RECEIVED
04-16-2019
CLERK OF COURT OF APPEALS
OF WISCONSIN

STATE OF WISCONSIN

COURT OF APPEALS

DISTRICT II

Case No. 2018AP2074-CR

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

JAMES L. JACKSON, JR.,

Defendant-Appellant.

ON APPEAL FROM A JUDGMENT OF CONVICTION AND A DECISION DENYING POSTCONVICTION RELIEF ENTERED IN CALUMET COUNTY CIRCUIT COURT, THE HONORABLE JEFFREY S. FROEHLICH, PRESIDING

RESPONSE BRIEF OF PLAINTIFF-RESPONDENT

JOSHUA L. KAUL
Attorney General of Wisconsin

SARAH L. BURGUNDY
Assistant Attorney General
State Bar #1071646

Attorneys for Plaintiff-Respondent

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 261-8118
(608) 266-9594 (Fax)
burgundysl@doj.state.wi.us

TABLE OF CONTENTS

Page

Page

TABLE OF AUTHORITIES

Cases

Page

Page

Statutes

Other Authorities

ISSUES PRESENTED

1. Did James L. Jackson, Jr., waive, by pleading no contest, his as-applied First Amendment challenge to provisions in Wis. Stat. § 301.45(2)(a)6m. requiring him, as a sex offender, to report his internet email addresses and user names to DOC?

The circuit court said yes.

This Court should affirm.

2. Alternatively, does subparagraph 6m., as applied to Jackson, pass First Amendment intermediate scrutiny?

The circuit court applied the guilty plea waiver rule and did not answer this question.

If this Court reaches the question, it should affirm.

3. Are the provisions of subparagraph 6m. requiring sex offenders to inform DOC of their internet identifiers facially overbroad in violation of registrants' First Amendment right to anonymous speech?

The circuit court said no.

This Court should affirm.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

The State agrees with Jackson that publication is warranted to clarify that Wis. Stat. § 301.45(2)(a)6m. is facially constitutional. The State does not believe that oral argument will be necessary, but welcomes it if this Court will find it helpful.

INTRODUCTION

Is it a violation of a person's First Amendment right to anonymous speech to require sex offenders to report their email addresses and other internet identifiers to Wisconsin's sex offender registry? Jackson thinks so, but he is wrong.

To start, Jackson attempts to advance an as-applied challenge, without identifying how the law is unconstitutional to him specifically. He has waived this claim by pleading no contest, and this Court should not exercise its discretion to disregard the waiver rule. Even if this Court reaches the claim, subparagraph 6m. satisfies intermediate scrutiny because it is narrowly tailored to serve the statute's purpose.

Further, subparagraph 6m. is not facially overbroad measured against the plainly legitimate sweep of the statute. This Court should affirm.

STATEMENT OF THE CASE

In 1990, when he was 37 years old, Jackson was convicted of second-degree sexual assault of a child after he groomed and sexually assaulted a 14-year-old girl. (R. 4:1–2; 23:10.) As a result of that felony conviction, Jackson is required to comply with sex registry requirements in Wis. Stat. § 301.45. (R. 4:1–2.)

In February 2016, Calumet County police learned from R.P., an acquaintance of Jackson and Jackson's housemate, C.D., that Jackson was using C.D.'s computer "at all hours of the night and is trying to talk to young girls in the area over the internet." (R. 4:2.) Police learned during their investigation that Jackson had created a Facebook profile with the name "Lendord Jackson" that was in active use. (R. 4:2.) Jackson acknowledged that he had failed to report to the sex offender registry the Facebook profile and the email address associated with that profile. (R. 4:3–4.)

Based on Jackson's failures to report that information, the State charged Jackson with one count of sex offender registry violation, repeater, contrary to Wis. Stat. § 301.45(2)(a)6m. (R. 4:1.) Jackson pleaded no contest and received a stayed four-year sentence with three years' probation, including conditional jail time. (R. 29:1–2.)

Jackson filed a postconviction motion claiming that the requirement that he report his internet user names and email addresses to the sex offender registry (1) violates the First Amendment as applied to him and (2) is facially overbroad. (R. 44.) In a written decision, the postconviction court concluded that Jackson waived his as-applied claim by his no-contest plea and rejected the facial claim on its merits. (R. 57.) Jackson appeals.

ARGUMENT

I. Jackson waived his as-applied challenge by pleading no contest.

Whether Jackson's no-contest plea relinquished his right to appeal the constitutionality of his statute of conviction on an as-applied basis is a question of law that this Court reviews de novo. *See State v. Kelty*, 2006 WI 101, ¶ 13, 294 Wis. 2d 62, 716 N.W.2d 886.

A. A guilty or no-contest plea waives (or forfeits) an as-applied constitutional challenge to the statute of conviction.

With a few exceptions not relevant here, a valid guilty or no contest plea waives all nonjurisdictional defenses to a conviction, including constitutional violations. *See State v. Riekkoff*, 112 Wis. 2d 119, 122–23, 332 N.W.2d 744 (1983). Courts refer to this as the guilty plea waiver rule, although it is more accurately described as a rule of forfeiture. *See Kelty*, 294 Wis. 2d 62, ¶ 18 & n.11.

In Wisconsin, whether a guilty plea forecloses review of a claim that the defendant was convicted of violating an unconstitutional statute depends on whether the challenge is facial or as-applied. The guilty plea waiver rule does not foreclose a facial constitutional challenge because that type of challenge involves an issue of subject matter jurisdiction. *See State v. Cole*, 2003 WI 112, ¶ 46, 264 Wis. 2d 520, 665 N.W.2d 328; *see also State v. Olson*, 127 Wis. 2d 412, 420, 380 N.W.2d 375 (Ct. App. 1985) ("A statute, unconstitutional on its face, is void from its beginning to the end . . . .") (quoting *State ex rel. Comm'rs of Pub. Lands v. Anderson*, 56 Wis. 2d 666, 672, 203 N.W.2d 84 (1973)).

