, based on the *mere possibility* that the search *might* reveal a threat or some untoward communication. Indeed, as discussed *ante*, the electronic search condition authorizes law enforcement to search through information which previously would never have been recorded and stored, let alone subject to discovery by law enforcement.

The Attorney General asserts that searches of electronic devices are no different than traditional search conditions authorizing probation officers to search homes, vehicles, and the persons of probationers. At oral argument, the Attorney General repeatedly asserted that the home is the "pinnacle of the Fourth Amendment," and that if a probation officer can search a probationer's home under a general search condition, by even greater force of reason, the probation officer can search a probationer's electronic devices. For the reasons discussed *ante*, I disagree with the fundamental assumption of this contention; electronic devices are different qualitatively and quantitatively from homes, containing more information, including information that previously would not be discoverable. The touchstone of Fourth Amendment analysis is not the home or the location or focus of the search; the "touchstone of the Fourth Amendment is *reasonableness*, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.' " (*United States v. Knights* (2001) 534 U.S. 112, 118-119 [151 L.Ed.2d 497, 505] (*Knights*), italics added; accord *Riley, supra*, 189 L.Ed.2d at p. 439; *People v. Sanders* (2003) 31 Cal.4th 318, 333 (*Sanders*).)

Furthermore, the intrusions on the privacy of third parties who communicate with probationers via electronic devices is far greater than any such intrusion related to searches of the common areas in physical places where the third party might be located or reside. Additionally, unlike the search of a physical location, where there is a greater

likelihood that the third party will become aware of the search, searches of data from a probationer's electronic device and the collection of private information about third parties may never become known to them.

Moreover, unlike searches of physical locations, searches of electronic devices can be conducted outside the presence of other people, including the probationer. Indeed, the search condition here authorizes seizure of electronic devices, which means review of the data from a seized device could take place at some location other than the place where it is found. Consequently, in such situations, there is no way to monitor compliance with the requirements that searches not be done arbitrarily or capriciously or for purposes of harassment (see *Bravo, supra*, 43 Cal.3d at p. 610), and that searches reasonably relate to the purposes of probation (see *People v. Robles* (2000) 23 Cal.4th 789, 797 (*Robles*)). Fishing expeditions and unjustifiable invasions of privacy could take place in the seclusion of an office.

None of this is to say that electronic devices cannot be the subject of search conditions imposed on probationers. Rather, the purpose of this discussion is to illustrate how these devices present new issues in the context of such probation search conditions and to provide the backdrop against which the validity and constitutionality of such search conditions must be evaluated.

II. Nexus to Circumstances Pertinent to the Case and the Probationer

A. Fourth Amendment Reasonableness, the *Lent* Test, and *Olguin*

In *Lent, supra*, 15 Cal.3d 481, our high court held that a "condition of probation will not be held invalid 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 . . . .' " (*Id*. at p. 486.) The *Lent* test is conjunctive: "all three prongs must be satisfied before a reviewing court will invalidate a probation term." (*People v. Olguin* (2008) 45 Cal.4th

375, 379 (*Olguin*).) "As such, even if a condition of probation has no relationship to the crime of which a defendant was convicted and involves conduct that is not itself criminal, the condition is valid as long as the condition is *reasonably related* to preventing future criminality." (*Id*. at pp. 379-380, italics added.)

As noted by the majority (Maj. opn., *ante*, at p. 8), in *Olguin* our high court addressed a probation condition requiring the probationer to inform the probation department about the presence of pets at his residence. (*Olguin, supra*, 45 Cal.4th at p. 378.) Relying on *Lent*, the *Olguin* court stated: "[T]he relevant test is *reasonableness* [citation], and defendant does not persuasively explain why it is *unreasonable* to place the burden on defendant to keep the probation officer informed of the presence of any pets at the residence." (*Olguin*, at pp. 383-384.) The *Olguin* court cited with approval *People v. Balestra* (1999) 76 Cal.App.4th 57 (*Balestra*). In *Balestra*, the defendant was placed on probation after being convicted of elder abuse (*Balestra*, at p. 62), and the appellate court upheld a general search condition of the defendant's person and property for any violation of law (*id*. at pp. 61, 66-68). The *Balestra* court authorized this general search condition even when the underlying offense was not reasonably related to theft, narcotics, or firearms. (*Id*. at p. 67.) In doing so, the court relied primarily on the statute authorizing courts to impose conditions of probation. Penal Code section 1203.1[1] gives courts the discretion to impose conditions of probation to provide for the "reformation and rehabilitation of the probationer."[2] Neither *Olguin* nor *Balestra* involved electronic

---

[1] Further undesignated statutory references are to the Penal Code in effect at the time of the charged offense.

[2] Section 1203.1, subdivision (j), provides in pertinent part: "The court may impose . . . reasonable conditions, as it may determine are fitting and proper to the end that justice may be done, that amends may be made to society for the breach of the law, for any injury done to any person resulting from that breach, and generally and specifically *for the reformation and rehabilitation* of the probationer . . . ." (Italics added.)

search conditions and, consequently, whether and when such conditions are "*reasonably related* to preventing future criminality" was not considered by either court. (See *Olguin*, at pp. 379-380, italics added.) As I explain, we must do so here.

B. Proceedings in the Trial Court

In the trial court, the prosecution grounded its request for the electronic search condition on a nexus between the crime and the probation condition. For example, the prosecution stated: "it is imperative that *where these devices are shown to have a nexus to the type of criminal conduct committed by the probationer*, the search conditions traditionally extended to persons, homes, and objects should also be extended to include the electronic devices of those probationers." (Italics added.) The prosecution relied on cases requiring or discussing such a nexus, including *Malik J.*, *supra*, 240 Cal.App.4th 896, *Appleton*, *supra*, 245 Cal.App.4th 717, *In re Erica R.* (2015) 240 Cal.App.4th 907 (*Erica R.*), and *In re P.O.* (2016) 246 Cal.App.4th 288 (*P.O.*).[3]

The deputy sheriff's boilerplate declaration accompanying the prosecution's memorandum suggests a focus on a nexus by identifying the type of evidence that can be found on electronic devices in various types of cases.[4] Regarding domestic violence, the declaration noted that electronic device data sometimes contain evidence of restraining order or no-contact order violations, stating: "The offender may communicate with the victim via text, chat, or email," and "[g]eolocation data may provide evidence that the suspect's device was near the victim location in violation of an order." The declaration *did not* assert that an electronic search condition could also facilitate monitoring whether

---

[3] I discuss these cases, *post*.

[4] The types of cases referenced in the declaration include: "Drug Sales/Transportation"; "Fraud, Identity Theft, Financial Crimes"; "Sex Offenses"; "Human Trafficking, Pimping and Pandering"; "Domestic Violence"; "Weapons-Related Offenses"; and gang cases. (Italics omitted.)

a probationer complies with the requirement that he or she obeys all laws. Nor did the prosecutor advance that theory in its boilerplate memorandum.

Against this backdrop, it is understandable that the nexus or lack thereof was the focus of the parties at the sentencing hearing. The prosecution did not argue that the search condition was necessary to ensure that defendant obeyed all laws, and the trial court did not rule that it was. Defense counsel argued that the electronic search condition was "without a nexus to the particular facts of this case, as well as being overbroad. [¶] If the Court does impose a search condition on cell phones, that condition should be limited only to material on that phone which would have a nexus to the charge." The prosecutor replied: "The People are asking that it be imposed particularly because this is a domestic violence case. That a protective order is being issued. And that in domestic violence related crimes, it is a violation of those criminal protective orders or restraining orders post the offense and after the conviction that have resulted in violations. Those violations often are found on electronic devices. The offenders may communicate with the victim via text, chat or email communication. They may use third parties to deliver that communication to the victim on the offender's behalf. [¶] There are various program applications to mask communication in an attempt to avoid detection. So the People are asking that that probation condition regarding search[e]s of electronic devices in possession of the defendant *pursuant to 1546*[5] be imposed." (Italics added.) Without consideration of the circumstances of the case or defendant's background and history or

---

5 "1546" is apparently a reference to section 1546, which is a part of the Electronic Communications Privacy Act (Stats. 2015, ch. 651, § 1 (SB 178)) (ECPA). Section 1546 is the definitions section. Section 1546.1, subdivision (c)(4), allows government entities to "access electronic device information by means of physical interaction or electronic communication with the device. [¶] . . . [¶] With the specific consent of the authorized possessor of the device."

the breadth of the search condition, the court simply ruled: "The Court would impose it as stated."

