SUMMARY
February 16, 2023

2023COA16

No. 20CA1503, *People v. Silvanic* — Criminal Law — Sentencing — Colorado Sex Offender Lifetime Supervision Act of 1998 — Sex Offender Intensive Supervision Probation

The defendant, a convicted sex offender, appeals the district court's denial of his objection to the probation department's request to continuously monitor all aspects of his electronic devices and internet usage. As a matter of first impression, a division of the court of appeals concludes that before imposing a condition that subjects a probationer to ongoing, unfettered monitoring of their electronic devices and internet usage, the district court must (1) make sufficient factual findings concerning the extent of the electronic monitoring necessary to accomplish the legitimate purposes of the probationary sentence, and (2) evaluate whether less restrictive means are available to achieve those ends. Because

the court failed to make such findings and conclusions, the division reverses the order and does not reach the defendant's First and Fourth Amendment challenges.

The dissent concludes that there is no material difference between the subject monitoring condition and other previously approved sex offender intensive supervised probation conditions that the defendant does not challenge on appeal. To the extent there are material differences, the dissent concludes that the additional restrictions are warranted given the nature of the defendant's convictions.

The dissent also addresses the defendant's remaining constitutional challenges, concluding that any impingement the monitoring condition imposes upon the defendant's First or Fourteenth Amendment rights is substantially outweighed by the government's interest in ensuring he complies with the terms and conditions of his probation.

COLORADO COURT OF APPEALS **2023COA16**

Court of Appeals No. 20CA1503
Weld County District Court No. 18CR2132
Honorable Vincente G. Vigil, Judge

The People of the State of Colorado,

Plaintiff-Appellee,

v.

Justin Daniel Silvanic,

Defendant-Appellant.

ORDER REVERSED

Division IV
Opinion by JUDGE SCHUTZ
Graham*, J., concurs
Grove, J., dissents

Announced February 16, 2023

Philip J. Weiser, Attorney General, Frank R. Lawson, Assistant Attorney General, Denver, Colorado, for Plaintiff-Appellee

Megan A. Ring, Colorado State Public Defender, Brian Sedaka, Deputy State Public Defender, Denver, Colorado, for Defendant-Appellant

*Sitting by assignment of the Chief Justice under provisions of Colo. Const. art. VI, § 5(3), and § 24-51-1105, C.R.S. 2022.

¶ 1 Appellant, Justin Daniel Silvanic, asks us to conclude that the district court's order requiring him to submit to ongoing monitoring of all uses of his personal electronic devices and the internet is an unnecessarily broad method of achieving the legitimate purposes of his probation sentence and infringes upon his constitutional rights. Because it does not comply with our statutory requirements for the imposition of probation conditions restricting a defendant's constitutional rights, we reverse the district court's order permitting unfettered monitoring of Silvanic's electronic devices and internet usage.

I. Background Facts and Procedural Posture

¶ 2 Silvanic was charged with one count of sexual assault on a child by one in a position of trust and one count of sexual assault on a child as part of a pattern of abuse. The charges against Silvanic, who was twenty-nine years old at the time, were based on allegations that he sexually assaulted his friend's fifteen-year-old daughter, H.F.

¶ 3 The allegations detailed Silvanic's use of electronic communications to facilitate the assault. He anonymously contacted H.F. through text messages sent to her phone. In

response, H.F. blocked these numbers, and her parents changed her phone number. But Silvanic continued to anonymously send H.F. text messages. Over time, H.F. began to suspect the texts were from Silvanic. Although he denied being the source of the texts, Silvanic told H.F. that he thought she was "pretty" and that he was attracted to her. He then texted her invitations to come to his home while her parents were at work.

¶ 4 Over the next few months, Silvanic texted H.F.'s parents with offers to pick her up from school. He used these times to be alone with H.F. and initiate sexual contact. Subsequently, Silvanic texted H.F., suggesting that she send him nude photographs. Thereafter, Silvanic and H.F. exchanged sexual photographs by text.

¶ 5 In January 2018, H.F.'s mother returned home early from work. She found H.F. naked in her bedroom with Silvanic's work clothes by her bed and Silvanic naked in the bathroom. H.F.'s mother filed a police report, and the district attorney filed sexual assault charges against Silvanic.

¶ 6 Prior to trial, Silvanic entered a written waiver and guilty plea to one count of criminal attempt to commit sexual assault on a child by one in a position of trust. The plea agreement called for a

probationary sentence pursuant to Sex Offender Management Board (SOMB) standards and offense-specific treatment.

¶ 7 In advance of the sentencing hearing, the district court received a presentence investigation report and a sex offense specific evaluation (SOSE) of Silvanic. The SOSE revealed that Silvanic was at a high level of denial, lacked accountability for the offense, and blamed H.F. for the unlawful sexual contact. The SOSE also revealed that Silvanic had impulse control problems and did not recognize his various risk factors.

¶ 8 At the sentencing hearing, and consistent with the court's identified accountability concerns, Silvanic tried to excuse his actions by suggesting that H.F. sought him out, in part, for comfort because of her parents' alleged alcohol abuse. Silvanic did admit to attempted sexual assault, but he also minimized his culpability by stating, "I feel that it takes two to tango." The district court initially expressed hesitation about accepting the plea agreement, but after Silvanic clarified that he understood that it was wrong to blame H.F. for what happened, the court agreed to a probationary sentence. The court then sentenced Silvanic to ten years of sex offender intensive supervision probation (SOISP).