An as-applied challenge, in contrast, raises a non-jurisdictional defect that may be waived. *See Cole*, 264 Wis. 2d 520, ¶ 46. For example, in *Cole*, Cole pleaded guilty to a violation of Wis. Stat. § 941.23, which prohibited his carrying a concealed weapon, and he raised an as-applied constitutional challenge in a postconviction motion. *Id.* The supreme court held that as a result of his plea, Cole "waived the opportunity to challenge the constitutionality of" section 941.23 as applied to him. *Id.*

So too, here. Jackson pleaded no contest to a count of violating the sex offender registry statute, and he raised no constitutional challenge to the statute of conviction until his postconviction proceedings. He therefore waived his as-applied challenge, and the Court may deny it on that basis.

B. *Class* has no effect on Wisconsin's guilty plea waiver rule.

Jackson contends that *Class v. United States*, 138 S. Ct. 798 (2018), calls into question Wisconsin's longstanding guilty plea waiver rule to provide that defendants who plead guilty or no contest retain the right to raise an as-applied constitutional challenge to the statute of conviction. (Jackson's Br. 13–14.) Jackson is wrong.

Class involved a federal criminal defendant who entered an unconditional guilty plea under the Federal Rule of Criminal Procedure 11 (Rule 11). He then challenged the statute of conviction, which bars individuals from carrying a firearm on Capitol grounds, as violating the Second Amendment and violating the due process fair-notice requirement. *Class*, 138 S. Ct. at 802. The question before the Supreme Court was "whether a guilty plea by itself bars a federal criminal defendant from challenging the constitutionality of the statute of conviction on direct appeal." *Id*. at 803.

The Court held that Class's guilty plea did not waive his constitutional claims on direct appeal because they "challenge the Government's power to criminalize Class' (admitted) conduct. They thereby call into question the Government's power to 'constitutionally prosecute'" him. *Class*, 138 S. Ct. at 805. Moreover, the Court held, nothing in Rule 11 prevented Class from raising the claims simply based on his guilty plea. *Id.* at 805–07.

Class does not impact Wisconsin's guilty plea waiver rule. By the Court's own words, the question presented was whether a *federal* criminal defendant's guilty plea pursuant to Rule 11 waived his constitutional challenges to the statute of conviction. *Class*, 138 S. Ct. at 803.

Further, it is not clear from the Court's decision whether it considered Class's claims to be facial, as applied, or a combination of the two. But the Court 's distinction between a constitutional challenge that questions the government's power to prosecute and one that does not echoes the jurisdictional distinction between facial and as-applied challenges. To wit, a facial challenge is one that "strip[s] the government of its ability to enter a conviction against any defendant." *United States v. Phillips*, 645 F.3d 859, 863 (7th Cir. 2011). In contrast, an as-applied challenge "does not dispute the court's power to hear cases under the statute;

rather it questions the court's limited ability to enter a conviction in the case before it." *Id.* (citing *Blackledge v. Perry*, 417 U.S. 21, 30 (1974)). Wisconsin courts, in developing the guilty plea waiver rule, have long recognized that distinction between facial challenges, which implicate the court's jurisdiction, and nonjurisdictional as-applied challenges.[1]

Accordingly, *Class* does not affect Wisconsin's guilty plea waiver rule, which is not based in Rule 11. Nor does the *Class* holding overturn the facial/as-applied distinction in the guilty plea waiver context.[2] Thus, *Class* does not require this Court to address Jackson's as-applied challenge.

C. This Court should otherwise decline to exercise its power to address Jackson's as-applied challenge.

Like the general rule of waiver, the guilty plea waiver rule is one of administration and does not involve a court's power to address the issues raised. *See Kelty*, 294 Wis. 2d 62, ¶ 18. Thus, this Court may decline to apply the rule "particularly if the issues are of state-wide importance or resolution will serve the interests of justice and there are no

---

[1] *See, e.g.*, *State v. Cole*, 2003 WI 112, ¶ 46, 264 Wis. 2d 520, 665 N.W.2d 328; *State v. Trochinski*, 2002 WI 56, ¶ 34 n.15, 253 Wis. 2d 38, 644 N.W.2d 891; *State v. Molitor*, 210 Wis. 2d 415, 419, 565 N.W.2d 248 (Ct. App. 1997); *see also State ex rel. Skinkis v. Treffert*, 90 Wis. 2d 528, 538, 280 N.W.2d 316 (Ct. App. 1979) (a successful facial constitutional challenge renders statute void and deprives court of power to convict any defendant for violating it).

[2] At least one state court has understood *Class*'s holding to be limited to allowing facial constitutional claims to proceed despite a guilty or no contest plea. *See, e.g.*, *In re N.G.*, 115 N.E.3d 102, 122–23 (Ill. 2018) (concluding that, based on *Class*, "[d]efendants convicted under a *facially* unconstitutional statute may challenge the conviction at any time, even after a guilty plea, because the State or Government had no power to impose the conviction to begin with" (emphasis added)).

factual issues that need to be resolved." *State v. Tarrant*, 2009 WI App 121, ¶ 6, 321 Wis. 2d 69, 772 N.W.2d 750 (quoted source omitted). Jackson asks this Court to disregard his forfeiture and address the merits of his as-applied challenge because, in his view, all three criteria are met. (Jackson's Br. 14–15.)

This Court should decline Jackson's invitation. Jackson fails to identify—based on the facts of his case or the court's application of the law to him, specifically—why subparagraph 6m. is constitutionally infirm. *See, e.g.*, *State v. Hamdan*, 2003 WI 113, ¶ 43, 264 Wis. 2d 433, 665 N.W.2d 785 (stating that courts assess as-applied challenges based on facts of defendant's case and application of law to specific circumstances).

Moreover, while the constitutionality of any statute is generally of state-wide importance, Jackson has fully advanced a reviewable facial overbreadth challenge that addresses similar concerns—i.e., the State's demands exceed its purpose—Jackson identifies in his as-applied argument. *Compare United States v. Stevens*, 559 U.S. 460, 472 (2010) (stating that a facial challenge for overbreadth must show "'a substantial number of [the statute's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep'") with *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (providing that an as-applied, intermediate-scrutiny challenge considers whether content-neutral restrictions on speech are "narrowly tailored to serve a significant governmental interest"). Accordingly, this Court's resolution of both the as-applied and facial challenge to determine whether the statute demands too much information of Jackson and other registrants does not promote efficient use of judicial resources and will not serve the interests of justice.