Thus, the prosecution here requested the search condition based on the need to monitor compliance with a restraining order. However, defense counsel informed the court, both before the court agreed to impose the search condition and after, that the restraining order would be a "peaceful contact order." Defendant was not prohibited from contacting or living with the victim. The prosecutor had provided a copy of the written order for the court's signature and advised the court that the proposed no-contact order suggested by the probation department would be modified to a peaceful contact order. However, the trial court stated: "That will be modified except for the peaceful contact order. And I've also signed the *no contact* order prepared by the District Attorney, that will be served on [defendant]." (Italics added.) The order the court signed, however, was not a no-contact order; it was a peaceful contact order as requested by the prosecution, prohibiting defendant from, among other things, harassing, striking, threatening, and assaulting his wife.[6] Thus, there was no need to monitor whether defendant stayed away from or otherwise contacted the victim as long as those contacts were peaceful.[7]

---

[6] The order also prohibited defendant from attempting to dissuade any victim or witness from attending a hearing or testifying or making a report to law enforcement.

[7] The entire search condition as set forth in the written probation conditions signed by defendant reads as follows: "15. P.C. 1546 searchable - Defendant shall submit his/her person, place, property, automobile, electronic storage devices, and any object under his/her control, including but not limited to cell phones and computers, to search and seizure by any law enforcement officer or probation officer, any time of the day or night, with or without a warrant, with or without his/her presence or further consent. [¶] Defendant being advised of his/her constitutional and statutory rights pursuant to Penal Code section 1546 et seq. in this regard, and having accepted probation, is deemed to have waived same and also specifically consented to searches of his/her electronic storage devices. [¶] Defendant shall provide access to any electronic storage devices and

C. The People's Newly Minted Contention on Appeal Relying on the Probation Condition that Defendant to Obey All Laws

On appeal, the People contend the electronic search condition is "rationally related to [defendant's] crimes." According to the People, this is so because the condition is reasonably related to preventing future criminality in the form of violations of the criminal protective order. The People argue that the condition would enable probation officers "to determine if [defendant] was continuing with his threatening[8] or violent conduct," and help them to "assess if [defendant] was attempting to harass or abuse his victim through electronic, telephonic, or written contact or otherwise violating the criminal protective order." This essentially mirrors the prosecution's contention in the trial court sans the nexus requirement. Additionally, the People argue on appeal that the search condition would enable probation officers to monitor whether defendant is attempting to dissuade the victim or any witness from attending a hearing or testifying or making a report to law enforcement.

However, the People also argue on appeal, *for the first time*, that the electronic search condition would help ensure that defendant abides by the condition that he obey all laws. It appears that the People on appeal have abandoned, and indeed now refute, their contention in the trial court that a nexus is required between the probationer's offense and the search condition imposed. The majority approves of an electronic search condition here based on the People's belated contention. (Maj. opn., *ante*, at p. 9.)

---

data contained therein, including disclosing and providing any and all information necessary to conduct a search."

8 While the record demonstrates that defendant assaulted the victim, there is no evidence in the record that defendant "threatened" the victim and thus there is no factual basis upon which to assert the condition was necessary to determine if defendant was "*continuing* with his threatening" conduct. (Italics added.)

D. Evolving Case Law Regarding Electronic Search Conditions

In *People v. Bryant* (2017) 10 Cal.App.5th 396, review granted June 28, 2017, S241937 (*Bryant*), the defendant was convicted of possessing a concealed and loaded firearm in a vehicle. (*Id*. at p. 398.) The trial court imposed a two-year sentence, part of which was to be served by the defendant under mandatory supervision. (*Ibid*.) As part of his supervision, the trial court required the defendant to submit to searches of his "text messages, e-mails, and photographs on any cellular phone or other electronic device in his possession or residence." (*Ibid*.) On appeal, the *Bryant* court struck the electronic search condition because there was "no showing of any connection between [the defendant]'s use of a cellular phone and criminality, *past or future*. [The defendant] was convicted of possessing a concealed weapon in a vehicle. No cellular phone or electronic device was involved in the crime and *there is no evidence that [the defendant] would use such devices to engage in future criminal activity*. [Citation.] Nor was there any showing as to how the search condition would reasonably prevent any future crime or aid in [the defendant]'s rehabilitation. *Although it is conceivable that future searches of* [*the defendant*]*'s cellular phone might yield information concerning criminal activity*, '*[n]ot every probation condition bearing a remote, attenuated, tangential, or diaphanous connection to future criminal conduct can be considered reasonable*.' [Citation.] The fact that a search of [the defendant]'s cellular phone records might aid a probation officer in ascertaining [his] compliance with other conditions of supervision is, without more, an insufficient rationale to justify the impairment of [his] constitutionally protected interest in privacy." (*Id*. at pp. 404-405, quoting *People v. Brandão* (2012) 210 Cal.App.4th 568, 574 (*Brandão*), italics added.) The *Bryant* court noted that "[w]hether an electronic search condition is reasonably related to preventing future criminality depends upon the facts and circumstances in each case." (*Bryant*, at p. 402.) The court concluded that the electronic search condition was invalid under *Lent*. (*Bryant*, at p. 406.)

The *Bryant* court also distinguished *Olguin*, stating: "Unlike the pet notification condition in *Olguin . . . , a search of a defendant's cellular phone and other electronic devices implicates a defendant's constitutional rights*." (*Bryant, supra*, 10 Cal.App.5th at p. 402, italics added.) "In contrast to information about a defendant's pets, a cellular phone search could potentially reveal 'a digital record of nearly every aspect of [its owner's life]—from the mundane to the intimate' [citation], including 'vast amounts of personal information unrelated to defendant's criminal conduct or his potential for future criminality' [citation]. *Olguin*, therefore, does not resolve the question presented here, and the 'fact that a search condition would facilitate general oversight of the individual's activities is insufficient to justify an open-ended search condition permitting review of all information contained or accessible on the [individual's] smart phone or other electronic devices.' " (*Bryant*, at p. 402.)

The *Bryant* court relied on several cases as examples of the application of this nexus rule. Several of these were cases cited by the prosecution in the trial court in its briefing calling for a nexus.

In *Erica R., supra*, 240 Cal.App.4th 907, an electronic search condition was imposed on a juvenile who was placed on probation after admitting to misdemeanor possession of Ecstasy. (*Id*. at p. 910.) The *Erica R*. court invalidated the search condition under the third prong of *Lent*, noting: "There is nothing in this record regarding either the current offense or [the minor]'s *social history* that connects her use of electronic devices or social media to illegal drugs. In fact, the record is wholly silent about [the minor]'s usage of electronic devices or social media." (*Erica R.*, at p. 913, italics added.) The court concluded: " '[b]ecause there is nothing in [the minor's] *past or current offenses or [her] personal history* that demonstrates a predisposition' to utilize electronic devices or social media in connection with criminal activity, 'there is no reason to believe the current restriction will serve the rehabilitative function of precluding [the minor] from any future criminal acts.' " (*Ibid.*, italics added.) The court acknowledged,

however, that "there can be cases where, based on a *defendant's history and circumstances*, an electronic search condition bears a reasonable connection to the risk of future criminality." (*Id*. at p. 914, italics added.)

In *In re J.B.* (2015) 242 Cal.App.4th 749 (*J.B.*), a juvenile who committed petty theft was placed on probation with a search condition that required him to allow searches of and disclose the passwords to his electronic devices and social media sites. (*Id*. at p. 752.) The trial court found that the search condition would deter the minor from committing new crimes and allow probation officers to monitor the minor's compliance with the terms and conditions of probation. (*Id*. at p. 753.) On appeal, the Attorney General argued the condition was reasonably related to future criminality because it served to facilitate monitoring by probation officers of the conditions prohibiting the use of alcohol and drugs, requiring the minor to stay away from the coparticipant with whom he committed the theft, requiring the minor to attend school, and requiring him to obey his parents. (*Id*. at p. 755.) Following the reasoning in *Erica R.*, the *J.B.* court held that the search condition was invalid under *Lent* because there was "no showing of any connection between the minor's use of electronic devices and his *past or potential future criminal activity*." (*J.B.*, at p. 756, italics added.)

