

**UNITED STATES OF AMERICA,**  
**v.**  
**BRANDEN HOLENA, Appellant.**

No. 17-3537.

**United States Court of Appeals, Third Circuit.**

Argued July 10, 2018.

Filed: October 10, 2018.

On Appeal from the United States District Court for the Middle District of Pennsylvania, (D.C. No. 3:07-cr-00169-001), District Judge: Honorable Matthew W. Brann.

Heidi R. Freese, Esq., Federal Public Defender for the Middle District of Pennsylvania, Frederick W. Ulrich, Esq. [ARGUED], Assistant Federal Public Defender, Office of Federal Public Defender, 100 Chestnut Street, Suite 306, Harrisburg, PA 17101, *Counsel for Appellant*.

David J. Freed, Esq., United States Attorney for the Middle District of Pennsylvania, Carlo D. Marchioli, Esq. [ARGUED], Office of United States Attorney, 228 Walnut Street, P.O. Box 11754, 220 Federal Building and Courthouse, Harrisburg, PA 17108, Francis P. Sempa, Esq., Office of United States Attorney, 235 North Washington Avenue, P.O. Box 309, Suite 311, Scranton, PA 18503, *Counsel for Appellee*.

Before: GREENAWAY, JR., RESTREPO, and BIBAS, *Circuit Judges*.

## **OPINION OF THE COURT**

BIBAS, Circuit Judge.

To protect the public, a sentencing judge may restrict a convicted defendant's use of computers and the internet. But to respect the defendant's constitutional liberties, the judge must tailor those restrictions to the danger posed by the defendant. A complete ban on computer and internet use "will rarely be sufficiently tailored." *United States v. Albertson*, 645 F.3d 191, 197 (3d Cir. 2011). This case illustrates why.

Branden Holena was convicted of using the internet to try to entice a child into having sex. As a condition of his supervised release from prison, he may not possess or use computers or other electronic communication devices. Nor may he use the internet without his probation officer's approval. Restricting his internet access is necessary to protect the public. But these restrictions are not tailored to the danger he poses. So we will vacate and remand for resentencing.

## **I. BACKGROUND**

Holena repeatedly visited an online chatroom and tried to entice a fourteen-year-old boy to have sex. He made plans to meet the boy. He assured the boy that his age was not a problem, as long as the boy did not tell the police. But the "boy" was an FBI agent. So when Holena arrived at the arranged meeting spot in a park, he was arrested and charged with attempting to entice a minor to engage in sexual acts.

Holena pleaded guilty. He was sentenced to ten years' imprisonment and a lifetime of supervised release. As a special condition of that supervised release, he was forbidden to use the internet without his probation officer's approval. He had to submit to regular searches of his computer and home. And he had to let the probation office install monitoring and filtering software on his computer.

After serving his prison sentence, Holena violated the terms of his supervised release—twice. The first time, he went online to update social-media profiles and answer emails. The second time, he logged into Facebook without approval, then lied about it to his probation officer. After each violation, the court sentenced him to nine more months' imprisonment and reimposed the special conditions.

At Holena's latest revocation hearing, the judge imposed another condition, forbidding him to possess or use any computers, electronic communications devices, or electronic storage devices. Holena objected to this lifetime ban.

## II. JURISDICTION AND STANDARD OF REVIEW

The District Court had jurisdiction under 18 U.S.C. §§ 3231 and 3583(e). We have jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a).

We review revocation of supervised release for abuse of discretion. *United States v. Bagdy*, 764 F.3d 287, 290 (3d Cir. 2014). We insist on "some evidence" that the special conditions imposed are "tangibly related" to the goals of supervised release. *United States v. Voelker*, 489 F.3d 139, 144 (3d Cir. 2007); see 18 U.S.C. § 3583(d). To justify special conditions, district courts must find supporting facts. *United States v. Thielemann*, 575 F.3d 265, 272 (3d Cir. 2009). We may affirm if we can "ascertain any viable basis" in the record for the restriction. *Id.* (quoting *Voelker*, 489 F.3d at 144). Here, we cannot.

## III. THE SPECIAL CONDITIONS ARE NOT SUFFICIENTLY TAILORED

Holena argues that the bans on computer and internet use are both contradictory and more restrictive than necessary. We agree. And we note that the lack of tailoring raises First Amendment concerns.