And as for unresolved factual issues, two points: first, as noted, Jackson fails to identify what facts, if any, about him

or his case, render subparagraph 6m. unconstitutional as applied to him. *See, e.g.*, *Hamdan*, 264 Wis. 2d 433, ¶ 43 (stating that courts consider facts of defendant's case, not hypotheticals, in assessing merits of as-applied challenge). He argues that subparagraph 6m. allows the State to monitor and publicly disseminate internet identifiers of sex offender registrants. Those features would apply to anyone required to register as a sex offender, not Jackson uniquely.

Second, Jackson otherwise relies heavily on unresolved factual issues, particularly that the government has the ability to monitor his online activity and that it can broadcast his internet identifiers publicly. But there is no factual record establishing whether or how the government can monitor registry individuals on the basis of email addresses and user names or identifying when or how the government could publicly disclose those identifiers. The absence of those facts deprives this Court of the ability to make an as-applied determination. *See, e.g.*, *Hamdan*, 264 Wis. 2d 433, ¶ 43; *accord People v. Minnis*, 67 N.E.3d 272, 282 (Ill. 2016) (declining to consider defendant's as-applied challenge to similar registry requirements in "a factual vacuum").

To be sure, even in the First Amendment context, a defendant seeking as-applied relief faces better prospects for success than he does with a facial challenge. *See State v. Culver*, 2018 WI App 55, ¶¶ 9–10, 384 Wis. 2d 222, 918 N.W.2d 103 (stating that a proponent of "a facial challenge for overbreadth must show 'a substantial number of [the statute's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep,'" a "steep" standard) (quoting *Stevens*, 559 U.S. at 473). But that Jackson may prefer the as-applied framework is not a reason to overcome the waiver rule, particularly where the claim is as-applied by label only.

This Court should decline to address Jackson's claim for as-applied relief.

II. If this Court reaches Jackson's as-applied challenge, subparagraph 6m. is a content-neutral regulation narrowly tailored to serve a significant government interest.

Wisconsin Stat. § 301.45 governs the state sex offender registry, which requires people who have committed a sex offense to provide certain information to the DOC, such as the offender's name and aliases and his home, school, and work addresses. Wis. Stat. § 301.45(2)(a). Subparagraph 6m. of paragraph (2)(a) provides that an offender must also provide DOC with his or her virtual names and addresses, including:

- "[t]he name or number of every electronic mail account the person uses,"
- "the Internet address of every website the person creates or maintains,"
- "every Internet user name the person uses," and
- "the name and Internet address of every public or private Internet profile the person creates, uses, or maintains."

Wis. Stat. § 301.45(2)(a)6m. That required information is further limited to "an account, website, Internet address, or Internet profile the person creates, uses, or maintains for his or her personal, family, or household use." *Id.*

In his as-applied challenge, Jackson argues that subparagraph 6m.'s requirements chill his First Amendment right to anonymous speech because, by providing his internet identifiers, he is under threat of the government monitoring his online communication and facilitating others in doing so by releasing that information to the public. (Jackson's Br. 5–12.)

The State agrees with Jackson's statement of the standard of review (de novo), the burden of proof (the State bears the burden to prove constitutionality beyond a reasonable doubt), and that, as a content-neutral provision,

intermediate scrutiny applies to subparagraph 6m. (Jackson's Br. 4.) But it disagrees with virtually all of his other points.

A. Under intermediate scrutiny, a content-neutral speech regulation need not be the least restrictive or intrusive means of advancing the government's interest.

The intermediate-scrutiny test allows the government to impose reasonable, content-neutral restrictions on speech that are "narrowly tailored to serve a significant governmental interest, and that . . . leave open ample alternative channels for communication of the information." *Ward*, 491 U.S. at 791.

"To satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests." *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. 622, 662 (1994). "Rather, the requirement of narrow tailoring is satisfied 'so long as the . . . regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.'" *Ward*, 491 U.S. at 799 (quoting *United States v. Albertini*, 472 U.S. 675, 639 (1985)). "Narrow tailoring in this context requires, in other words, that the means chosen do not 'burden substantially more speech than is necessary to further the government's legitimate needs.'" *Turner Broad. Sys.*, 512 U.S. at 662 (quoting *Ward*, 491 U.S. at 799).

B. The State has a well-recognized and significant interest in protecting the public from recidivist sex offenders.

The purpose of Wisconsin's sex offender registry statute is to effectuate an "intent to protect the public and assist law enforcement"; it is "related to community protection" and designed to "further the governmental interests of public safety and enhance strategies for crime detection and

prevention." *State v. Smith*, 2010 WI 16, ¶ 26, 323 Wis. 2d 377, 780 N.W.2d 90; *see also State ex rel. Kaminski v. Schwarz*, 2001 WI 94, ¶ 41, 245 Wis. 2d 310, 630 N.W.2d 164. This purpose is well-recognized as a legitimate, substantial public interest. *Smith*, 323 Wis. 2d 377, ¶ 26; *see City of Los Angeles v. Alameda Books, Inc.*, 535 U.S. 425, 435 (2002) (recognizing substantial governmental interest in "reducing crime"); *New York v. Ferber*, 458 U.S. 747, 757 (1982) ("The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance."); *see also Smith v. Doe*, 538 U.S. 84, 90 (2003) (noting that since 1996 every state in the nation had enacted sex offender registry statutes).

Jackson does not dispute the legitimacy of the State's substantial interest; he instead claims that the disclosure provision in subparagraph 6m. is not narrowly tailored to advance that interest because it violates his right to anonymous speech. (Jackson's Br. 5–12.) As discussed below, he is wrong.

C. Subparagraph 6m. is constitutional as applied.

1. Subparagraph 6m. is narrowly tailored to advance the State's compelling interest and leaves ample alternative channels.