The *J.B.* court also discussed *Olguin, supra*, 45 Cal.4th 375, stating: "we question whether the Supreme Court decision in . . . *Olguin* [citation] justifies a probation condition that facilitates general supervision of a ward's activities if the condition requires or forbids noncriminal conduct bearing no relation to the minor's offense that is not reasonably related to potential future criminality *as demonstrated by the minor's history and prior misconduct*. In our view, such a broad condition cannot be squared with the limitations imposed by *Lent, supra*, 15 Cal.3d at page 486, and in some cases may exceed constitutional limitations." (*J.B., supra,* 242 Cal.App.4th at p. 757, italics added.) The court in *J.B.* explained that *Olguin* focused on whether the probation condition there—notification of the presence of pets—was reasonable, given that the

" 'relevant test is *reasonableness*.' " (*J.B.*, at p. 757.) It further noted that the *Olguin* court "had no occasion to consider the reasonableness of requiring a probationary minor to submit all of his electronic devices to inspection without any evidence or indication that the minor was likely to use the devices for unlawful or other proscribed activity. The Supreme Court certainly was not considering any of the privacy concerns articulated in *Riley v. California* . . . 573 U.S. ___ [189 L.Ed.2d 430 . . .] and in . . . *Malik J., supra*, 240 Cal.App.4th 896."[9] (*J.B.*, at p. 757.) The *J.B.* court went on to reject the application of *Olguin* in the context of electronic search conditions, stating: "The fact that a search condition would facilitate general oversight of the individual's activities is insufficient to justify an open-ended search condition permitting review of all information contained or accessible on the minor's smart phone or other electronic devices." (*J.B.*, at p. 758.)

In *Appleton*, the defendant met the victim through a social media application. (*Appleton, supra,* 245 Cal.App.4th at p. 719.) The defendant and two other men forced the victim to orally copulate them at defendant's house. (*Id.* at p. 720.) The defendant pleaded no contest to false imprisonment by means of deceit and was granted probation. (*Id*. at p. 720.) The trial court imposed a condition providing that electronic devices belonging to the defendant would be subject to search, and prohibiting the defendant from deleting the Internet browsing activity on his electronic devices. (*Id*. at p. 721.) The court explained that it was imposing this condition because, in the underlying offense, contact between the defendant and the victim was initiated through social media. (*Ibid.*) On appeal, the *Appleton* court stated: "We agree with defendant that the nexus between the offense and the probation condition is somewhat attenuated. But under the deferential standard of review required in the *Lent* analysis, we find no abuse of discretion in the trial court's finding that 'either social media or some kind of computer

---

[9] I discuss *Malik J. post* in addressing overbreadth and third party privacy rights.

software' was involved in the offense. Accordingly, the probation condition does not run afoul of the first *Lent* factor requiring 'no relationship to the crime.' Because the probation condition must trigger all three *Lent* factors to be invalid, we conclude the condition is valid under *Lent*." (*Appleton*, at p. 724.)

As an example of a case in which a nexus between the probationer's offense and the search condition imposed *was* found, the courts in *Erica R.*, *J.B.*, and *Bryant* discussed *People v. Ebertowski* (2014) 228 Cal.App.4th 1170 (*Ebertowski*). In *Ebertowski*, the defendant pleaded no contest to making criminal threats and resisting or deterring an officer, admitted a gang enhancement allegation, and was granted probation. (*Id*. at p. 1172.) Probation conditions imposed required the defendant to provide passwords to any electronic devices in his custody or control, submit those devices to searches, and provide all passwords to social media sites and submit those sites to search as well. (*Ibid*.) The prosecutor asserted in the trial court that these probation conditions were appropriate because the defendant had used social media in the past to promote his gang. (*Id*. at p. 1173.) The *Ebertowski* court held that these electronic search conditions were related to the defendant's crimes, "which were plainly gang related, because they were designed to allow the probation officer to monitor defendant's gang associations and activities. Defendant's association with his gang was also necessarily related to his future criminality. His association with his gang gave him the bravado to threaten and resist armed police officers. The only way that defendant could be allowed to remain in the community on probation without posing an extreme risk to public safety was to closely monitor his gang associations and activities. The password conditions permitted the probation officer to do so. Consequently, the password conditions were reasonable under the circumstances, and the trial court did not abuse its discretion in imposing them." (*Id*. at pp. 1176-1177.)

Similar to *Ebertowski*, the court in *In re J.E.* (2016) 1 Cal.App.5th 795, review granted October 12, 2016, S236628 (*J.E.*), upheld an electronic search condition because,

among the "constellation of issues requiring intensive supervision," the minor had significant drug issues and school attendance and discipline issues, he "admitted to being involved with" gang members, there was gang graffiti in his locker, and he had an unstable home life. (*J.E.*, at pp. 801-802.) These circumstances, according to the *J.E.* court, supported the juvenile court's finding that the electronic search condition served the rehabilitative function of preventing the minor from committing future criminal acts. (*Id*. at p. 802.) The court in *J.E.* distinguished *Erica R.* as "not reflect[ing] the array of criminal and social issues found in the case at hand." (*J.E.*, at p. 802.)

Similarly, in *P.O., supra*, 246 Cal.App.4th 288, another case upon which the prosecution here relied in the trial court in discussing the required nexus, the court held that the electronic search condition was reasonably related to future criminality. (*Id*. at p. 295.) The minor, who was found under the influence of drugs at school, admitted to using hashish oil earlier that morning and had 11 Xanax tablets in his pocket. (*Id*. at p. 292.) After admitting to one count of misdemeanor public intoxication, the minor was placed on probation. (*Ibid*.) The minor objected to an electronic search condition which required him to submit any electronics including passwords to search, pointing out there was no evidence he was buying or selling drugs. (*Id*. at p. 293.) The juvenile court made an express finding, emphasizing the need to help the minor avoid substance abuse. The juvenile court stated why it found the condition to be necessary: " '[T]o properly supervise these drug conditions, we need to go on your web sites, check what you may be presenting as far as your ability to purchase, to sell drugs, your ability to—we have people who present themselves on the Internet using drugs or . . . in possession of paraphernalia, and that's the only way we can properly supervise these conditions . . . .' " (*Ibid*.) On appeal, the *P.O.* court concluded the search condition was reasonably related to future criminality because it enabled probation officers to supervise the minor effectively. (*Id*. at p. 295.) The court reasoned: "the condition enables peace officers to review [the minor]'s electronic activity for indications that [he] has drugs or is otherwise

engaged in activity in violation of his probation. We cannot say that the juvenile court's given reason for imposing the condition—that minors are apt to use electronic devices to show off their drug use or ability to procure drugs—was speculative or otherwise constituted an abuse of discretion." (*Ibid.*) However, the *P.O.* court went on to conclude the search condition was overbroad. (*Id.* at pp. 297-298.)

