STATE OF NEW HAMPSHIRE

ROCKINGHAM, SS. SUPERIOR COURT

[redacted]

STATE OF NEW HAMPSHIRE

v.

[redacted]

DEFENDANT'S REPLY TO THE STATE'S OBJECTION TO MOTION TO DISMISS

NOW COMES Defendant, by and through his attorneys, and respectfully submits his Reply to the State's Objection to his Motion to Dismiss.

INTRODUCTION

The State's Objection confirms that RSA 651-B:4-a, on its face, violates the First Amendment and Part I, Article 22 to the New Hampshire Constitution. The State does not contest that, even under its tortured construction of RSA 651-B:4-a, this law requires all registrants—including those who are not a danger to the public and who have never been accused or convicted of not complying with their reporting obligations—to provide information about online activities that are innocent and have no relationship to criminality. The State does not contest that, under RSA 651-B:4-a, disclosure to the government of an online identifier is a necessary prerequisite to using that identifier to engage in innocent, protected speech. The State does not contest the fact that the legislature failed to consider less intrusive means to address its public safety concerns, including the possibility of narrowing the law so it only impacted registrants who were convicted of offenses involving the Internet, who are at high risk of reoffending, or who previously failed to comply with their reporting obligations. The State has also failed to produce any evidence either justifying the challenged law's intrusion on free speech rights or rebutting Defendant's evidence demonstrating RSA 651-B:4-a's lack of tailoring.

Instead, in a last-ditch effort to save RSA 651-B:4-a, the State has manufactured—nearly seven years after the law was enacted—two "narrowing constructions" of RSA 651-B:4-a and RSA 651-B:7. These constructions must be rejected because they improperly rewrite Chapter 651-B. It is the job of the legislature, not the Attorney General's Office or this Court, to rewrite an overbroad and ambiguous statute. Moreover, these constructions are inconsistent with (i) the New Hampshire Supreme Court's broad construction of RSA 651-B:4-a in *State v. White* ("*White*"), 164 N.H. 418 (2012), (ii) the Office of the Attorney General's prior construction in *White*, and (iii) the federal statute upon which the State now relies for guidance. And even if these constructions were tethered to Chapter 651-B's terms—which they are not—they would still be unconstitutional.

The State's own interpretation of RSA 651-B:4-a in this case before Defendant filed his Motion to Dismiss in August 2015 further undercuts the State's newfound narrowing constructions. In February 2015, the State indicted Defendant for allegedly not disclosing a www.brandyourself.com account. But this account may fall *outside* the very narrowing construction that the State has now proffered. *See* Indictments (First Biss. Dec., ¶ 33, *Ex. FF* at BON003). Perhaps in recognition that this indictment would undermine this manufactured construction, the State *nolle prossed* this charge on October 27, 2015—six (6) days before the State's Objection was due. Until Defendant filed his Motion to Dismiss in August, the State did not construe Chapter 651-B consistent with these constructions. For the past seven years until the State's Objection was filed on November 2, 2015, no one knew that these constructions existed. No law enforcement agency had adopted such constructions in their policies or procedures. The State has simply made up these constructions in response to Defendant's Motion.

RSA 651-B:4-a must be struck down, just like its counterparts in California, Nebraska, Georgia, and elsewhere. Most recently in July 2015, a court in Illinois struck down that state's

Internet Identifier statute, holding that it was "plainly overbroad and facially unconstitutional." *See Illinois v. Innis*, No. 14-CF-1076 (11th Cir., McLean Cty., Ill. July 7, 2015) (Second Biss. Dec., ¶ 2, *Ex. II*). RSA 651-B:4-a is no different. It ignores the reality that "the internet is our town square" in modern society. *See Doe v. State*, 167 N.H. 382, 406 (2015).

ARGUMENT

The State contends that Defendant "bears a heavy burden of proof in this matter." *See* State's Br. at 5. The State is wrong. As Defendant has brought a colorable facial challenge under the First Amendment and Part I, Article 22 of the New Hampshire Constitution, it is now the State's burden to demonstrate that RSA 651-B:4-a is constitutional. *See, e.g., United States v. Playboy Ent. Group, Inc.*, 529 U.S. 803, 816-17 (2000) ("When the Government restricts speech, *the Government* bears the burden of proving the constitutionality of its actions.") (collecting cases) (emphasis added); *see also McCullen v. Coakley*, 134 S. Ct. 2518, 2540 (2014) ("To meet the requirement of narrow tailoring, *the government must demonstrate* that alternative measures that burden substantially less speech would fail to achieve the government's interests, *not simply that the chosen route is easier*."; addressing content-neutral law) (emphasis added); *Doe v. Harris*, 772 F.3d 563, 570 (9th Cir. 2014) (in addressing content-neutral law, noting that "the government bears the burden of justifying its speech-restrictive law"); *Cutting v. City of Portland*, 802 F.3d 79 (1st Cir. 2015) ("*But the City* did not try—or adequately explain why it did not try—other, less speech restrictive means of addressing the safety concerns it identified."; addressing content-neutral law) (emphasis added); *Rideout v. Gardner*, No. 14-cv-489-PB, 2015 U.S. Dist. LEXIS 105194, at *29 (D.N.H. Aug. 11, 2015) (same). The State has produced no evidence to meet its burden, while Defendant has demonstrated the law's overbreadth through actual evidence.[1]

[1] The State's reliance upon *State v. Pierce*, 152 N.H. 790 (2005)—where the Court noted that "[t]he party challenging a statute's constitutionality bears the burden of proof"—is misplaced because Defendant here is making a free speech

I. The State's Sole Reliance On Narrowing Constructions Demonstrates That RSA 651-B:4-a, As Written, Raises Serious Constitutional Doubts.