First Amendment rights include a right to anonymous speech. *See McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 343–44 (1995). Of course, the right to speak anonymously is not unlimited. *See Lefkoe v. Jos. A. Bank Clothiers, Inc.*, 577 F.3d 240, 248 (4th Cir. 2009); *see also* Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 Notre Dame L. Rev. 1537, 1599–1600 (2007) (positing that the "right" to anonymous speech is better termed a "qualified privilege"). The government may impose

regulations on anonymous speech that are subject to varying levels of judicial scrutiny, depending on the nature of the regulation. *See, e.g.*, *Turner Broad. Sys.*, 512 U.S. at 640–41; *Ward*, 491 U.S. at 791–92.

There is no dispute that the provision at issue in Wis. Stat. § 301.45(2)(a)6m. is content-neutral—i.e., that its requirement that sex offender registrants provide internet identifiers[3] such as "the name and number of every electronic email account the person uses, the Internet address of every website the person creates or maintains, every Internet user name the person uses, and the name and Internet address of every public or private Internet profile the person creates, uses, or maintains"—is unrelated to the content of speech. *See Turner Broad. Sys.*, 512 U.S. at 642.

Accordingly, as a content-neutral regulation, the internet-disclosure requirement in subparagraph 6m. is subject to intermediate scrutiny, which asks if the regulation is "narrowly tailored to serve a significant governmental interest, [and leaves] open ample alternative channels for communication of that information." *Ward*, 491 U.S. at 791. Again, "narrowly tailored" does not mean the least restrictive means of advancing the State's interest; rather, the requirement is satisfied as long as the law promotes a substantial governmental interest that would be achieved less effectively absent the law. *See Ward*, 691 U.S. at 800.

Here, the internet disclosure requirement directly and effectively serves Wisconsin's substantial interest in protecting the public from recidivist sex offenders. To start, "[t]he State's interest in protecting children from recidivist sex offenders plainly applies to internet use." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1739–40 (2017) (Alito, J.,

---

[3] The State uses the term "internet identifiers" in this brief as shorthand for the collective online information (email addresses, user names, and web site addresses) registrants must provide.

concurring). "[C]hildren often use the internet in a way that gives offenders easy access to their personal information." *Id.* Moreover, "the internet provides previously unavailable ways" for offenders to communicate with, stalk, and ultimately abuse children, particularly given the ease with which internet users can create false identities, share images, and track childrens' patterns and activities. *Id.* "Such uses of the internet are already well documented, both in research and in reported decisions." *Id.* (footnotes omitted).

Requiring registered sex offenders to provide DOC with their active email addresses, user names, and online identities promotes the State's interest by providing law enforcement with a tool to quickly identify and apprehend recidivist sex offenders. For example, if police receive a complaint that a child has been receiving inappropriate communications from a particular email address or internet account, law enforcement can request information from DOC regarding the emails or user names it has in its registry records. Or if police receive credible reports that a particular sex offender is using the internet to solicit children or engage in other illegal activity, law enforcement has internet identifiers available to assist it in promptly conducting a public search or obtaining a search warrant. In all, absent the disclosure provision in subparagraph 6m., the State's substantial interest in protecting the public from recidivist sex offenders "would be served less effectively." *Ward*, 491 U.S. at 801.

Further, the provision leaves "open ample alternative channels" for registrants to engage in anonymous speech. *See Ward*, 491 U.S. at 791. Jackson's premise appears to be that the only way he can express anonymous speech is through the internet. *See* Jackson's Br. at 6 ("Subdivision 6m. . . . prevents [Jackson] from communicating anonymously.") To start, that premise is faulty, given that no one—sex offender registrant

or not—enjoys true anonymity on the internet.[4] And nothing in the sex offender registry prevents him from engaging in anonymous speech off the Internet, i.e., erecting signage, distributing leaflets, or posting printed notices anonymously. Moreover, nothing in the sex offender registry prevents him from accessing and using online forums, unlike the struck-down provisions in *Packingham*, 137 S. Ct. at 1739–40.

And even assuming that one can enjoy some anonymity on the internet, subsection 6m. does not limit Jackson's internet use or access. Like anyone else—sex offender or not—Jackson can access any internet platform he chooses. Like anyone else, he may post and add content using any user name he chooses. And it bears repeating that no one using email, news, or social media websites enjoys complete privacy or pure anonymity. Registering a user name with a particular site typically requires an active email address or phone number at the very least. Other accounts, such as for Amazon, are tied to physical addresses, phone numbers, and credit cards. And when a person reveals a user name by posting online or email address by sending an email, anyone—other users, the platform, commercial entities that track and gather online data—seeing that information can ostensibly track or monitor that usage, the user's IP address, and other identifying information. All that subparagraph 6m. does is provide DOC with a more direct tie between a registrant's actual and online identities, which, as noted, better serves the protective and law-enforcement purposes of the registry.

---

[4] *See, e.g.,* Griffin, Eric, *How to Stay Anonymous Online*, PCmag.com (Jan. 26, 2018, 4:05 PM EST), https://www.pcmag.com/article/250523/how-to-stay-anonymous-online ("Ultimately, the only way to stay truly anonymous online is to not go online at all.").

In the face of similar First-Amendment-based challenges, multiple courts have held that similar disclosure provisions in other states' sex-offender registry laws satisfy intermediate scrutiny.[5] For example, the Illinois Supreme Court upheld, under intermediate scrutiny, the internet identifiers disclosure provision of its statute. *Minnis*, 67 N.E.3d at 289–90. That provision required registrants to report both their email addresses and online identities; moreover, that information was included in the state's public web site. *Id.* at 284–85. The court determined that the provision was narrowly tailored in relation to the substantial government interest advanced by the statute. *Id.* at 289–90. Comparing Wisconsin's statute to Illinois' more-sweeping provisions, *Minnis*'s reasoning persuades that Wisconsin's scheme is sufficiently narrowly tailored in relation to the State's compelling interest, that the State's compelling interest is better served with it than without out it, and that it leaves open ample opportunities for expression.