Recently, in *Trujillo*, *supra*, 15 Cal.App.5th 574, the court rejected the notion that a nexus to the charged crime is required, but appeared to establish a requirement that is almost indistinguishable from a nexus requirement. In *Trujillo*, the defendant was convicted of attempted robbery and aggravated assault, and the parties agreed the electronic search condition had no relationship to the crimes. (*Id.* at pp. 578-579, 582.) Thus, the main issue was whether the condition was reasonably related to future criminality. In imposing the electronic search condition, the trial court made an express finding, stating: " 'I think that in order to supervise the defendant now on two felonies, . . . one is legally violent [attempted robbery], the other is just violent [assault by means likely to result in great bodily injury]. And that is to supervise him and make sure that he's not engaging in criminal activity, I think it would assist the probation department to be able to review what is on his computer, his cell phone, et cetera, to make sure he's being law abiding and also he's rehabilitating.' " (*Id.* at p. 581.) In upholding the search condition, the *Trujillo* court observed that defendant claimed to have committed the crimes because of alcohol intoxication and that the record showed "substantial risk factors relevant to reoffending, including significant untreated alcohol abuse, social isolation, family history of suicide (one of which he witnessed), family members who had been gang members, and economic stress." (*Id.* at p. 583.) The court in *Trujillo* further noted that the trial court imposed the search condition with an awareness of these circumstances and the probation department's conclusion that the defendant required close supervision to his daily activities to succeed on probation. (*Ibid.*)

The *Trujillo* court concluded: "The [trial] court made an express finding that 'in order to supervise the defendant now on two [violent] felonies,' the probation department needs to be able to 'view what is on his computer, his cell phone . . . .' *The record shows the court did not impose this condition as a matter of routine, but considered the specific facts relevant to Trujillo's case*." (*Trujillo*, *supra*, 15 Cal.App.5th at p. 583, italics added.) The *Trujillo* court stated that the trial court had "a reasonable basis" to conclude that the electronic search condition was the most effective way to confirm that the defendant remained law abiding, "rather than relying on a meeting or telephone conversation." (*Id*. at p. 584.) The *Trujillo* court rejected the defendant's argument that the third *Lent* prong required a connection between the defendant's past criminal conduct and the use of electronic devices and social media or that the search condition would facilitate supervision of the defendant's compliance with other specific probation conditions. (*Trujillo*, at p. 584.) The absence of such facts, according to the *Trujillo* court, "does not mean the search condition was unreasonable as a matter of law. The primary focus of *Lent*'s third-prong jurisprudence has been on *the particular facts and circumstances of the case* before the court, rather than on establishing bright-line rules. [Citations.] This makes sense given that the *appropriateness of a particular probation condition necessarily depends on a myriad of tangible and intangible factors before the trial court, including the defendant's particular crime, criminal background, and future prospects*." (*Trujillo*, at p. 584, italics added.) It appears to me that the *Trujillo* court concluded that the particular facts in the record related to the defendant's history and circumstances supported a finding that the electronic search condition was reasonably related to future criminality. In my view, this is essentially the same as concluding the defendant's background and history provided a nexus to the search condition.

E. Analysis

I agree with the courts in *Bryant*, *Erica R.*, *J.B.*, and *Appleton*, as well as the reasoning supporting electronic search conditions in *Ebertowski*, *J.E.*, and *P.O.*

Electronic devices and the data they record and store are fundamentally different than physical objects to be found in the home or vehicle or on the person. Application of the *Lent* test and the reasonableness requirement relative to electronic search conditions must take that difference into account. Given the nature of electronic search conditions, *Lent* cannot be satisfied unless there is a showing of a nexus. But the nexus need not relate to the charged crime. Based on the cases I have discussed, I conclude there must be a nexus between the electronic search condition and either (1) defendant's present crime (this is the first *Lent*-prong), *or* (2) defendant's past crimes or misconduct, *or* (3) defendant's background, history and circumstances. This goes beyond the first *Lent* prong, " 'no relationship to the crime of which the offender was convicted' " (*Lent, supra*, 15 Cal.3d at p. 486), and requires an examination not just of the facts of the case, but also the *defendant's prior crimes and misconduct, as well as the defendant's history and circumstances* to determine whether the probation condition is reasonably related to potential future criminal activity. In making the determination as to the reasonable relation to potential future criminality, trial courts can rely on expert testimony or declarations. A trial court may also rely on its own experience. (See *P.O., supra*, 246 Cal.App.4th at p. 293 [court relied on its experience that people " 'present themselves on the Internet using drugs' " or in possession of paraphernalia]; *Brandão, supra*, 210 Cal.App.4th at p. 575 [noting that in determining reasonableness, "courts are called upon to make judgments based on long experience with evaluating human affairs and conduct"].)

Given the record before us in the instant case, there is no dispute that the electronic search condition has no relationship to defendant's crime, and the use of electronic devices is not itself criminal. Thus, the third prong of the *Lent* test—whether the electronic search condition is reasonably related to future criminality—is the only prong at issue. In my view, no nexus has been shown between the electronic search condition and defendant's potential future criminality that would satisfy the

reasonableness requirement. Indeed, as the majority says in its overbreadth discussion, "there appears to be no substantial reason for believing that evidence of future criminal activity by defendant is likely to be found on electronic storage devices under his control." (Maj. opn., *ante*, at p. 18.) Reviewing courts "must decide whether the condition is *reasonably related* to a risk that defendant will reoffend." (*Brandão*, *supra*, 210 Cal.App.4th at p. 574.) And "[n]ot every probation condition bearing a remote, attenuated, tangential, or diaphanous connection to future criminal conduct can be considered reasonable." (*Ibid.*; accord, *Bryant*, *supra*, 10 Cal.App.5th at p. 405; *J.B.*, *supra*, 242 Cal.App.4th at p. 755; *Erica R.*, *supra*, 240 Cal.App.4th at p. 913.) When a probation condition " 'lack[s] any reasonable nexus to . . . present or future criminality' [citation], there is 'no reasonable basis for sustaining [the] condition.' " (*Brandão*, at p. 574.)

Here, there is no record supporting the premise that electronic devices played any role in the underlying offense. Indeed, the record is utterly silent on the subject of defendant's use of electronic devices. This is not to say that the required nexus must necessarily show the use of electronic devices in defendant's current or past crimes or misconduct. Other circumstances may support the nexus, such as the nature of prior crimes or misconduct—for example, in the context of a domestic violence case, evidence of prior threats, harassment, attempts at dissuasion, whether orally in person or over the phone, in writing or electronically might provide the required nexus. Here, however, there is no evidence in the record concerning any past crimes or misconduct by defendant. More particular to the search condition, there is no evidence showing that defendant ever threatened the victim or anyone else in the past, verbally, in writing or electronically. Nor is there any evidence that defendant committed past acts of verbal abuse or harassment against the victim or anyone else. Nor is there evidence defendant attempted to dissuade the victim or anyone else from reporting abuse or cooperating with the authorities. Nor are there any other relevant background or historical circumstances

from which a court could conclude the electronic search condition here is reasonably related to future criminality or to a potential violation of the peaceful contact order. If there had been such prior misconduct, it would be reasonable to predict defendant might use electronic devices to engage in that same type of conduct in the future, even if such devices were not the method of communication in the past.

Allowing probation searches of electronic devices, which as I have noted, are quantitatively and qualitatively different from the home or other physical locations, without the nexus discussed *ante*, is unreasonable. Moreover, as I will discuss, the absence of a nexus makes the narrow tailoring required to overcome an overbreadth challenge problematic at best.

The prosecutor in the trial court stated that she was requesting the electronic search condition because this is a domestic violence case, a protective order would be issued, and protective order violations "often are found on electronic devices" in various forms of communication. While the prosecutor's representations concerning electronic device usage relative to domestic violence crimes may be true as a general proposition, they would seem to have little to no application to the facts and circumstances of this case given the absence of information specific to defendant. Furthermore, here, the trial court issued a peaceful contact protective order,[10] so a major reason advanced for an electronic search condition in the boilerplate supporting declaration—monitoring a defendant's movements to determine whether there had been a violation of a no-contact restraining order—was not applicable here. This is important because, as I have noted, the trial court appeared to have been confused about the nature of the restraining order; it appears the

---

[10] Defendant notes on appeal that he has not been prohibited from living with his wife, the victim and that he, in fact, does live with her. However, the record itself sheds no light on whether the couple was, in fact, living together when the electronic search condition was imposed.

trial court thought it was signing a no-contact order. Given the true nature of the restraining order, the necessity for an electronic search condition would seem to be drastically reduced where defendant could communicate directly with the victim without the need for resort to electronic devices or third parties.