¶ 9 The proposed conditions of his probation included, among other things, four requirements relevant to this appeal. Standard condition five, in pertinent part, read, "I will submit to a search of my person, property, residence, vehicle, or personal effects, including but not limited to any electronic devices, by the probation officer when there are reasonable grounds to search."

¶ 10 Proposed SOISP condition nineteen stated,

> I will not use computer systems, [i]nternet-capable devices, or similar electronic devices (to include but not be limited to satellite dishes, PDA's, electronic games, web televisions, [i]nternet appliances, and cellular/digital telephones) in a manner that violates my supervision conditions or the requirements of the signed "Computer Use Agreement for Sex Offenders."[1] Additionally, I will allow the probation officer, or other trained person, to conduct searches of computers or other electronic devices used by me. The person conducting the search may include a non-judicial employee and I may be required to pay for such a search.

¶ 11 Proposed SOISP condition twenty-four included the following language:

> I will only use or access computer systems, [i]nternet-capable devices, and/or similar

[1] For reasons that are unexplained, no Computer Use Agreement for Sex Offenders is included in the record on appeal.

> electronic devices . . . for the following purposes:
>
> □ Employment (including seeking employment)
> □ School
> □ Other: _____
>
> Use of any computer systems, [i]nternet-capable devices, and/or similar electronic devices for any purpose not authorized herein is strictly prohibited absent prior approval from the probation officer.

None of the optional checkboxes were marked.

¶ 12 Finally, proposed SOISP condition twenty-nine, in relevant part, read, "I will not access or utilize, by any means, any commercial social networking site except under circumstances approved in advance and in writing by the probation officer in consultation with the community supervision team."

¶ 13 Silvanic objected to proposed SOISP conditions twenty-four and twenty-nine on the grounds that they violated his First and Fourth Amendment rights. Silvanic did not object to any other condition.

¶ 14 After receiving briefing and holding a hearing on the issue, the court entered a written order on July 14, 2020 (July order), in which it struck both conditions twenty-four and twenty-nine. In

striking these two conditions, the district court rejected the People's argument that Silvanic could be prohibited from any use of the internet or possession of electronic devices. Similarly, the court rejected the requirement that Silvanic's use of the internet and connected devices be approved in advance by his probation officer in consultation with his community supervision team.

¶ 15 In the place of these conditions, the court entered less restrictive conditions designed to meet the purposes of Silvanic's probation without unnecessarily infringing on his rights to access the internet and use electronic devices. Specifically, the court ruled,

> The Defendant is to disclose and specifically identify to his probation officer the possession or use of any internet capable device, including, but not limited to, any computers, laptops, cellular telephones, gaming systems, or any other device capable of accessing the internet. If any new possession or use occurs the Defendant is to immediately disclose such possession or use to his probation officer.
>
> The Defendant is to disclose and specifically identify to his probation officer any internet related accounts he currently has, to include email accounts, social media accounts, gaming accounts, message board accounts, financial accounts, commercial accounts, or any other accounts related to internet activities. If any

> new accounts are created, the Defendant is to immediately notify his probation officer of their creation.
>
> The Defendant is to provide all usernames, email addresses, and passwords for any of the above accounts to his probation officer, and to disclose the same information if new accounts are created, or if there is any change to the username, email address, password, or other account information.
>
> The Defendant is not to delete any information associated with his internet usage during the period of his probation, to include browser history, messaging history, sent or received emails, or any other information documenting or arising as a result of his activities on the internet.
>
> Nothing in these additional conditions is to be construed as modifying Standard Condition of Supervision number five as currently written.

¶ 16 Thus, by virtue of the July order, Silvanic was permitted to use electronic devices and the internet, subject to the requirement that he disclose the devices he was using and provide the associated usernames, email addresses, and passwords to his probation officer. In the final paragraph of the July order, the court reiterated that the newly fashioned additional conditions would not be deemed to modify condition number five, which permitted the

probation officer to search any of Silvanic's property, including electronic devices "when there are reasonable grounds to search."

¶ 17 Neither party appeals the July order.

II. The Probation Officer's Demand for Continuous Monitoring

¶ 18 Shortly after entry of the July order, Silvanic's probation officer ordered him to enroll, at his own expense, in a program to monitor his electronic devices. The proposed electronic monitoring agreement provided,

> The employee of [the monitoring company] may view any and all content on [the] device which includes, but [is] not limited to, text messages (SMS & MMS), instant messages, call logs, internet history, photo logs, video logs, applications/software installed/used, screenshots, online searches, document tracking, files transferred, keystrokes, GPS location and email content. Data collected could include sensitive information, such as passwords and conversations with attorneys.

The agreement also provided,

> All information obtained by employees of [the monitoring company] can be provided to a representative of your supervision team to include, but not limited to, your supervising officer, therapist, pre-sentence investigator, or other supervising official. I will not be given any logs or reports without a court order.