2. Jackson's arguments are not persuasive.

That the law applies to all sex offenders, not just those who have committed internet-based crimes (*see* Jackson's Br. 11), is irrelevant. As noted above, courts have recognized that (1) sex offenders pose a high risk of recidivism and (2) the internet provides offenders easy access to children. *See Packingham*, 137 S. Ct. at 1739–40 (Alito, J., concurring); *see*

---

[5] *See, e.g.*, *Doe v. Shurtleff*, 628 F.3d 1217, 1224–25 (10th Cir. 2010) (upholding Utah's statute requiring disclosure of internet identifiers); *Does #1–7 v. Abbott*, 345 F. Supp. 3d 763, 780–81 (N.D. Tex. 2018); *Harris v. State*, 985 N.E.2d 767, 776 (Ind. Ct. App. 2013); *People v. Minnis*, 67 N.E.3d 272, 289–90 (Ill. 2016); *Ex Parte Odom*, No. 01-18-00169-CR, 2018 WL 6694790, at *8 (Tex. App. Dec. 20, 2018).

also Smith v. Doe, 538 U.S. at 103 (stating that a legislature could conclude that "a conviction for a sex offense provides evidence of substantial risk of recidivism" because the "risk of recidivism posed by sex offenders is 'frightening and high'" (quoting *McKune v. Lile*, 536 U.S. 24, 34 (2002))).

Jackson also complains that the scope of information he must disclose is not narrowly tailored because it captures "considerable conduct" unrelated to the State's interest. (Jackson's Br. 11.) He claims that requiring him to provide information like his email address or Facebook user name is especially problematic because he has completed his sentence and is not subject to limited constitutional rights like a probationer. (Jackson's Br. 12.)

That Jackson has completed his sentence does not change the fact that he has committed a sex offense, and because of that, he poses a high risk of recidivism. He invokes no cases holding that requiring internet identifiers of offenders who are no longer serving a sentence violates the First Amendment. As for the scope of information Jackson must provide, he offers no explanation why his having to disclose his email address and Facebook user name—both of which would be tools a person could use to contact children over the internet—captures conduct unrelated to the statute's purpose. His citations to cases invalidating statutes that expressly prevent sex offenders from *using* certain internet sites[6] are clearly off-point: nothing about providing his internet identifiers prevents Jackson from using and participating on online forums. And, as discussed in more detail below, that the State could possibly pierce a person's anonymity does not amount to a chilling effect on First Amendment expression.

---

[6] *See* Jackson's Br. 11 (citing *Doe v. Prosecutor, Marion Cty., Indiana*, 705 F.3d 694, 697 (7th Cir. 2013) and *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017)).

D. Speculation that the government might monitor registrants does not chill speech.

Jackson complains that the disclosure requirement "prevents him from communicating anonymously" because, by giving the government his internet identifiers, he cannot engage in "protected activities" online "without the threat of law enforcement surveilling his communications." (Jackson's Br. 6–7.) For support, he invokes *Millard v. Rankin*, 265 F. Supp. 3d 1211, 1229 (D. Colo. 2017). (Jackson's Br. 7–8.)

To start, the language Jackson quotes in *Millard* is dicta to that case and unpersuasive. *Millard* is not a First Amendment case. Rather, the *Millard* court considered the punitive nature of Colorado's reporting scheme under the Eighth Amendment. In considering whether the statute was punitive in nature, the court criticized that statute's provision requiring disclosure of internet identifiers. *Millard*, 265 F. Supp. 3d at 1228. It then remarked, without support, that "[b]y requiring certain offenders to register email addresses and other internet identities, [Colorado's sex offender registry law] provides law enforcement a supervisory tool to keep an eye out for registered sex offenders using email and social media." *Id.*

The *Millard* court's broad remark that providing the government with user names and email addresses allows it to monitor sex offenders' online activity—and Jackson's adoption of that reasoning—is speculative. Unless DOC uses special software, it is not clear how it could monitor a person's internet usage based on email addresses or user names. The statute does not require registrants to disclose passwords or any other information that would give DOC access to a registrant's online accounts. Even if it were legal and feasible for DOC to routinely surveil the online activity of any of the

over 25,000 people[7] on the sex offender registry without reasonable suspicion or probable cause, there is nothing to suggest that the State operates spyware or maintains staffing to allow it to monitor a person's online communications based solely on emails and user names.

Further, the online sites that Jackson seems most concerned with, like Facebook (Jackson's Br. 6, 8, 11–12), offer privacy settings that a user can activate to block or limit others from seeing his or her page and posts. Nothing in subparagraph 6m. requires registrants to grant DOC access to their social media pages or forbids them from activating internet privacy settings. Moreover, nothing in the registry prevents sex offenders from setting up firewalls or using commercial software designed to protect private information from surveillance.

In any event, the threat that the government might pierce a person's anonymity does not chill speech, which the Tenth Circuit's reasoning in *Shurtleff* makes clear. There, the defendants argued that providing his online identifiers allowed the state (Utah) to monitor his communications at any time and threatened to unnecessarily chill his speech. *Shurtleff*, 628 F.3d at 1225. The court first noted that Utah's statute appeared to limit the State's ability "to look beyond the anonymity surrounding a username" to investigations of new crimes. *Id.*

But the court also explained that the State does not impermissibly infringe upon anonymous speech simply because it might pierce anonymity after a person engages in such speech: "Speech is chilled when an individual whose

---

[7] *See* Wisconsin Dep't of Corrections, *Division of Community Corrections: 2018 A Year in Review,* 6 (Dec. 2018), https://doc.wi.gov/DataResearch/DataAndReports/DCCYearInReview.pdf (providing that Wisconsin's sex offender registry had 25,126 registrants as of June 30, 2018).

speech relies on anonymity is forced to reveal his identity as a pre-condition to expression. In other words, the First Amendment protects anonymity where it serves as a catalyst for speech." *Id.* (citation omitted). Thus, even if "a government agent would have access to [a person's] identity at the time he was speaking," that possibility does not necessarily impose a constitutionally improper burden on speech. *Id.* The court found support for that reasoning in language from the United States Supreme Court:

> [T]his Court has found in a number of cases that constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights. In none of these cases, however, did the chilling effect arise merely from the individual's knowledge that a governmental agency was engaged in certain [information-gathering] activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some other or additional action detrimental to that individual.