Abandoning the nexus requirement, the Attorney General advances the contention that the electronic search condition would help ensure that defendant abides by the condition that he obey all laws. (See *Balestra, supra*, 76 Cal.App.4th at p. 67; see also *Reyes, supra*, 19 Cal.4th at p. 752 [the purpose of an unexpected, unprovoked search of a probationer is to ascertain whether the probationer is complying with the terms of probation, to determine not only whether the probationer disobeys the law, but also whether the probationer obeys the law].) This was neither argued before nor decided by the trial court. It is possible that this rationale could support the issuance of an electronic search condition, assuming the development of facts showing a nexus. However, the matter was never raised nor litigated in the trial court.

Our role as the reviewing court is different from that of the trial court. "Under *Olguin*, our role in evaluating the third *Lent* factor is to determine *whether there is a reasonable factual basis* for the trial court to decide that the probation condition will assist the probation department to supervise the defendant." (*Trujillo, supra*, 15 Cal.App.5th at pp. 584-585, italics added.) In my view, it is not our role to justify a search condition based on grounds not contemplated by the parties or the trial court. Rather, the determination of the underlying basis for the search condition is for the trial court in the first instance. I am of the opinion that we should remand the matter to the trial court for a determination as to whether the obey all laws ground (or another ground) would serve as an appropriate and reasonable rationale under *Lent* for the issuance of the electronic search condition and to develop the factual basis necessary to establish a nexus. Indeed, with the development of additional facts and circumstances, the trial court might conclude that it is unnecessary to impose an electronic search condition to ensure

that defendant obey all laws (for example, if the facts demonstrate that defendant and the victim are currently residing together). In any event, I do not read the majority's opinion to prohibit the trial court from making such a finding.

III. Constitutional Overbreadth

Even if the electronic search condition is valid as reasonable under *Lent*, there remains the separate issue of constitutional overbreadth. I agree with the majority that the search condition here is overbroad because its potential impact on defendant's rights exceed what is reasonably necessary to serve the government's legitimate interest in ensuring that he complies with the terms of his probation. (Maj. opn., *ante*, at p. 2.) However, as will be seen, narrowly tailoring an electronic search condition is complicated by the absence of the nexus discussed *ante*.

"A probation condition that imposes limitations on a person's constitutional rights must closely tailor those limitations to the purpose of the condition to avoid being invalidated as unconstitutionally overbroad." (*In re Sheena K.* (2007) 40 Cal.4th 875, 890.) " 'The essential question in an overbreadth challenge is the closeness of the fit between the legitimate purpose of the restriction and the burden it imposes on the defendant's constitutional rights—bearing in mind, of course, that perfection in such matters is impossible, and that practical necessity will justify some infringement.' " (*J.E., supra,* 1 Cal.App.5th at p. 803, quoting *In re E.O.* (2010) 188 Cal.App.4th 1149, 1153 (*E.O.*).) "It is not enough to show the government's ends are compelling; the means must be carefully tailored to achieve those ends. A state may restrict a constitutional right, but only when the restriction is narrowly drawn to serve a compelling state interest." (*People v. Harrisson* (2005) 134 Cal.App.4th 637, 641.) Under this doctrine, " ' " 'a governmental purpose to control or prevent activities constitutionally subject to state regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms.' " ' " (*Ebertowski, supra,* 228

Cal.App.4th at p. 1175.) I submit that the search condition here was not merely insufficiently tailored; I submit that it was not tailored at all.

There are two separate sets of privacy interests involved in the overbreadth analysis here: defendant's privacy interests and the privacy interests of third parties. I focus first on the privacy rights of third parties, then on defendant's privacy interests.

A. Third Party Privacy Rights

On appeal, defendant argues that the electronic search condition infringes on the privacy interests of third parties. The People do not address this argument in their briefing.

1. Forfeiture

Even though the People do not argue forfeiture, the majority concludes that defendant forfeited his third party privacy rights argument by failing to raise it before the trial court. (Maj. opn., *ante*, at pp. 9-10.) For the reasons I discuss *post*, I believe we should exercise our discretion to address defendant's contention. (See *People v. Williams* (1998) 17 Cal.4th 148, 161-162, fn. 6 [appellate courts have discretion to reach issues forfeited other than rulings concerning the admission and exclusion of evidence].) Additionally, it seems inappropriate to *sua sponte* invoke forfeiture because the defendant did not specifically object on third party privacy grounds in the trial court, but at the same time justify the electronic search condition on the ground that it is reasonably related to the condition that defendant obey all laws, a theory not advanced by the prosecution in the trial court.

2. Standing

Because the majority deems the issue forfeited, it does not address defendant's contention concerning third party privacy rights, stating that it expresses no opinion on the matter, other than to observe that "defendant may lack standing to assert the privacy rights of persons other than himself. (See *B.C. Cotton, Inc. v. Voss* (1995) 33 Cal.App.4th 929, 947-948 [(*B.C. Cotton*)] ['courts will not consider issues tendered by a

person whose rights and interests are not affected'].)" (Maj. opn., *ante*, at p. 10, fn. 5.) Like forfeiture, the People made no standing argument in their briefing (although, they did make a standing argument during oral argument).

The issue of third party standing was addressed by the court in *J.B., supra*, 242 Cal.App.4th 749. While agreeing that the minor had no standing to raise the privacy interests of third parties as such, the *J.B.* court noted: "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." (*Id.* at p. 759.) I agree with the court in *J.B.*, particularly since the third party privacy interests here extend to private forms of communications such as email and text messaging. Allowing searches involving such private communications is an invasion of privacy potentially far more intrusive than when a search is conducted of common areas of a probationer's home where third parties reside. In my view, the impact on third party privacy rights is one that should be considered in deciding whether the search condition, as worded, is overbroad.

Moreover, *B.C. Cotton*, cited by the majority, is inapposite. In *B.C. Cotton*, the court noted: "Courts are created to resolve cases and controversies and not to render advisory opinions or resolve questions of purely academic interest. Accordingly, courts will not consider issues tendered by a person whose rights and interests are not affected." (*B.C. Cotton, supra*, 33 Cal.App.4th at pp. 947-948.) Here, the privacy rights of defendant, his wife, and potentially others, *are* affected. This is not a controversy involving parties not before us; nor is our resolution of the issue an advisory opinion. Rather, the matter we address relates to the propriety of courts issuing orders infringing on the privacy rights of defendant *and* third parties when imposing sentence on defendant. As the *J.B.* court declared, the fact that a defendant may lack standing to litigate third party privacy rights is no justification for courts to authorize the infringement of these rights. (*J.B., supra*, 242 Cal.App.4th at p. 759.) A trial court may not simply ignore those rights when imposing an electronic search condition on the

ground that the person before the court has no standing to complain; nor, in my view, may a reviewing court ignore the privacy rights of third parties on appeal.

Additionally, as with forfeiture, it seems equally inappropriate to *sua sponte* raise standing, an argument not made by the People in the trial court (or in their appellate briefing), and at the same time affirm the search condition here on a ground not raised by the prosecution or litigated in the trial court—that the condition is reasonably related to the condition that defendant obey all laws.

In any event, the rules related to standing have no application here,[11] and if the prosecution had objected on that ground in the trial court, the court would have been within its discretion to overrule the objection.[12]

3. Privacy Rights and Third Party Privacy Rights in General

Privacy is an important constitutional right. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have

---

[11] Of course, if law enforcement collects information on a third party by searching a probationer's electronic device pursuant to a search condition, the third party would have standing to challenge the search condition and the search itself if prosecuted based on the information gathered in that search. (See *People v. Schmitz* (2013) 55 Cal.4th 909 [third party charged with crimes resulting from parole search related to a passenger in the third party's car]; *Robles, supra*, 23 Cal.4th at p. 798 [noting that although a probationer who is subject to a search condition "has a severely diminished expectation of privacy over his or her person and property, there is no doubt that those who reside with such a person enjoy measurably greater privacy expectations in the eyes of society"]; *People v. Romeo* (2015) 240 Cal.App.4th 931, 935, 939 [reversing a conviction of a resident in a home where a search was based on a probation search condition for one of the other residents and the prosecution failed to establish the scope of the search condition].)