¶ 19 Silvanic objected to the monitoring agreement on the grounds that it was inconsistent with the modified conditions of his probation and violated his Fourth Amendment right to be free from unlawful searches.[2] He argued that the monitoring agreement contemplated ongoing surveillance of his phone and did not comply with standard probation condition five, which required the probation department to have "reasonable grounds" before searching his property. Silvanic also argued that subjecting him to a search at all times without reasonable grounds violated his Fourth Amendment right to be free from governmental searches absent reasonable suspicion of wrongdoing. Moreover, he argued,

---

[2] Silvanic's written objection asserts the monitoring software would apply to "all internet capable devices." As our colleague in dissent notes, Silvanic's arguments in the objection specifically refer to the installation of the monitoring software on his phone. But on appeal, both parties assume and argue that the contemplated monitoring program would apply to all of Silvanic's electronic devices and internet use. We note that the district court's order interpreted the objection to apply to condition nineteen, which addresses Silvanic's use of all internet-capable devices. We also note that the extensive disclosure requirements set forth in the district court's July order apply to any internet device in Silvanic's "possession or use." Given these conditions, and the absence of record support for any alternative electronic devices that would be excluded from the monitoring condition, we are unable to assume the existence of such alternatives.

constant surveillance would inhibit all of his communications, and could reveal medical information, religious affiliation, political affiliations, and other sensitive and private information, including communications with his attorney.

¶ 20 The People contended that the monitoring agreement is consistent with the probation conditions that Silvanic had agreed to abide. The People suggested that if Silvanic didn't like the probation requirements, he could simply self-revoke his probation in favor of a prison sentence.

¶ 21 No hearing was held to address Silvanic's objection, and the district court resolved the dispute by entering a written order on September 29, 2020 (September order). The court construed the objection as pertaining to SOISP condition nineteen — which authorized the probation officer or other trained person to conduct "searches of [Silvanic's] computers or other electronic devices." The court denied the objection, concluding that its review of the facts demonstrated that Silvanic was

> willing to attempt to circumvent an attempt by the victim . . . to prevent communication by attempting to contact her on unfamiliar numbers after his original number was blocked . . . that he shows little accountability

> for this offense, [and that he] repeatedly placed the blame for this offense on the victim and her parents.

In view of these facts, the district court concluded that Silvanic was "at a high risk of attempting to cover up and minimize illicit behavior," and that the "monitoring condition" was appropriately imposed. The court's order did not address whether any of these concerns could be addressed in a manner that was less restrictive than that contemplated by the monitoring agreement.

¶ 22 Silvanic now appeals the September order.

III. Discussion

¶ 23 Silvanic contends the district court erred by denying his objection to the monitoring condition.[3] He attacks the condition's validity on three grounds: (1) there are less restrictive means[4] of

---

[3] Although on appeal Silvanic framed the legal issue as a challenge to SOISP condition nineteen (presumably in response to the district court's framing of the objection), we have reframed the argument because Silvanic does not contend that SOISP condition nineteen is invalid in its entirety; rather, he argues, the monitoring condition is invalid.

[4] Silvanic and the People both use the phrase "narrowly tailored" when discussing this issue. The district court used the phrase "least restrictive" in its September order. We use the phrase "less restrictive" because it comports with our existing precedent analyzing the enforceability of probation conditions that restrict constitutional rights.

achieving the legitimate purpose of his probation; (2) it permits the government to engage in unreasonable searches of his electronic devices and internet use in violation of the Fourth Amendment because the monitoring condition requires no particularized suspicion prior to the search; and (3) it imposes an unlawful penalty on his Fourth Amendment right because the only way he can avoid the allegedly unlawful search is by forfeiting his First Amendment right to use the internet. We conclude the first issue is dispositive and thus do not reach Silvanic's remaining constitutional challenges.

A. Standard of Review and Relevant Law

¶ 24 Generally, a sentencing court has discretion in determining the appropriate conditions of probation. *People v. Fleming*, 3 P.3d 449, 451 (Colo. App. 1999). Our review is limited to determining whether a sentencing court abused this discretion by imposing a particular condition. *People v. Brockelman*, 933 P.2d 1315, 1319 (Colo. 1997).

¶ 25 But a sentencing court's imposition of probation conditions is not without limitation. Any condition that restricts a constitutional right must serve the statutory purposes of a probation sentence,

and the court must consider whether less restrictive means of achieving that objective are available. *Id.* (applying this standard to restrictions on the right to travel); *People v. Landis*, 2021 COA 92, ¶¶ 13-20 (applying the standard to a probation condition restricting the defendant's use of the internet and social media); *People v. Cooley*, 2020 COA 101, ¶ 31 (applying the standard to conditions of SOISP probation prohibiting contact with family members under the age of eighteen); *People v. Forsythe*, 43 P.3d 652, 654-55 (Colo. App. 2001) (applying the standard to a condition requiring probationer's contact with her child to be supervised). Numerous jurisdictions have applied the same or a similar standard to probation conditions requiring a defendant to submit to monitoring of their electronic devices. *See, e.g.*, *United States v. Shiraz*, 784 F. App'x 141, 145 (4th Cir. 2019) (per curiam) (vacating order approving probation condition that permitted unfettered monitoring of sex offender's computer because the condition "involves a greater restriction of liberty than is reasonably required"); *State v. Bouchard*, 2020 VT 10, ¶¶ 18-27, 228 A.3d 349, 357-61 (probation condition authorizing limitless monitoring of a probationer's computer and internet use is not "sufficiently well defined and narrowly tailored"

to comply with Vermont constitutional and statutory law). We consider de novo whether a probation condition was properly imposed. *Cooley*, ¶ 26.