Id. (quoting *Laird v. Tatum*, 408 U.S. 1, 11 (1972) (brackets in *Shurtleff*)); *see also Odom*, 2018 WL 6694790 at *8 (adopting reasoning from *Shurtleff*).

Accordingly, the possibility that the State might pierce Jackson's anonymity—based on the fact that he reported his online identifiers to it—does not impermissibly chill anonymous speech.

E. Wisconsin law does not authorize widespread public release of a sex offender's internet identifiers.

1. Wisconsin Stat. §§ 301.45 and 46 limit the state's ability to use and share a registrant's internet identifiers.

Jackson invokes cases in which courts enjoined similar statutes based, in part, on provisions in those statutes allowing law enforcement, in its discretion, to release a registrant's internet identifiers to the public. (Jackson's Br. 8–10 (discussing *White v. Baker*, 696 F. Supp. 2d 1289, 1311 (N.D. Ga. 2010), and *Doe v. Harris*, 772 F.3d 563 (9th Cir. 2014))). He cherry-picks two sentences from Wis. Stat. § 301.46—which provides rules regarding access to information regarding sex offenders—and asserts that Wisconsin officials have overly broad discretion to release an offender's internet information to the public and that that discretion serves to chill registrants' anonymous speech. (Jackson's Br. 8–10.)

To be sure, courts assessing First-Amendment anonymous-speech challenges to internet disclosure provisions in sex offender registries consider the degree to which a given statute permits state officials to make publicly available a registrant's internet identifiers. In cases where the statute does not authorize state officials to publicly release that information, the statute does not burden the right to anonymous speech.

For example, in *Shurtleff*, Utah's registry statute provided that the government was to use internet identifiers for criminal investigations and that those identifiers were considered private information not to be publicly disclosed. 628 F.3d at 1221. "Nowhere in the Utah code," the court wrote, did the legislature use the word "share . . . to indicate

the unrestricted disclosure of information to the general public." *Id.* at 1224. The court held that the limited risk of disclosure of the plaintiff's internet identifiers to other state officials did not chill his rights to anonymous speech. *Id.* at 1224–25.

Similarly, in *Coppolino v. Noonan*, 102 A.3d 1254, 1283–84 (Pa. Commw. Ct. 2014), a Pennsylvania court concluded that its sex offender registry law did not authorize widespread public disclosure of internet identifiers. As a result, the court held, "the requirement that registrants disclose their Internet identifiers does not burden the right to anonymous speech." *Id.* at 1284.

And even where a statute authorized unfettered public dissemination of internet identifiers, it was sufficiently narrowly tailored. In *Minnis*, the Illinois Supreme Court upheld a statute that expressly permitted law enforcement to disclose internet identifiers to agencies and individuals "on the Internet or in other media." 67 N.E.3d at 285. Despite the broadness of those disclosure and notification provisions, they were sufficiently narrowly tailored to the statutory purpose because

> [t]he disclosure provision identifies the locations on the Internet to which the sex offender has transferred expressive material . . . or has otherwise engaged in communication. These disclosures empower the public, if it wishes, to make the informed decision to avoid such interactions. The information required for the public to protect itself is broad because any communication by a sex offender with the public is related to the statutory purpose.

Id. at 290.

Unlike Illinois's statute, Wisconsin's statute does not authorize widespread online public disclosure of a sex offender's internet identifiers. And contrary to Jackson's suggestions (Jackson's Br. 8, 12), Wisconsin's registry statute does not authorize state officials to broadcast a registrant's

internet identifiers to the general public without a particularized justification.

To start, as Jackson acknowledges, DOC is not authorized to include internet identifiers on its publicly accessible registry web site. *See* Wis. Stat. § 301.45(2)(a)6m. (providing that "[t]he department may not place the information provided under this subdivision on any registry that the public may view but shall maintain the information in its records on the person"). Indeed, the default status of a registrant's internet identifiers is confidential "except as needed for law enforcement purposes" and "except as provided" in section 301.46. *See* Wis. Stat. § 301.45(7).

In section 301.46, law enforcement appears to have limited, by-request-only access to the internet identifiers. Wisconsin Stat. § 301.46(2) requires the DOC to provide "access" to law enforcement of information regarding sex offender registrants; none of the enumerated information includes the subparagraph 6m. internet identifiers. Wis. Stat. § 301.46(2)(b)1.–10. That said, "in addition to having access to information under pars. (a) and (c), a police chief or sheriff may request that the department provide information concerning a registered sex offender." Wis. Stat. § 301.46(2)(d). And, a police chief may provide "any of the information to which he or she has access under this subsection . . . to members of the general public if, in the opinion of the police chief or sheriff, providing that information is necessary to protect the public." Wis. Stat. § 301.46(2)(e).

As a corollary to subsections (2)(d) and (e), members of the public may request information regarding a sex offender. Wis. Stat. § 301.46(5)(a). If the DOC, police chief, or sheriff acquiesce to the request, they may provide limited information regarding the person and "[a]ny other information concerning the person that the department or the

police chief or sheriff determines is appropriate." Wis. Stat. § 301.46(5)(b)4.

That determination of appropriate disclosure is circumscribed: "a person acting under" section 301.46 is under a good-faith duty "regarding the release of information authorized under this section." Wis. Stat. § 301.46(7). A person "whose act or omission [with regard to the release of registry information] constitutes gross negligence or involves reckless, wanton or intentional misconduct" can be subject to civil liability. *Id.*

Thus, in situations where law enforcement requests a registrant's internet identifiers, or where a member of the public requests such information, DOC or law enforcement would have discretion—tempered by a good faith duty—to provide and disclose that information if doing so is necessary and appropriate to protect the public.

In sum, that provision is narrowly tailored to the statute's purpose: it provides a limited exception to the general rule of confidentiality to members of the public when there is a particularized need for public protection. Nothing in section 301.46 suggests that law enforcement may engage in widespread, unjustified public dissemination of a registrant's internet identifiers.

Given that, absent the provisions in sections 301.45(2)(a)6m. and 301.46 allowing limited disclosure of internet identifiers to members of the public when required for public safety, the state's statutory interest in assisting law enforcement and protecting the public with regard to recidivist sex offenders would be less well served. *See Ward*, 491 U.S. at 800. Subparagraph 6m. passes intermediate scrutiny.