### A. The conditions are contradictory

Holena's conditions of supervised release contradict one another, so we cannot be sure that they fit the goals of supervised release. We cannot tell what they forbid, nor can Holena. So we must vacate and remand.

One condition forbids Holena to "possess and/or use computers . . . or other electronic communications or data storage devices or media." App. 8 (¶ 11). But the very next condition provides that he "must not access the Internet except for reasons approved in advance by the probation officer." *Id.* (¶ 12). These requirements conflict. How can he use the internet at all if he may neither possess nor use a computer or electronic communication device?

Two other conditions likewise conflict with the ban. One requires him to have monitoring software installed "on any computer" he uses. *Id.* (¶ 7). The other requires him to submit to searches of his computers. These

conditions are difficult to reconcile given his computer ban.

Nothing in the record helps us or Holena to harmonize these contradictory conditions. Even the Government "hesitates to discern" what the District Court meant to forbid. Appellee's Br. 28. And the Government admits that the ban conflicts with several other conditions.

Even so, the Government urges us to read the probation-officer-approval provision as an exception to the ban. But we are not interpreting a statute. Due process requires district courts to give defendants fair warning by crafting conditions that are understandable. See United States v. Fontaine, 697 F.3d 221, 226 (3d Cir. 2012).

Holena cannot follow these conditions because he cannot tell what they forbid. So we will vacate and remand.

## **B. The conditions are more restrictive than necessary**

Section 3583(a) places "real restriction[s] on the district court's freedom to impose conditions on supervised release." United States v. Pruden, 398 F.3d 241, 248 (3d Cir. 2005). Special conditions may not deprive the defendant of more liberty "than is reasonably necessary" to deter crime, protect the public, and rehabilitate the defendant. 18 U.S.C. § 3583(d)(2); see *id.* § 3553(a). The same is true when district courts alter conditions of supervised release. *Id.* § 3583(e)(2).

The scope and intrusiveness of Holena's conditions, on this sparse record, violate this requirement. So, on remand, the District Court must tailor any restrictions it imposes to Holena's conduct and history. *Id.* § 3583(d)(2), (e)(2); see also Voelker, 489 F.3d at 146. Our remand is not "limited" to clarifying the special conditions. Appellee's Br. 29. The District Court should conduct another revocation hearing. At that hearing, it should make findings to support any restrictions it chooses to impose on Holena's internet and computer use. And it should ensure that Holena understands those restrictions.

A defendant's conduct should inform the tailoring of his conditions. For instance, a tax fraudster may be forbidden to open new lines of credit without approval. United States v. Bickart, 825 F.3d 832, 840 (7th Cir. 2016). A child molester may be forbidden to linger near places where children congregate. United States v. Zobel, 696 F.3d 558, 575 (6th Cir. 2012). And a child-pornography collector may be forbidden to possess pornography or visit pornographic websites. See United States v. Freeman, 316 F.3d 386, 392 (3d Cir. 2003). So internet bans and restrictions have a role in protecting the public from sexual predators.

Still, internet bans are "draconian," and we have said as much "even in cases where we have upheld them." United States v. Heckman, 592 F.3d 400, 408 (3d Cir. 2010). To gauge whether an internet or computer restriction is more restrictive than necessary, we consider three factors: the restriction's length, its coverage, and "the defendant's underlying conduct." *Id.* at 405 (emphasis removed). Sometimes we also consider a fourth factor: the proportion of the supervised-release restriction to the total restriction period (including prison). Albertson, 645 F.3d at 198. But we cannot rely on that proportion because the numerator is a lifetime ban. So we give the fourth factor no weight here.

Our analysis must be fact-specific. *Id.* We do not simply tally the factors, nor does one factor predominate. Here, both the length and coverage of the computer ban and internet restriction are excessive. And they are not tailored to Holena's conduct.

## 1. Length.

We are troubled that Holena's "restrictions will last as long as he does." Voelker, 489 F.3d at 146. Without a more detailed record, we cannot uphold such a "lifetime cybernetic banishment." *Id.* at 148.

We have never upheld a lifetime ban in a precedential opinion. And we have had trouble "imagin[ing] how [a defendant] could function in modern society given [a] lifetime ban" on computer use. *Id.* But we do not suggest that a lifetime ban could never be sufficiently tailored. And the Sentencing Guidelines recommend the statutory maximum term (which may be a lifetime term) of supervised release for sex crimes. U.S. Sentencing Guidelines Manual §5D1.2(b)(2) (U.S. Sentencing Comm'n 2016) (policy statement).