[12] Additionally, an argument could be made by defendant (if given the opportunity to make one) that he does have standing to object based on the privacy rights of third parties. To the extent that the privacy rights of those individuals relate to communications defendant has with them, defendant's privacy rights are also impacted. Indeed, as discussed *post*, discouraging communications with third parties could impair defendant's ability to succeed on probation and thus be counterproductive to his "reformation and rehabilitation." (See section 1203.1, subd. (j); fn. 2, *ante*.)

inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." (Italics added.) The ballot argument put before the voters in connection with the electorate's enactment of this constitutional provision included "broad references to a 'right to be left alone,' calling it a 'fundamental and compelling interest,' and purporting to include within its dimensions no less than 'our homes, *our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose*.' " (*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1, 20-21, quoting Ballot Pamp., Gen. Elec. (Nov. 7, 1972), proposed amends. to Cal. Const. with arguments to voters, p. 27, italics added.)

In ordering electronic search conditions, courts should not impair the privacy rights of third parties unless there is a compelling state interest that outweighs the privacy rights of the third parties. Thus, where the privacy rights of third parties are implicated in electronic search conditions, courts should engage in a balancing analysis. While exposing and prosecuting crime is a legitimate public interest (*Baughman v. State of California* (1995) 38 Cal.App.4th 182, 190), that does not mean courts should ignore third party privacy rights when imposing electronic search conditions, especially when the state interest is a "remote, attenuated, tangential, or diaphanous connection to future criminal conduct" (*Brandão, supra*, 210 Cal.App.4th at p. 574) that may or may not occur while a person is on probation. (See *Bryant, supra*, 10 Cal.App.5th at p. 405; *J.B., supra*, 242 Cal.App.4th at p. 755; *Erica R., supra*, 240 Cal.App.4th at p. 913.)

4. Privacy Rights of the Victim

No regard was given by the prosecution and the trial court here to the privacy rights of the victim, defendant's wife. Yet she clearly has a privacy interests in jointly owned electronic devices and electronic devices belonging to her over which defendant might be considered by an officer to have "control" by virtue of his proximity to it or its location. Additionally, communications between defendant and the victim that might be

found on defendant's electronic devices also implicate her privacy rights. The electronic search condition here allows probation officers and law enforcement to review intimate communications between a husband and wife based on the off chance that defendant *might* write something that violates the peaceful contact order. Additionally, such intimate communications may involve communication of a sexual nature, in which case the search condition could result in an intrusion into the victim's sexual privacy. (See *Boler v. Superior Court* (1987) 201 Cal.App.3d 467, 469 [deposition questions concerning defendant's sexual activities with unnamed women in a sexual harassment lawsuit impermissibly intruded on the sexual privacy rights of defendant *and his companions*].) This probation condition could thus be counterproductive because it could chill the kind of intimate communications spouses may have, and that these two spouses may need to have in order to repair their relationship and put the battering episode underlying this case behind them. This may impact the success of the couple's marriage in addition to defendant's success on probation which, of course, could be counterproductive to defendant's "reformation and rehabilitation." (See section 1203.1, subd. (j); fn. 2, *ante*.) The record does not demonstrate that anyone ever consulted the victim about this or considered these ramifications, and, at oral argument before this court, the Attorney General conceded that, to his knowledge, the victim was not consulted.

Also, the law is clear that the victim has a privacy interest in her personal financial records to which the search condition might provide access on her electronic devices over which defendant might have control. (See *Babcock v. Superior Court* (1994) 29 Cal.App.4th 721, 726 [nonmarital cohabitant has a privacy interest in her bank records].) There may also be financial or other sensitive or confidential information pertinent to the victim on defendant's electronic devices.

Additionally, Proposition 9, the Victims' Bill of Rights Act of 2008: Marsy's Law (Prop. 9, as approved by voters, Gen. Elec. (Nov. 4, 2008) eff. Nov. 5, 2008) (Marsy's

Law) made amendments to article I, section 28 of the California Constitution, "The Victims' Bill of Rights" (*People v. Hannon* (2016) 5 Cal.App.5th 94, 99) that are implicated here. Section 28, subdivision (a), paragraph (2), states the goal of ensuring that crime victims are treated with "respect and dignity." (Cal. Const., art. I, § 28, subd. (a), par. (2).) Subdivision (a), paragraph (3), states that "[t]he rights of victims pervade the criminal justice system." (Cal. Const., art. I, § 28, subd. (a), par. (3).) Subdivision (b) sets forth these rights, including a victim's rights: "(1) [t]o be treated with fairness and *respect for his or her privacy* and dignity . . ."; paragraph (6), to be "informed before any pretrial disposition of the case"; and paragraph (8), "[t]o be heard, upon request, at any proceeding, including . . . any proceeding in which a right of the victim is at issue." (Cal. Const., art. I, § 28, subd. (b), par. (1), (6), (8), italics added.) "Marsy's Law clearly demands a broad interpretation protective of victims' rights." (*Santos v. Brown* (2015) 238 Cal.App.4th 398, 418.) On this record, it appears that the electronic search condition was imposed without notice to the victim or extending to her an opportunity to object or otherwise be heard, even though her privacy interests are clearly implicated.

Malik J., supra, 240 Cal.App.4th 896, a case upon which the prosecution here relied in the trial court, illustrates the care courts should take concerning the privacy rights of household members. In *Malik J.*, the juvenile court imposed a search condition, orally stating: " 'you're to—and the family—is to provide all passwords to any electronic devices including cell phones, computers and notepads within your custody and control, and submit to search of devices at any time to any peace officer. And also provide any passwords to any social media sites, including [F]acebook, Instagram, and submit those [s]ites to any peace officer with or without a warrant.' "[13] (*Malik*, at p. 900,

---

[13] The minute order in *Malik J.* stated the condition differently, omitting references to the juvenile's family and social media sites. The condition in the minute order read:

fn. omitted.) On appeal, the People argued that the condition was justified by the minor's history of robbing people of their cell phones and the condition allowed law enforcement to determine if any phone he possessed while on probation was stolen. (*Id*. at p. 902.) The Court of Appeal treated the ownership issue as a constitutional consideration and concluded that the search condition was overbroad because it went further than necessary to determine ownership. (*Ibid*.) In doing so, the court noted the impact of the electronic search condition on third party privacy rights. (*Ibid*.) The court wrote: "Under the overbreadth doctrine, 'conditions of probation that impinge on constitutional rights must be tailored carefully and reasonably related to the compelling state interest in reformation and rehabilitation.' [Citations.] The mismatch here is of concern, because the threat of unfettered searches of [the minor]'s electronic communications significantly encroaches on his *and potentially third parties' constitutional rights of privacy and free speech*. . . . [Citation.] In view of these significant privacy implications, the electronics search condition must be modified to omit the requirement that [the minor] turn over passwords to social media sites and to restrict searches to those electronic devices found in his custody and control." (*Ibid*., italics added.)

The *Malik J.* court went on to clarify: "this does not mean that officers would have the unfettered right to retrieve *any* information accessible from any phone or computer in [the minor]'s possession." (*Malik J., supra*, 240 Cal.App.4th at p. 902.) Such a condition would allow searches as long as they are not arbitrary, capricious or harassing, but, given the nature and proliferation of electronic devices, the court reasoned that it was compelled to consider the extent to which an officer could search such devices pursuant to the search condition. (*Id*. at pp. 902-903.) In so doing, the court stated:

" 'Minor is ordered to provide all passwords to any electronic devices, including cell phones, computers or [notepads], within your custody or control, and submit such devices to search at any time without a warrant by any peace officer.' " (*Malik J., supra*, 240 Cal.App.4th at p. 900.)

"Remotely stored information may . . . implicate the privacy interests of *third parties* who are not otherwise subject to search or court supervision." (*Id*. at p. 903, italics added.) Therefore, in searching a phone to determine ownership, "officers must show due regard for information that may be beyond a probationer's custody or control or implicate the privacy rights of the probationer *or third parties*." (*Id*. at pp. 903-904, italics added.)

The *Malik J*. court then addressed the third party rights of people within the minor's household. The court concluded that because only the minor was placed on probation, only the minor could be subjected to the search conditions. (*Malik J., supra*, 240 Cal.App.4th at p. 905.) The court held that whether or not the trial court meant what it said when it referenced the minor's family in orally imposing the search condition, the condition would be "indisputably unconstitutional so far as it could be read to require individuals other than [the minor] to submit to warrantless searches of their electronic devices or turn over their passwords to police on demand." (*Id*. at pp. 905-906.)