2. *White* and *Doe v. Harris* do not persuade otherwise.

In *White*, a federal district court determined that a Georgia statute that granted general discretion to law enforcement to release an offender's internet information for "law enforcement purposes" or to "protect the public" could have a chilling effect on anonymous speech. 696 F. Supp. 2d at 1310–11. That case is distinguishable for two reasons. First, Georgia's registry requirements posed an actual risk of law enforcement or the public monitoring registrants because registrants were required to provide passwords in addition to user names and emails. *Id.* at 1308. Second, the notification provision at issue appeared to allow broader dissemination of internet identifiers (and possibly passwords) to the public than what Wisconsin's law allows, as discussed above. *See id.* at 1310–11.

In *Doe v. Harris*, the Ninth Circuit concluded that California's internet identifier requirement unnecessarily chilled speech for three reasons: (1) it "does not make clear what [information] sex offenders are required to report"; (2) it has insufficient safeguards to prevent public release of the information reported; and (3) its 24-hour reporting requirement was onerous and overbroad. 772 F.3d at 578. The first and third reasons are not present here, so it is not clear how those factors impacted that court's view of the second reason.

Moreover, California appeared to allow broader public dissemination of a sex offender's internet identifiers, by allowing law enforcement to "provide information to the public . . . *by whatever means the entity deems appropriate*, when necessary to ensure the public safety." *Doe v. Harris*, 772 F.3d at 580. In contrast, as discussed, Wisconsin law does not endorse widespread public dissemination. What's more, the Ninth Circuit analysis is flawed because it did not balance the state's substantial interest in preventing repeat sex

offenses against the risk of public disclosure, as required by intermediate scrutiny. *Id.* at 581. Rather, it simply focused on general statements regarding the importance of anonymous speech without assessing whether the chilling effect was substantially broader than what the statute's purpose demanded. *Id.*

Finally, here, authorities did not disclose Jackson's email or internet user information publicly nor did they apprehend him after monitoring his online activity without reasonable suspicion. Jackson came to law enforcement's attention after it received a complaint that he was attempting to communicate with children online. (R. 4:1–2.) Law enforcement contacted DOC to learn what Jackson's reported email addresses were. (R. 4:2.) It conducted "open searches" on Facebook and located a profile with an alias affiliated with Jackson's phone number; police later learned that Jackson had created the profile, he actively used it, and that it was associated with an email address that Jackson had not reported. (R. 4:2.)

In other words, nothing happened here to suggest that law enforcement unconstitutionally applied the provisions of Wis. Stat. § 301.45 to Jackson, let alone that it was routinely monitoring him or publicly disclosing his internet identifiers. He is not entitled to relief on his as-applied claim.

III. Wisconsin Stat. § 301.45(2)(b)6m. is not overly broad.

A facial challenge permits a person to challenge a statute as "unconstitutional even when his or her own First Amendment rights are not affected." *Culver*, 384 Wis. 2d 222, ¶ 9 (citation omitted). Normally, a facial challenge requires proof "'that no set of circumstances exists under which [the statute] would be valid.'" *Id.* (quoting *Stevens*, 599 U.S. at 472). But "a less stringent standard" applies when First Amendment rights are implicated. *Id.*

Under those circumstances, "a facial challenge for overbreadth [under the First Amendment] must show 'a substantial number of [the statute's] applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep.'" *Id.* (quoting *Stevens*, 559 U.S. at 472). "The challenger bears this burden." *Id.* (citing *Virginia v. Hicks*, 539 U.S. 113, 122 (2003)); *see also New York State Club Ass'n, Inc.*, *v. City of New York*, 487 U.S. 1, 14 (1988) ("To succeed in its challenge, appellant must demonstrate from the text of Local Law 63 and from actual fact that a substantial number of instances exist in which the Law cannot be applied constitutionally.").[8]

Although the substantiality standard is a lesser one than the "under no circumstances" standard demands, "the substantiality standard is nonetheless steep." *Culver*, 384 Wis. 2d 222, ¶ 10. Moreover, invalidating a statute in its entirety is "strong medicine" and is to be "'employed by the Court sparingly and only as a last resort.'" *State v. Janssen*, 219 Wis. 2d 362, 373, 580 N.W.2d 260 (1998) (quoting *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973)). Statutes challenged as overbroad may be sustained "if a limiting and validating construction of the state's language is readily available." *Id.* at 378 (citing *Broadrick*, 413 U.S. at 613).

Jackson claims that two aspects of subparagraph 6m. are overbroad: (1) the provision requiring a registrant to

---

[8] Jackson is correct that generally, when First Amendment rights are implicated, the government bears the burden to prove that a statute is constitutional beyond a reasonable doubt. *See* Jackson's Br. 4, 17. But based on *Culver*, *Hicks*, and *New York State Club Ass'n*, cited above, the appellant appears to bear the burden of establishing that a statute cannot be applied constitutionally in a "substantial number of instances."

That said, even if the entire burden to prove First Amendment constitutionality rests on the State, it has satisfied its burden here.

notify the DOC of "the Internet address of every Web site the person creates or maintains," and (2) the provision requiring the registrant to supply "every Internet user name the person uses, and the name and Internet user address of every public or private Internet profile the person creates, uses, or maintains." (Jackson's Br. 17–19.)

The State will address each in turn, but it first notes that the provisions overlap, to the extent Jackson seeks to maintain a web site anonymously. Specifically, if Jackson seeks to maintain an anonymous blog, even without the first provision he would still need to provide the web address and the user name of his anonymous profile under the second provision.

Regardless, Jackson's obligation to reveal the web address and user name of web sites he creates or maintains does not result in a "substantial" number of unconstitutional applications. To start, this provision has a plainly legitimate sweep: while blogs and other web sites offer an opportunity for their creators to expound on topics, they also offer a means of communication with readers. To that end, Jackson does not identify a substantial number of applications where a sex offender registrant may wish to maintain a web site under a pseudonym that would be unrelated to the statute's legitimate sweep. And as for Jackson's concern that the DOC or law enforcement can inform the public about any reported anonymous sites, those agents may only do so if the need for public safety warranted it.