¶ 26 The purposes of a probation sentence are articulated by the legislature and courts through statute and case law. Section 18-1.3-202(1)(a), C.R.S. 2022, provides that a district court may grant a defendant a sentence to probation rather than a term of incarceration when "the ends of justice and the best interest of the public [and] the defendant . . . [are] served." Because it affords a defendant an opportunity to avoid incarceration, courts have described probation as "a privilege, not a right." *People v. Smith*, 2014 CO 10, ¶ 8.

¶ 27 The probation conditions imposed serve the "dual purpose[s] of enhancing the reintegration of the offender into a responsible lifestyle and affording society a measure of protection against recidivism." *Brockelman*, 933 P.2d at 1318-19 (quoting *People v. Ressin*, 620 P.2d 717, 719 (Colo. 1980)). To effectuate these dual purposes, Colorado courts generally require that probation conditions be reasonably related to a defendant's rehabilitation and the purposes of probation. *Landis*, ¶ 10.

¶ 28 As a probationer, Silvanic has a significantly diminished expectation of privacy and liberty. *People v. Samuels*, 228 P.3d 229, 236 (Colo. App. 2009). By statute, the sentencing court may impose "a host of conditions on probationers curtailing their liberty." *Id.* And when a probationer, like Silvanic, is sentenced to SOISP, the court can impose standard conditions and additional conditions that further curtail the probationer's liberty. *Id.*

¶ 29 SOISP is authorized by statute. § 18-1.3-1007, C.R.S. 2022. In section 18-1.3-1007(2), the General Assembly has specified,

> The judicial department shall require that sex offenders and any other persons participating in the intensive supervision probation program created pursuant to this section receive the highest level of supervision that is provided to probationers. The intensive supervision probation program may include but not be limited to severely restricted activities, daily contact between the sex offender or other person and the probation officer, monitored curfew, home visitation, employment visitation and monitoring, drug and alcohol screening, treatment referrals and monitoring, including physiological monitoring, and payment of restitution. In addition, the intensive supervision probation program shall be designed to minimize the risk to the public to the greatest extent possible.

¶ 30 Thus, the clear mandate of SOISP is to subject sex offenders to the highest level of supervision that is available for probation. But this broad mandate does not permit sentencing courts to impose conditions of probation that violate constitutional strictures or are otherwise contrary to law. *Cooley*, ¶ 26.

¶ 31 We apply a five-factor test to determine whether a particular probation condition is "reasonably related to the statutory purposes of probation":

> (1) whether the restriction is reasonably related to the underlying offense; (2) whether the restriction is punitive to the point of being unrelated to rehabilitation; (3) whether the restriction is unduly severe and restrictive . . . ; (4) whether the defendant may petition the court to lift the restriction temporarily when necessary; and (5) whether less restrictive means are available.

Brockelman, 933 P.2d at 1319.

¶ 32 Because we determine it is dispositive, we address the last *Brockelman* factor first.

B. Whether Less Restrictive Means Are Available

¶ 33 The question of whether the monitoring condition ordered by the probation department is statutorily authorized depends on whether the court considered the availability of less restrictive

means than the monitoring agreement to achieve the legitimate ends of Silvanic's probation sentence. We begin this analysis by returning to the substance of the district court's September order.

¶ 34 The court reasoned, "The monitoring conditions at issue in the latest motion were previously imposed as [SOISP] condition nineteen." We disagree with this conclusion. Condition nineteen did not authorize ongoing, continuous monitoring of all Silvanic's electronic devices and internet usage. Rather, it provided, "I will allow the probation officer, or other trained person, to conduct searches of computers or other electronic devices used by me. The person conducting the search may include a non-judicial employee and I may be required to pay for such a search."

¶ 35 The operative term in condition nineteen is "search," not continuous, all-encompassing monitoring. As the district court noted in its July order, the term "search" is also addressed in standard condition five, by which Silvanic consented to the "*search* of my person, property, residence, vehicle, or personal effects, including but not limited to any electronic devices, by the probation department officer *when there are reasonable grounds to search*."

(Emphasis added.) Taken together, what these conditions authorize is a search, not ongoing, unlimited monitoring.[5]

¶ 36 Reasonable grounds to search a probationer exist when there is "reasonable suspicion" that they "violated conditions of his probation." *Samuels*, 228 P.3d at 238. But nothing in the record suggests that the constant monitoring the probation department ordered was based on such "reasonable suspicion." Indeed, when demanding that Silvanic agree to this ongoing condition, and in defending their demand to the district court, the People did not identify a "reasonable suspicion" that Silvanic was using or intended to use electronic devices or the internet to violate the terms of his probation. Rather, the request for ongoing monitoring was grounded in matters of convenience, particularly to free the probation officer from the burdens of having to conduct periodic searches. Constant, ongoing monitoring may be most

---

[5] For these reasons, we respectfully disagree with our dissenting colleague's conclusion that there is little that distinguishes condition nineteen from continuous monitoring. As noted, the district court expressly stated in its July order that the additional conditions remained subject to condition five, which permits searches of Silvanic's property when there are reasonable grounds to search.

administratively convenient to the probation department, but it does not equate to reasonable suspicion.