Still, we are "conscious" that "[t]he forces and directions of the Internet are so new, so protean, and so far reaching" that any restrictions imposed today "might be obsolete tomorrow." Packingham v. North Carolina, 137 S. Ct. 1730, 1736 (2017). So the lifetime duration of the blanket ban is presumptively excessive.

## 2. Scope.

The computer and internet bans both sweep too broadly. They are the "antithesis of [the] 'narrowly tailored' sanction[s]" we require. Voelker, 489 F.3d at 145.

The ban on using a computer "or other electronic communications . . . device[]" is particularly draconian. App. 8 (¶ 11). In Thielemann, we upheld a qualified ten-year ban, one of the longest and most restrictive bans we have upheld yet. 575 F.3d at 278. But that ban involved some tailoring; the defendant could still "own or use a personal computer as long as it is not connected to the internet." *Id.* (emphasis removed).

Not so here. Even under the Government's less restrictive reading, Holena can use no computer without his probation officer's approval, nor even a cellphone. These restrictions apply even to devices that are not connected to the internet. These limitations prevent him from doing everyday tasks, like preparing a résumé or calling a friend for a ride. None of these activities puts the public at risk. So the computer and communication-devices ban is too broad.

The internet ban fares little better. It prevents Holena from accessing anything on the internet—even websites that are unrelated to his crime. True, the District Court did some limited tailoring of this restriction (if one reads the contradictory conditions as adding up to less than a blanket ban). It imposed a monitoring requirement and let him use the internet with his probation officer's prior approval. Those tweaks move the internet ban closer to the "comprehensive, reasonably tailored scheme" that we require. United States v. Miller, 594 F.3d 172, 188 (3d Cir. 2010).

But the District Court gave the probation office no guidance on the sorts of internet use that it should approve. The goal of restricting Holena's internet use is to keep him from preying on children. The District Court must tailor its restriction to that end.

On this record, we see no justification for stopping Holena from accessing websites where he will probably never encounter a child, like Google Maps or Amazon. The same is true for websites where he cannot interact with others or view explicit materials, like Dictionary.com or this Court's website. The District Court need not list all the websites that Holena may visit. It would be enough to give the probation office some categories of websites or a guiding principle.

None of this is to say that the District Court may not impose sweeping restrictions. In appropriate cases, it may. We hold only that, on this record, the scope of the restrictions is too broad.

### **3. Conduct.**

Holena used the internet to solicit sex from a minor. And he repeatedly violated the terms of his supervised release. That conduct warrants special conditions to limit his internet use. But we examine whether the District Court has tailored the special conditions to protect the public from similar crimes that Holena might commit. That tailoring is inadequate here.

We recognize that the need to protect the public is strongest in cases like this, when the defendant used the internet to try to molest children. See *Thielemann*, 575 F.3d at 278; *United States v. Crandon*, 173 F.3d 122, 128 (3d Cir. 1999). Holena's conduct underscores that point. He solicited sex from a (supposedly) fourteen-year-old boy. He graphically described the sexual acts he wanted to perform. And he knew what he was doing was wrong, but did it anyway. So there is still a strong need to protect the public. That is particularly true because the internet provides almost limitless opportunities to interact with people anonymously and nearly untraceably.

Even so, Holena's bans are not tailored to his conduct. They apply broadly to many internet and computer uses that have nothing to do with preying on children.

On remand, the District Court must sculpt Holena's restrictions to his conduct. Any restrictions it imposes must aim to deter future crimes, protect the public, or rehabilitate Holena. And the District Court must find facts so that we can review whether the restrictions are informed by Holena's conduct and directed toward those goals.

It is almost certainly appropriate to prevent Holena from using social media, chat rooms, peer-to-peer file-sharing services, and any site where he could interact with a child. On the other hand, it may not be appropriate to restrict his access to websites where he is unlikely to encounter a child. And there are difficult cases in between, like restricting email access. We leave it to the District Court to make those close calls based on the record.

But, on this record, the court may not prevent Holena from doing everyday tasks that have migrated to the internet, like shopping, or searching for jobs or housing. The same is true for his use of websites conveying essential information, like news, maps, traffic, or weather. Nor does this record justify banning benign use of a computer without internet access. Absent specific factual findings, we cannot say that forbidding Holena to write a novel or listen to music on his computer makes the public any safer.