Contrary to Jackson's argument, *Doe v. Nebraska*, 898 F. Supp. 2d 1086 (D. Neb. 2012), does not persuade otherwise. (Jackson's Br. 18.) There, a federal district court held overbroad provisions of Nebraska's registry law requiring registrants to provide Internet identifiers and addresses *and* "to constantly update the government" every time they added something to a blog or added content to a commercial web sites they may maintain. *Doe v. Nebraska*, 898 F. Supp. 2d at

1121–22. In the district court's view, the demand that registrants update the State every time they added something to an already-registered web site tipped the balance into overbreadth:

> To be clear, requiring Internet identifiers and addresses, including designations for purposes of routing or self-identification, as permitted by the federal Attorney General's Guidelines, is one thing. Requiring sex offenders to constantly update the government about when and where they post content to internet sites and blogs is an entirely different thing.

Id. at 1122 The court opined that Nebraska, by creating the overly onerous "blog-uploading" requirement, was attempting through indirect means to prevent sex offenders from accessing the internet entirely, something it could not do directly. *Id.*

Unlike Nebraska's scheme, Wis. Stat. § 301.45 simply requires registrants to provide the name of web sites they maintain. There is no requirement that registrants alert DOC every time they add or upload content to those sites. *See Doe v. Nebraska*, 898 F. Supp. 2d at 1121–22. There is no requirement that registrants provide passwords or an especially high risk of public disclosure of that information, like in Georgia's law. *See White*, 696 F. Supp. at 1311. Nor does Wisconsin's law have particularly onerous or overbroad timing requirements. *See Doe v. Harris*, 772 F.3d at 582 (holding that a requirement that registrants report changes to internet identifiers within 24 hours was onerous and overbroad).

Nor does the provision in subparagraph 6m. requiring registrants to disclose "every Internet user name" and "every public or private Internet profile" they use satisfy the "substantiality" standard. Jackson attempts to frame this provision as being a de facto bar on registrants' using the

internet. (Jackson's Br. 19–20.) He also attempts to draw a line between social media forums designed for broad communication and those that offer more limited communication features, like Amazon or Washington Post stories. (Jackson's Br. 20.)

Oddly enough, those examples also appear in Justice Alito's concurrence in *Packingham*, 137 S. Ct. at 1741–42. There, Justice Alito used those examples to explain why North Carolina's statute barring sex offenders' *use* of those sites was overbroad. Indisputably, a statute making a "set of websites categorically off limits from registered sex offenders" is unconstitutional. *See Packingham*, 137 S. Ct. at 1737; *id.* at 1743 (Alito, J., concurring). But requiring a sex offender to provide his user names is neither a direct nor indirect bar on use, nor is it overly broad. Indeed, courts that have assessed provisions similar to Wisconsin's subparagraph 6m. have held that they are not overbroad in relation to the respective statute's plainly legitimate sweep.[9]

Moreover, a cursory review of any newspaper's comment section or Amazon's product reviews demonstrate that users do not necessarily limit their communication to product reviews or on-point commentary. That most users may not use those forums as a primary source of

---

[9] *See, e.g.*, *Coppolino v. Noonan*, 102 A.3d 1254, 1284 (Pa. Commw. Ct. 2014) (holding that requirement that registrants disclose their internet identifiers does not "burden the right to anonymous speech," in part because Pennsylvania law does not appear to permit public disclosure of that information); *Minnis*, 67 N.E.2d at 291 (holding that internet identifier requirement was not overbroad); *Odom*, 2018 WL 6694790, at *9 (rejecting overbreadth challenge to statute requiring all sex offenders to provide internet sites and user names they use for communication).

communication does not mean that the statute is overbroad. As the circuit court aptly put it, "Designating one type of Internet use or electronic communication as 'reporting required' and another type as 'not reporting required' is not feasible due to the ever-evolving capabilities of electronic communication, and its use by technologically savvy individuals." (R. 57:6.) Again, the internet and its myriad opportunities for communication create a significant area of concern when it comes to sex offenders. *See Packingham*, 137 S. Ct. at 1739–40 (Alito, J., concurring) (summarizing the many ways abusers can use internet to access children).[10] Asking registrants to provide user names on web sites where communication with others—including children—is feasible does not render the requirement overbroad.

At best, Jackson speculates that subparagraph 6m. could capture some conceivable protected conduct unrelated to its purpose. But that conduct is not real or substantial in relation to the statute's plainly legitimate sweep. *See Janssen*, 219 Wis. 2d at 373. Invalidation is not warranted "because in some conceivable, but limited, circumstances the regulation might be improperly applied." *Id.* The "strong medicine" of invalidation is not warranted here. *See id.*

---

[10] Jackson further laments that under the reporting requirement, he must tell the government if he "becomes a member of the ACLU, or joins the Republican Party." (Jackson's Br. 19.) The State fails to understand why that is necessarily so. If Jackson wishes to be a member of those organizations, he may do so without creating an online user name. He further fails to explain why providing his user name for things like his bank or iTunes is particularly invasive or onerous to his right to anonymous online speech.

CONCLUSION

This Court should affirm the judgment of conviction and order denying postconviction relief.

Dated this 16th day of April 2019.

Respectfully submitted,

JOSHUA L. KAUL
Attorney General of Wisconsin

SARAH L. BURGUNDY
Assistant Attorney General
State Bar #1071646

Attorneys for Plaintiff-Respondent

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 261-8118
(608) 266-9594 (Fax)
burgundysl@doj.state.wi.us

CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 8,295 words.

_____
SARAH L. BURGUNDY
Assistant Attorney General

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § 809.19(12)

I hereby certify that:

I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of Wis. Stat. § 809.19(12).

I further certify that:

This electronic brief is identical in content and format to the printed form of the brief filed as of this date.

A copy of this certificate has been served with the paper copies of this brief filed with the court and served on all opposing parties.

Dated this 16th day of April 2019.

_____
SARAH L. BURGUNDY
Assistant Attorney General