¶ 37 Moreover, reasonable suspicion to search contemplates a search that is focused on particular items of property that the probation officer has reasonable grounds to believe will be or have been used by the probationer to violate the terms and conditions of their probation. The reasonable suspicion standard does not contemplate unfettered, continuous searching of all of a probationer's property, electronic or otherwise. Rather, the scope of a search is limited to those portions of a probationer's property that contain evidence of the probation violation. But the surveillance requested by the People does not relate to specific items of property. Rather, it contemplates continuous monitoring of all of Silvanic's electronic communications. Thus, the district court erred by concluding that the requested monitoring was authorized by condition nineteen.

¶ 38 After referencing condition nineteen, the district court went on to assess whether continuous monitoring was reasonably related to Silvanic's underlying offense. As previously noted, the court emphasized that Silvanic used electronic devices, including various

deceptive phone numbers, to contact H.F. and manipulate her into a relationship that culminated in him sexually assaulting her. The court also credited the concerns expressed in the SOSE about Silvanic's impulsivity, his regular use of the internet to engage in online sexual behavior, his victim blaming and rationalizations for the crime, and his lack of genuine remorse. These findings have record support, and we agree that these facts may justify appropriately confined conditions designed to monitor Silvanic's future use of electronic devices and the internet.

¶ 39 Citing *Forsythe*, the district court went on to acknowledge that "the condition must be the least restrictive means available to accomplish the probation's legitimate purpose." But having acknowledged this requirement, the district court then failed to conduct any analysis of whether there were less restrictive means available to accomplish the defined objective. This omission is strikingly different from the less restrictive alternatives analysis the court conducted and implemented incident to the entry of its July order modifying conditions twenty-four and twenty-nine. In failing to apply the less restrictive *Brockelman* factor, the court erred. *See Cooley*, ¶ 36 ("With so little to go on — and without any immediately

apparent connection between [the probationer's offense and the condition] — we lack a sufficient record to apply the *Brockelman* factors."); *see also United States v. Matteson*, 327 F. App'x 791, 793 (10th Cir. 2009) (Gorsuch, J.) (vacating a district court order permitting unlimited monitoring of a probationer's computers and remanding to the district court for consideration in light of the boundaries of permissible computer monitoring).

¶ 40 The breadth of the monitoring agreement is remarkable. Without limitation in terms of time, duration, subject matter, and parties, the agreement allows the monitoring company to view "any and all" communications Silvanic may have via the internet or any electronic device.[6] All of the gathered information may be disseminated to Silvanic's probation officer and the treatment team. The agreement requires Silvanic to notify all users of covered electronic devices that the monitoring agreement is installed on the

---

[6] We appreciate that the monitoring agreement contained in the record is not signed and does not specifically identify any electronic device. But, as previously noted, Silvanic, the People, and the district court all proceeded on the understanding that the monitoring would be applied to all internet-enabled devices Silvanic used. This understanding is consistent with the other SOISP conditions requiring disclosure of all usernames and passwords for any electronic device Silvanic possessed or used.

device. The agreement also provides that the monitoring company "may, at any time, and at [the company's] sole discretion, modify the Agreement Terms of Use, with or without notice to [Silvanic]."

¶ 41 Given the breadth of these conditions, it is paramount that the district court meaningfully evaluate and make factual findings about the precise nature of electronic monitoring that is purportedly needed and any alternative means by which it may be accomplished. It is not sufficient to simply recite that Silvanic is a sex offender, his offense involved the use of a cell phone, and therefore continuous monitoring is permitted. Rather, the district court must determine what the legitimate safety concerns are and if there are less intrusive means of monitoring or searching that would adequately address those concerns. This analysis must also be mindful that the monitoring agreement ordered by the probation department gives the government unfettered access to Silvanic's private matters — such as his medical portals, his places of worship, data related to any financial support he may provide to political organizations, and the newspapers to which he subscribes and reads online — and severely restricts Silvanic's ability to communicate with his family and attorney confidentially.

¶ 42 As the United States Supreme Court recognized nearly a decade ago,

> 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 . . . .
>
> [And] there is an element of pervasiveness that characterizes cell phones but not physical records. . . . [I]t 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. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.
>
> . . . .
>
> 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.

Riley v. California, 573 U.S. 373, 394-96 (2014) (citations omitted).

¶ 43 The concerns the Supreme Court articulated in 2014 are amplified by our ever-increasing reliance upon electronic communications in all aspects of our personal, business, and social lives. The type of blanket prospective monitoring conditions ordered by the probation department would capture substantial amounts of information for which there may be no legitimate probationary purpose, and which may be privileged.[7]

¶ 44 Our district courts carry out an essential role, through the application of the *Brockelman* less restrictive alternatives factor, to ensure that an appropriate balance is struck between a probationer's constitutional rights and the government's legitimate interest in protecting the public. The district court did not conduct

---

[7] As noted by our colleague in fn. 3 of the dissent, the proposed monitoring agreement raises numerous other concerns regarding security issues and the potential for improper disclosure of a probationer's accounts, data, and information. However, because these issues were not raised by the parties on appeal, we decline to address them further.

that essential analysis before entering the September order. As a consequence, it erred by concluding that the requested monitoring condition was statutorily authorized. We therefore reverse the district court's September order.