Here, the victim's privacy rights are undoubtedly implicated and, in my view, she should be given the opportunity to be heard on this matter. Additionally, even if the victim provides no input to the court, the trial court must consider her privacy rights in its overbreadth analysis in this case.

5. Privacy Rights of Other Third Parties

Like the privacy rights of the victim, the privacy rights of other third parties are implicated by a search condition authorizing access to the communications such third parties have with defendant as well as searches of electronic devices owned by those third parties over which defendant may have "control." While there is no evidence of defendant using computers outside of the home (for example, at work), in my view, that is the trial court's failing for not correlating the underlying purpose of the search condition with the electronic devices to which defendant might have "control." (But see *Trujillo, supra*, 15 Cal.App.5th at pp. 588-589 [rejecting the defendant's overbreadth

claim on the basis that the defendant failed to establish what electronic devices he owns or the type of sensitive information contained therein].) As for communications between third parties and defendant, these may be private, sensitive or confidential. Due regard for these interests should be given before an electronic search condition is ordered.

B. Privacy Rights of Defendant

Although defendant's privacy rights are diminished because of his probationary status (*Knights, supra,* 534 U.S. at pp. 119-121; *Sanders, supra,* 31 Cal.4th at p. 333), the privacy rights outlined in *Riley, supra,* 189 L.Ed.2d 430, are still at issue and given defendant's overbreadth objection, should have been considered by the trial court in determining whether the search condition could be more narrowly tailored. As the *Riley* court noted in discussing the capabilities of cell phones, there is an application for everything. (*Riley*, at p. 448.) " '[A]pps' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase 'there's an app for that' is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life." (*Ibid.*) As discussed *ante*, the search condition here is unreasonable because it gives officers access to all of this data without any nexus to defendant's present crimes, or past crimes or misconduct, or defendant's history and circumstances. The trial court made no effort to tailor the search condition to allow access only to those applications that are reasonably related to potential future criminality.

The majority observes that, while the electronic search condition "serves the state's legitimate interest in monitoring defendant's rehabilitation," it also "permits unprecedented intrusion into his private affairs -- and it does so on a record that demonstrates little likelihood, or even possibility, that evidence of illegal activity will be found in the devices the condition subjects to warrantless search." (Maj. opn., *ante*, at pp. 17-18.) This statement illustrates the problematic nature of narrowly tailoring the condition when there is no nexus supporting its imposition. It is difficult to conceive of a way in which an electronic search condition could be narrowly tailored where the record demonstrates "little likelihood, or even possibility, that evidence of illegal activity will be found in the devices the condition subjects to warrantless search." (Maj. opn., *ante*, at p. 18; cf. *P.O.*, *supra*, 246 Cal.App.4th at p. 298 [according to the juvenile court, the condition's purpose is to allow monitoring of the minor's involvement with drugs, but the condition does not limit the types of data that may be searched in light of this purpose; instead, it permits review of all sorts of private information that is highly unlikely to shed any light on whether the minor is complying with the conditions of his probation, drug-related or otherwise].)

Moreover, the electronic search condition could negatively impact defendant in ways that make it less likely he will successfully complete probation and become a productive, law abiding member of society. As I have noted, the search condition almost certainly will chill communications between defendant and the victim. Additionally, as worded, the search condition could affect his relationship with employers if he has "control" over a computer or other electronic devices on the job or because there are electronic communications between defendant and his employer, coworkers, or customers. The record is silent on whether defendant uses electronic devices at his job (or if he is even employed), but that is exactly the point. Before issuing a search condition, a trial court should make an effort to become aware of such information so that

it does not impose a search condition that is both overbroad and counterproductive to defendant's "reform and rehabilitation."

C. Narrow Tailoring

1. "Control"

It does not appear that the search condition here is limited to electronic devices owned by defendant, but rather extends to such devises under his "control." In pertinent part, the search condition refers to "electronic storage devices, and any object under his/her control, including but not limited to cell phones and computers." (See fn. 7, *ante*.) Search conditions must be interpreted on the basis of what a reasonable person would understand from the language of the condition itself. (*Bravo*, *supra*, 43 Cal.3d at p. 607; *People v. Sandee* (2017) 15 Cal.App.5th 294, 301.) In the absence of further clarification in the wording of the search condition, "control" in this context is reasonably understood to include constructive possession as well as actual possession or ownership. " 'Constructive possession does not require actual possession but does require that a person *knowingly exercise control* or *the right to control a thing*, either directly or through another person or persons.' " (*People v. Barnes* (1997) 57 Cal.App.4th 552, 555, italics added.) The scope of search conditions related to physical places typically focuses more on areas within defendant's control (e.g., home, vehicle, person) and defendant's actual or constructive possession of items found therein, not ownership. Also, traditional notions of possession do not necessarily apply to *access* to applications, Internet activity, and social media accessible in electronic devices. A defendant could have physical control over, and thus possession of, someone's electronic device, but not have *access* to the contents thereof. Thus, the search condition here was not narrowly tailored to allow

searches only of electronic devices owned by defendant or those to which the defendant had access to the applications, data and other items contained therein.[14]

As I have noted, the court in *Malik J.* suggested that electronic search conditions should not extend to devices owned by other members of the household. (*Malik J., supra*, 240 Cal.App.4th at pp. 905-906.) Given the lack of supporting evidence in this case, I conclude that the electronic search condition here should not apply to electronic devices exclusively owned or used by other members of the household where defendant

---

[14] I also note that the reference to searching devices over which defendant has "control" is not necessarily consistent with other wording in the search condition or the very statutes upon which the probation condition here is based, the ECPA. The express language of the probation condition here states that having been "advised of his/her constitutional and *statutory rights pursuant to Penal Code section 1546 et seq*.," defendant waived those constitutional and statutory rights and "specifically consented to searches of *his/her* electronic storage devices." (Italics added; see fn. 7, *ante*.) Thus, it appears that defendant only consented to searches of *his* devices. Moreover, the ECPA contains provisions that are inconsistent with allowing searches of the electronic devices owned by other people simply because defendant might be perceived by an officer as having "control" over those devices. Section 1546.1, subdivision (c)(4), provides that "[a] government entity may access electronic device information by means of physical interaction or electronic communication" when "the authorized possessor of the device" gives "specific consent," hence the statutory reference to the waiver of defendant's rights under the ECPA in the written probation condition. Subdivision (c)(10) of section 1546.1 provides that government entities can access electronic devices "if the device is seized from an *authorized possessor* of the device who is subject to an electronic device search as a clear and unambiguous condition of probation, mandatory supervision, or pretrial release." (Italics added.) Section 1546, subdivision (b), defines " '[a]uthorized possessor' " as "the owner of the device" or a person who "has been authorized to possess the device by the owner of the device." Consequently, having "control" over a device as the term "control" is typically understood in search conditions, is not necessarily the same as being an "authorized possessor" within the meaning of the statute. Defendant may not have the authority to give consent under the ECPA to search devices owned by other people even though he might have physical control over them. However, defendant's objections to the search condition here are limited to *Lent* and constitutional overbreadth. Defendant made no statutory objection and any such argument is forfeited. (See *People v. Cook* (2006) 39 Cal.4th 566, 594 [defendant has forfeited any statutory error by failing to state the specific ground for his objection].)

resides or to devices owned by any other third parties. On this record, the search condition is constitutionally overbroad as currently worded.

Tailoring the search condition to limit it to electronic devices owned by defendant would address the problem related to the privacy interests of third parties who might own electronic devices over which defendant has physical control. It would also make clear to officers in the field the scope of the search condition. In any event, for an electronic search condition to be narrowly tailored, it necessarily must identify the devices to be searched based on the probationer's connection to those devices and the applications, data, and other items contained therein.