In crafting Holena's restrictions, the District Court should also consider the availability and efficacy of filtering and monitoring software. See *Voelker*, 489 F.3d at 150; *United States v. Johnson*, 446 F.3d 272, 282-83 (2d Cir. 2006) (upholding a complete internet ban because the defendant could disable monitoring software). Special conditions should involve "no greater deprivation of liberty than is reasonably necessary" for its ends. 18 U.S.C. § 3583(d)(2). So if software or another measure (like limiting Holena's computer or internet use to the confines of the probation office) can achieve the goals of supervised release, then that is preferable to an outright ban. In any event, the court must create enough of a record to ground its findings and enable our review.

On remand, the District Court should also consider whether Holena may be allowed a cellphone. It should consider whether he can safely be allowed a smartphone with monitoring software installed. Alternatively, it may wish to permit a non-internet-connected phone, perhaps with text messaging that is monitored or disabled. Along the same lines, many other devices are connected to the internet, ranging from gaming devices to fitness trackers to smart watches. We leave all such determinations to the District Court.

## C. The conditions raise First Amendment concerns

Section 3583's tailoring requirement reflects constitutional concerns. Conditions of supervised release may not restrict more liberty than reasonably necessary, including constitutional liberty. So district courts must "consider the First Amendment implications" of their conditions of supervised release. Voelker, 489 F.3d at 150. Conditions that restrict "fundamental rights must be `narrowly tailored and . . . directly related to deterring [the defendant] and protecting the public.'" United States v. Loy, 237 F.3d 251, 256 (3d Cir. 2001) (quoting Crandon, 173 F.3d at 128). And a condition is "not `narrowly tailored' if it restricts First Amendment freedoms without any resulting benefit to public safety." *Id.* at 266.

Here, both Holena's computer ban and internet ban limit an array of First Amendment activity. And none of that activity is related to his crime. Thus, many of the restrictions on his speech are not making the public safer.

The Supreme Court recently struck down a North Carolina law banning sex offenders from using social-media websites. Packingham, 137 S. Ct. at 1738. Because the parties did not mention Packingham in their opening briefs, ordinarily we would not reach the issue. See Kost v. Kozakiewicz, 1 F.3d 176, 182 (3d Cir. 1993). But we asked for supplemental briefing on Packingham's import here. And, because we are remanding, we think it appropriate to offer guidance on how Packingham informs the shaping of supervised-release conditions.

The District Court can limit Holena's First Amendment rights with appropriately tailored conditions of supervised release. Defendants on supervised release enjoy less freedom than those who have finished serving their sentences. See United States v. Knights, 534 U.S. 112, 119 (2001); United States v. Rock, 863 F.3d 827, 831 (D.C. Cir. 2017). But, as we have noted, these restrictions must be tailored to deterring crime, protecting the public, or rehabilitating the defendant. Under Packingham, blanket internet restrictions will rarely be tailored enough to pass constitutional muster.

Here, even under Packingham's narrower concurrence, the bans fail. They suffer from the same "fatal problem" as North Carolina's restriction on using social media. Packingham, 137 S. Ct. at 1741 (Alito, J., concurring). Their "wide sweep precludes access to a large number of websites that are most unlikely to facilitate the commission of a sex crime against a child." *Id.* So on remand, the District Court must also take care not to restrict Holena's First Amendment rights more than reasonably necessary or appropriate to protect the public.

## D. The sentence was procedurally reasonable

Finally, we note briefly that the sentence is procedurally reasonable because it is consistent with United States v. Booker and its progeny. 543 U.S. 220 (2005). The District Court correctly calculated the applicable Guidelines range. It allowed the parties to argue for whatever sentence they deemed appropriate. It considered all of the § 3553(a) factors. And it sufficiently explained its reasoning on the record. See Gall v.

*United States*, 552 U.S. 38, 49-51 (2007); see also *United States v. Douglas*, 885 F.3d 145, 150 (3d Cir. 2018).

\* \* \* \* \*

Holena poses a danger to children, so the District Court may, and should, limit his liberty accordingly. But his supervised release must still be tailored to the danger that he poses. Holena's current conditions fail that test. They contradict one another. They also sweep too broadly, preventing him from reading the news or shopping online. And they limit his First Amendment freedoms beyond what is reasonably necessary or appropriate. We do not see how they are reasonably tailored to further the goals of supervised release, especially protecting the public. So we will vacate his sentence and remand for a new revocation hearing.

Save trees - read court opinions online on Google Scholar.