C. Issues We Have Not Addressed

¶ 45 Recognizing that Silvanic remains on probation, it is important to emphasize the limitations of our holding. By reversing the district court's September order, we are not suggesting that the district court is proscribed from subjecting Silvanic to continuous monitoring of his electronic communications or internet activity as a condition of his probation. Rather, consistent with *Brockelman*, we hold that the district court must consider whether less restrictive alternatives to the imposed condition would accomplish the legitimate ends of Silvanic's probation sentence. If the People decide to pursue continuous monitoring of Silvanic's electronic devices as a condition in the future, it will be essential for the prosecution to establish why this intrusion is reasonably necessary beyond the conclusory assertion that Silvanic is a sex offender. The prosecution must also prove that no less restrictive means are available to achieve the legitimate purposes of Silvanic's probation.

Finally, the district court must make the necessary factual findings and apply the correct legal standard to evaluate if the prosecution has met its burden of proof that the condition is necessary and no less restrictive means are available.

¶ 46 It is also important to emphasize that our analysis is predicated upon whether the monitoring condition is consistent with the statutory authority for imposing probation conditions. We recognize that Silvanic has also raised constitutional arguments based upon assertions that the monitoring condition would violate his Fourth Amendment and First Amendment rights. Because we have concluded that the continuous monitoring condition does not meet statutory muster, we have refrained from addressing these constitutional challenges. *See*, *e.g.*, *People v. Butler*, 251 P.3d 519, 522 (Colo. App. 2010) ("[A] court should not decide a constitutional issue unless the necessity for such [a] decision is clear and inescapable.").

¶ 47 If the People pursue a continuous monitoring condition in the future, the court must determine whether the revised condition meets the *Brockelman* factors and address any constitutional issues that may be presented. We express no opinion regarding the level

of scrutiny that may apply to any constitutional challenges made to any future conditions that the People may seek to impose.

IV. Disposition

¶ 48 For the reasons stated, we reverse the district court's September 29, 2020, order.

JUDGE GRAHAM concurs.

JUDGE GROVE dissents.

JUDGE GROVE, dissenting.

¶ 49 I share some of the majority's concerns about the one-size-fits-all nature of the monitoring agreement, and I agree that, before imposing such intrusive requirements, courts should take care to strike an appropriate balance between achieving the goals of probation and respecting a sex offender's constitutional and statutory rights. In my view, however, that balance was struck here. I would therefore affirm the district court's imposition of the monitoring requirement.

¶ 50 Because it informs much of my analysis, it is important at the outset to recognize the scope of Silvanic's contentions on appeal. Although Silvanic makes much of the fact that the monitoring agreement allows for "constant surveillance"[1] of his internet-enabled devices, he does not challenge — or even acknowledge —

---

[1] The record does not make clear how the software installed under the monitoring agreement works, including how and when it transfers data reflecting device usage. If the software does not transmit data in real time, or if it is triggered only by specific activity or keywords, then "constant surveillance" may be something of a misnomer. It would be helpful, on remand, for the record to be supplemented with additional information about which devices the monitoring agreement is intended to cover and how it works in practice.

his express agreement to allow suspicionless searches of those same devices as a condition of his sex offender intensive supervised probation (SOISP). Specifically, as a condition of SOISP, Silvanic agreed to "allow the probation officer to search [his] person, property, residence, vehicle, or personal effects, including but not limited to any electronic devices, *at any time with or without [his] consent*." (Emphasis added.) Conditions of this type are commonplace for sex offender probation in Colorado and elsewhere. *See, e.g.*, *People v. Salvador*, 299 Cal. Rptr. 3d 266, 270 (Ct. App. 2022); *Commonwealth v. Feliz*, 159 N.E.3d 661, 667-69 (Mass. 2020).[2]

¶ 51 Nor does Silvanic challenge the order that the district court entered after withdrawing conditions twenty-four and twenty-nine,

---

[2] For sex offenders granted supervised release, the federal sentencing guidelines recommend "[a] condition requiring the defendant to submit to a search, at any time, with or without a warrant . . . by any probation officer in the lawful discharge of the officer's supervision functions." U.S. Sent'g Guidelines Manual § 5D1.3(d)(7)(C) (U.S. Sent'g Comm'n 2021). And on the state level, "[a] defendant's 'own parole [or probation] agreement and the state regulations applicable to his case' determine whether a search of a parolee or probationer is authorized by state law." *United States v. Mathews*, 928 F.3d 968, 976 (10th Cir. 2019) (citation omitted). As contemplated by *Mathews*, suspicionless searches are specifically permitted by the conditions of Silvanic's SOISP agreement.

which I will refer to as the "account-sharing requirement." That order requires Silvanic to

- disclose every internet-capable device that he owns or possesses, and immediately inform his probation officer of any "new possession or use" of internet-capable devices;
- provide to his probation officer a list of every "internet related account[]" he currently has or creates in the future, including email, social media, gaming, message board, commercial, and financial accounts;
- "provide all usernames, email addresses, and passwords for any of the above accounts to his probation officer, and to disclose the same information if new accounts are created, or if there is any change to the username, email address, password, or other account information";
- refrain from "delet[ing] any information associated with his internet usage during the period of his probation," including "browser history, messaging history, sent or received emails, or any other information documenting or arising as a result of his activities on the internet."

¶ 52 When considered together with the suspicionless search provision described above, the court's order encompasses virtually all of Silvanic's online activity. Equipped with account information, Silvanic's probation officer could — with or without cause, and apparently with or without notice — remotely log in to Silvanic's accounts at any time and view all of his communications, financial records, and search and browser history.