2. Additional Tailoring

P.O., supra, 246 Cal.App.4th 288, provides an example of a case where the electronic search condition was valid under *Lent* but nevertheless constitutionally overbroad. In that case, the trial court stated the purpose of the search condition was to monitor the minor's drug use. (*P.O.*, at p. 293.) The condition required the minor "to submit to warrantless searches of his 'electronics including passwords.' " (*Id*. at p. 291.) The Court of Appeal observed: "the condition's purpose is to allow monitoring of [the minor]'s involvement with drugs, but the condition does not limit the types of data that may be searched in light of this purpose. Instead, it permits review of all sorts of private information that is highly unlikely to shed any light on whether [the minor] is complying with the other conditions of his probation, drug-related or otherwise." (*Id*. at p. 298.) The *P.O.* court required that the condition be modified "to limit authorization of warrantless searches of [the minor]'s cell phone data and electronic accounts to media of communication reasonably likely to reveal whether he is boasting about drug use or otherwise involved with drugs." (*Ibid*.) Additionally, the court limited the requirement to provide passwords to those accounts described. It also expressly stated that the minor was not required to provide passwords to other accounts. (*Ibid*.) While I do not

necessarily endorse the wording of the court's revised search condition, *P.O.* is an example of the need to narrowly tailor electronic search conditions.

The court in *Appleton, supra,* 245 Cal.App.4th 717, required the search condition to be more narrowly tailored in light of the nature of electronic data. The electronic search condition in that case read: " 'Any computers and all other electronic devices belonging to the defendant, including but not limited to cellular telephones, laptop computers or notepads, shall be subject to forensic analysis search for material prohibited by law. You shall not clean or delete internet browsing activity on any electronic device that you own and you must keep a minimum of four weeks of history.' " (*Id*. at p. 721.) The trial court limited the search condition to a search for " 'material prohibited by law,' " and expressly stated that the reason it imposed that condition was because social media was involved in the offense. (*Id*. at p. 721.) Even as limited by the trial court, the *Appleton* court concluded that the search condition was unconstitutionally overbroad as worded and remanded the matter to the trial court to consider whether it could impose a valid condition more narrowly tailored to the state's interests. (*Id*. at p. 727.)

In *Malik J., supra,* 240 Cal.App.4th 896, the court noted several ways in which the search condition in that case could be modified to protect the privacy interests of the minor given the nature of electronic devices and at the same time advance the state's interests. It noted that officers "should not be allowed to conduct a forensic examination of the device utilizing specialized equipment that would allow them to retrieve deleted information that is not readily accessible to users of the device without such equipment." (*Id*. at p. 904.) Additionally, officers should also "disable the device from any Internet and cellular connection" so as to limit the search to information stored on the device and thus limit the search to that which is in the probationer's possession and control. (*Ibid*.)

In a more recent case, *In re Q.R.* (2017) 7 Cal.App.5th 1231, review granted April 12, 2017, S240222 (*Q.R.*), the court concluded significant access to defendant's electronic data was required and the search condition was not overbroad. In *Q.R.*, the

minor was placed on probation for child pornography and extortion after he took video and photos of his girlfriend and then threatened to make them public after they broke up unless she paid him money and had sex with another boy. (*Id*. at p. 1233.) The trial court imposed an electronic search condition which required the minor to " '[s]ubmit all electronic devices under [his] control to a search of any *text messages, voicemail messages, call logs, photographs, email accounts and social media accounts*, with or without a search warrant, at any time of the day or night, and provide the probation or peace officer with any passwords necessary to access the information specified.' " (*Id*. at p. 1234, italics added.) While the parties and the *Q.R.* court did not address *Lent* (presumably because of the clear nexus between electronic device use and the crime), the court did address the minor's claim that the search condition was overbroad. The court held: "Given the direct relationship between minor's offenses and his use of an electronic device, we find the search condition appropriately tailored and we will affirm." (*Q.R.*, at p. 1233.) The court went on to explain: "the purposes of the electronic search condition here—ensuring that minor does not continue to use electronic devices to commit crimes—cannot be accomplished by a superficial search. The need for robust access is particularly critical given that minor previously stored illegal content in a password-protected application." (*Id*. at p. 1236.) And yet, even this "robust access" did not authorize probation officers or law enforcement to access financial or medical applications or websites or sources of data other than text messaging, voicemail messaging, call logs, photographs, email, and social media accounts.

The search condition at issue here is in need of narrow tailoring to appropriately balance, on one hand, privacy interests and, on the other hand, the degree to which it is needed for the promotion of legitimate governmental interests such as supervising defendant's probation and safeguarding the community. (*Knights, supra*, 534 U.S. at pp. 118-119; *Sanders, supra*, 31 Cal.4th at p. 333.) However, in my view, before tailoring of the search condition may even be undertaken, the trial court (rather than this

court in the first instance) should determine whether an electronic search condition is in fact warranted and for what particular purpose. If the trial court were to conclude that an electronic search condition is appropriate, the court could define the parameters of the state's interest in the context of *this* case and what is reasonably necessary to serve the government's legitimate interest. Then the court could consider what it would take to advance the state's interest and balance that interest against defendant's diminished, but not insignificant, privacy interests and the privacy interests of third parties, particularly the victim. Authorization to search should be limited to applications, data and other items reasonably likely to be relevant to the purpose of the search condition, for example, applications defendant could use to communicate with the victim. Because communications between defendant and the victim that took place before the grant of probation cannot constitute violations of probation conditions, the court should consider limiting searches to communications with the victim that took place after the grant of probation and imposition of the search condition. Moreover, depending on the circumstances that may be developed in the trial court, it may be appropriate to expressly limit the search condition to electronic devices *owned* by defendant. In light of the fact that a no-contact restraining order was not issued, and especially if it turns out that defendant and the victim are cohabiting, the trial court should also consider whether it is appropriate to deny access to geolocation data. To ensure that electronic searches are not executed arbitrarily, capriciously, for purposes of harassment, or in a way not consistent with the purpose of probation, the trial court might consider requiring that all electronic searches be executed in the presence of the probationer.

In summary, among the individualized factors that the trial court may consider in imposing and tailoring electronic search conditions are the following: the justification and purpose for the search condition; what types of devices will be subject to search; whether those devices will be limited to those owned by probationer, in probationer's possession and for which he has access to the applications, data or other items officers are

authorized to access, or for which the defendant is an "authorized user"; whether it is necessary to permit access to all information contained in the electronic devices or whether the search should be limited to specific applications, data or information; whether it is necessary to limit access to communications between defendant and specified individuals; whether the search may involve forensic analysis, including accessing data which has been deleted and accessing password protected data; whether it is permissible for the search to take place in some location other than where the electronic device is found; whether defendant must be present for the search; the privacy rights of the victim and third parties, and whether the scope of the search condition will be counterproductive to defendant's reformation and rehabilitation. This list is not exhaustive.

IV. Conclusion

In my view, electronic search conditions should not be imposed as "a matter of routine," but rather only if deemed appropriate after consideration of facts specific to the case. (See *Trujillo, supra,* 15 Cal.App.5th at p. 583.) Thus, the task of trial courts in imposing electronic search conditions does not lend itself to a one-size-fits-all approach. There must be a nexus between the electronic search condition and either (1) defendant's present crime, *or* (2) defendant's past crimes or misconduct, *or* (3) defendant's background, history and circumstances. A search condition should be closely tailored to the purposes for which it is imposed on each individual probationer. Additionally, it is my view that it is the professional obligation of the probation department and the attorneys appearing before the courts to inform the courts of all relevant circumstances and to make recommendations tailored to the facts of each case. I of course realize that perfect tailoring is " 'impossible, and that practical necessity will justify some infringement' " (*J.E., supra,* 1 Cal.App.5th at p. 803; *E.O., supra,* 188 Cal.App.4th at p. 1153); however, when an overbreadth objection is made, trial courts are constitutionally obligated to attempt to closely tailor probation conditions that impose

limitations on constitutional rights. I am mindful of the trial courts' workload and the demands of high volume calendar departments where many negotiated case resolutions take place, and that this approach calls for more time and consideration in connection with each case to which such a condition may be relevant. However, I am also of the opinion that this is what the law demands.

/s/
MURRAY, J.