¶ 53 There may well be circumstances in which such intrusive measures are inappropriate, at least in the absence of adequate findings by the court imposing them. *See, e.g.*, *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010). But because Silvanic does not challenge the court's order directing him to provide account information to his probation officer, that issue is beyond the scope of this appeal. *See Compos v. People*, 2021 CO 19, ¶ 35 (emphasizing the importance of applying the party presentation principle). Thus, the only question we are left to answer is whether or not, in light of the substantially intrusive baseline set by the account-sharing requirement, the monitoring agreement satisfies Colorado's statutory requirements, or, alternatively, whether it impermissibly infringes on Silvanic's constitutional rights.

¶ 54 In contrast to the majority, I would answer this question by looking to the incremental differences between the court-ordered account-sharing requirement and the monitoring agreement that Silvanic challenges on appeal, keeping in mind that, based on the special conditions of SOISP, he has already agreed to allow suspicionless searches of his electronic devices (thus vitiating any complaint that the monitoring requirement violates the Fourth Amendment). I conclude that those incremental differences are not substantial because Silvanic's probation officer is already empowered to monitor all of his online activity in real time. Even without the monitoring agreement, Silvanic must give his probation officer access to all of his online activity and history — and is barred from deleting any of it — whether it exists on a phone, a laptop, or a device belonging to someone else.[3]

---

[3] Although not discussed by the parties on appeal, I note that the account-sharing requirement raises an immense number of information security concerns and technical questions. For example, how is Silvanic's account information protected? Even companies that exist for the sole purpose of securing passwords have proved to be vulnerable. *See, e.g.*, Lily Hay Newman, *Yes, It's Time to Ditch LastPass*, Wired, https://perma.cc/4TFF-MYLB. Relatedly, is the account-sharing requirement compatible with important security measures such as two-factor authentication?

¶ 55 The monitoring agreement states that the monitoring company "may view any and all content on device which includes, but [is] not limited to, text messages (SMS & MMS), instant messages, call logs, internet history, photo logs, video logs, applications/software installed/used, screenshots, online searches, document tracking, files transferred, keystrokes, GPS location and email content." It does not specify which device or devices it would cover, but the objection that Silvanic filed in the district court focused exclusively on his cell phone, and many of the categories listed are clearly targeted at mobile devices. Irrespective of the agreement's breadth, however, the key question is this: What information does the monitoring agreement cover that the account-sharing requirement does not?

¶ 56 For many categories of data, there is a clear overlap between the account-sharing requirement and the monitoring agreement. Most obviously, Silvanic's internet history, email content, files

---

See, e.g., Cybersecurity & Infrastructure Sec. Agency, *Multi-Factor Authentication (MFA)*, https://perma.cc/3QHN-3JZC. And what internal security measures does the probation department employ to ensure that Silvanic's personal information is not misused by those who have access to it?

transferred, and applications installed and used all rely on the internet and would thus be subject to the account-sharing requirement. Other categories may be less certain. For example, while the account-sharing requirement would not apply to data created by and stored solely on the device (such as photos, call logs, and GPS tracking information), it would cover online backups or mobile applications that make use of that data. (GPS data, for instance, can be shared with mapping software that tracks a user's location history and stores it in the cloud. *See, e.g.*, *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 350 (N.D. Ill. 2020) (noting that, "[i]f permitted by the user," GPS data collected by a user's phone "is often used by the applications (apps) installed on a device as part of its operation").) Likewise, whether messaging involves use of the internet and would thus be covered by the account-sharing requirement would depend in large part on the type of message and the messaging service used. *See, e.g.*, *Moore v. Apple, Inc.*, 73 F. Supp. 3d 1191, 1195-96 (N.D. Cal. 2014) (describing differences between SMS, MMS, and applications such as iMessage).

¶ 57 Given this degree of overlap, I simply do not see much daylight between the account-sharing requirement and the monitoring agreement, at least in terms of what information is available to Silvanic's probation officer. And to the extent that the monitoring agreement makes more of Silvanic's data available to the probation department than would otherwise be available, it satisfies the five *Brockelman* factors, which I turn to next.

¶ 58 First, the monitoring agreement is reasonably related to the underlying offense because it can be used to ensure that Silvanic does not again use spoofed phone numbers to groom a child victim — regardless of the device, service, or application used.[4] While Silvanic waived the factual basis for his guilty plea, it appears to be undisputed that he began grooming the victim via text message — which almost certainly involved the use of a cell phone

---

[4] Other provisions that may not be covered by the account-sharing requirement likewise ensure compliance with various conditions of SOISP. GPS data, for example, can be reviewed to ensure that Silvanic does not "enter onto the premises, travel past, or loiter where the victim resides," conduct that is prohibited by SOISP condition six. Similarly, monitoring the local storage of any devices that he possesses helps ensure that Silvanic does not "access, possess, utilize, or subscribe to any sexually oriented or sexually stimulating material," conduct that is prohibited by SOISP condition twenty-six.

(and if not, another device capable of sending such messages). To the extent that the monitoring requirement extends to any other internet-capable devices that Silvanic might own, it is "reasonable to place restrictions on [Silvanic's] use of a medium that easily can be used to facilitate contact with children," *People v. Landis*, 2021 COA 92, ¶ 14, particularly in light of the presentence investigation report, which noted Silvanic's difficulties with impulse control and the fact that "he engages in online sexual behaviors on a regular basis."

¶ 59 Second, the monitoring requirement is not punitive to the point of being unrelated to rehabilitation. Offenders on SOISP are closely supervised to reduce the risk that they will reoffend. *See* § 16-11.7-101(2), C.R.S. 2022. Monitoring online activity — and requiring Silvanic to pay for the cost of the monitoring — is not punitive but is instead a critical part of that supervision, particularly in light of the First Amendment implications that, as the district court recognized here, would arise if Silvanic were simply prohibited from using the internet at all.

¶ 60 Third, the monitoring requirement is not unduly severe and restrictive. Most importantly, it does not outright prohibit Silvanic

from using the internet. *Cf. Landis*, ¶ 5 (rejecting probationer's challenge to condition that "prohibit[ed] use of the internet and social media without prior approval from his probation officer" unless such usage was associated with his employment). And while some privileged communications could be exposed — emails to an attorney or physician, for example — that is no different from what the account-sharing requirement already permits. Moreover, as was the case in *Landis*, for sensitive communications, Silvanic "obviously retain[s] other means for communication, including communication in person and over the telephone." *Id.* at ¶ 20.

¶ 61 Fourth, as the district court noted, Silvanic has the option of asking the court to lift the restriction in the future. *See* § 18-1.3-204(4)(a), C.R.S. 2022.

¶ 62 Fifth, given that the monitoring requirement would cover both the conduct and the device that Silvanic used to groom the victim, less restrictive means would not reasonably ensure his compliance with the terms and conditions of his probation. Indeed, the court's decision to lift the outright ban on certain types of internet usage and instead permit monitoring *was* the less restrictive alternative. In any event, monitoring is a proactive measure designed to

encourage an offender's compliance. Under the circumstances here, requiring a court to make more particularized findings before imposing the monitoring requirement would likely force the probation officer into a reactive role rather than a preventive one — a posture that would in my view be inconsistent with SOISP's paramount goal of protecting public safety. *See Commonwealth v. Shipps*, 142 N.E.3d 597, 608 (Mass. App. Ct. 2020) ("[W]e find it difficult to imagine how the probation department could effectively monitor the defendant's adherence to the condition that he not possess child pornography on his cell phone, absent a condition permitting [an] unannounced, targeted search.").

¶ 63 Having applied the *Brockelman* factors to conclude that the monitoring requirement is reasonably related to Silvanic's rehabilitation and the purposes of probation, I would also reject his constitutional challenges. Monitoring requirements have been widely recognized as an acceptable imposition on a probationer's Fourth Amendment rights, and that is particularly true in the context of sex offenses. *See, e.g.*, *United States v. Mixell*, 806 F. App'x 180, 185 (4th Cir. 2020) (upholding monitoring requirement

in part because it did "not prevent [the probationer] from using a computer or electronic device to access the Internet or to communicate on it"); *United States v. Browder*, 866 F.3d 504, 511 (2d Cir. 2017) (upholding monitoring requirement for probationer convicted of possession of child pornography); *United States v. Kappes*, 782 F.3d 828, 856 (7th Cir. 2015) (upholding monitoring requirement, and noting that "the sentencing judge reasonably found that the monitoring program will 'ensure compliance' with the other conditions" of probation).[5] Under the circumstances here, which involved grooming behavior using internet-related communications technology, a lack of accountability on Silvanic's

---

[5] In *State v. Bouchard*, 2020 VT 10, ¶ 26, 228 A.3d 349, 360, the Vermont Supreme Court invalidated a monitoring condition because it "authorize[d] limitless monitoring of defendant's computer and internet use." That holding made sense in a case where "[t]here [wa]s no evidence that [Bouchard's] offense was related to computers or the internet, or that he is at a high risk of violating his conditions of probation through online activity." *Id.* at ¶ 24, 228 A.3d at 359. Here, however, Silvanic clearly did use a cell phone or similar internet-enabled device to facilitate the offense, and his offense-specific evaluation raised concerns about his ongoing internet usage. Other cases cited by the majority did not involve sex offenses at all. *See, e.g.*, *United States v. Shiraz*, 784 F. App'x 141, 143 (4th Cir. 2019) (striking broad internet monitoring condition of supervised release for defendant who pleaded guilty to possession with intent to distribute a controlled substance and possession of a firearm by a felon).

part, and indications in the presentence report that he had difficulties with impulse control, any impingement on Silvanic's Fourth Amendment rights is substantially outweighed by the government's interest in ensuring his compliance with the terms and conditions of his probation.

¶ 64 I would also reject Silvanic's contention that the monitoring requirement forces him to choose between exercising his First Amendment rights and preserving the rights guaranteed to him by the Fourth Amendment. As I have already noted, the incremental difference between the unchallenged account-sharing requirement and the monitoring agreement is not substantial. And, of course, the restriction imposed here is far less onerous than outright prohibitions of the type that other courts have routinely upheld. *See, e.g.*, *Landis*, ¶ 25.[6]

---

[6] For similar reasons, I would reject Silvanic's challenge to the monitoring requirement under article II, section 10 of the Colorado Constitution. The only authority that he cites addresses prohibitions on speech, and not burdens of the type that he asserts exist here. But because the monitoring requirement does not prohibit Silvanic from using the internet to communicate, I find those authorities unpersuasive under the circumstances here.

¶ 65 For these reasons, I would uphold the monitoring agreement and thus respectfully dissent from the majority's opinion.