The State's exclusive reliance on narrowing constructions in an attempt to save RSA 651-B:4-a is a tacit acknowledgment that the law "raise[s] serious constitutional doubts." *See Harris*, 772 F.3d at 578 ("Although we will adopt a narrowing construction where a contrary construction *might raise serious constitutional doubts*, we can impose a limiting construction on a statute only if it is readily susceptible to such a construction.") (emphasis added).

The State does not appear to dispute that, if Defendant's interpretation of RSA 651-B:4-a is correct and the State's narrowing constructions are unreasonable, then the challenged law must be struck down due to lack of tailoring. For example, the State does not appear to contest that, if RSA 651-B:4-a broadly requires the disclosure of online identifiers that have *any* communicative functionality—including the ability to engage in private person-to-person communication *or* the ability to post messages that are accessible to the public (e.g., blogs, posts on newspaper sites, etc.)—then it would be unconstitutional. *See* State's Br. at 15. The State, quite correctly, seeks to avoid this plain reading of the challenged law's text because other courts have struck down similar statutes. *See Harris*, 772 F.3d at 579 (even if the trial court's limiting instruction applying the law to only identifiers used to engage in "interactive communication," concluding that the law still would be unconstitutional); *Doe v. Nebraska*, 898 F. Supp. 2d 1086, 1121 (D. Neb. 2012) (online identifier law applied to blog posts unconstitutional); *White v. Baker*, 696 F. Supp. 2d 1289, 1311 (N.D. Ga. 2010) (striking down online identifier law under strict and intermediate scrutiny because

---

claim. The Court's statement in *Pierce* was not made in the context of a free speech challenge, but rather in the context of the defendant's argument that New Hampshire's harassment statute unconstitutionally shifted the burden of proof to the defendant. *See also Smith v. N.H. Dep't of Revenue Admin.*, 141 N.H. 681, 692 (1997) (addressing burden on challenger, but in commerce clause, not free speech, context). To the extent this statement in *Pierce* even applies in this context, it can at most be read to confirm the axiomatic proposition that someone challenging a statute on free speech grounds has the threshold burden to demonstrate that free speech rights are implicated. Once that initial burden has been met—which it plainly has here—the burden shifts to the government to justify the law. *See Doe v. Harris*, 772 F.3d 563, 570 (9th Cir. 2014).

it failed to focus on "identifiers that are used in the kind of interactive communications that entice children into illegal sexual conduct" and "those sites and facilities where these kinds of interactive communications occur"). Nor does the State appear to dispute that, if RSA 651-B:4-a requires the disclosure of online identifiers—namely, "user identifications" or "user profile information"—that do not have communicative functionality, then it would be unconstitutional because it would encompass innocent online activities. But, as explained in Section II.A.1 *infra*, this is precisely what RSA 651-B:4-a says. Given these apparent concessions, it is of little surprise that the State has now resorted to narrowing constructions to avoid RSA 651-B:4-a's overbroad terms.

The State also does not appear to dispute that RSA 651-B:4-a would be unconstitutional if RSA 651-B:7(I)—which allows the police to make "any use or disclosure of any [online identifiers] as may be necessary for the performance of a valid law enforcement function"—provides the police with unbridled discretion in how to use and disclose online identifiers. *See, e.g., Montenegro*, 166 N.H. at 220 (striking down regulation that encouraged "arbitrary and discriminatory enforcement"). However, the "necessary for the performance of a valid law enforcement function" language provides little, if any, constraint on the ability of New Hampshire law enforcement to use or disclose online identifiers—a reality which creates a chilling effect on registrants' creation and use of online identifiers. *See Harris*, 772 F.3d at 581 ("But sex offenders' fear of disclosure in and of itself chills their speech."). Thus, this case is no different from cases in Georgia, California, and Utah (*Shurtleff I*) where similar laws were struck down for this reason. *See Baker*, 696 F. Supp. 2d at 1310-11 (language allowing disclosure <u>*to law enforcement*</u> for "law enforcement purposes" too broad); *Harris*, 772 F.3d at 580 (language allowing for disclosure to the public "when necessary to ensure the public safety" too broad); *Doe v. Shurtleff*, No. 1:08-CV-64 TC, 2008 U.S. Dist. LEXIS 73787, at *24-26 (D. Utah Sept. 25, 2008) ("*Shurtleff I*") (striking down Utah's original online identifier law where there were "no

restrictions on how [law enforcement] can use or disseminate registrants' internet information"; rejecting narrowing construction that law enforcement should only be allowed to "use internet information for criminal investigations only, and as prohibiting dissemination of that information to the public"), *vacated after law amended by* 2009 U.S. Dist. LEXIS 73955 (D. Utah Aug. 20, 2009) ("*Shurtleff II*"), *aff'd*, 628 F.3d 1217 (10th Cir. 2010) ("*Shurtleff III*").[2] As a result, the State is attempting to narrow this overbroad statute to only allow law enforcement to "use [online identifiers] … in furtherance of an investigation of criminal activity after it has occurred." *See* State's Br. at 14. But, as explained below, this construction also rewrites RSA 651-B:7 by inserting terms that do not exist.

II. The State's Two Narrowing Constructions Manufactured Seven Years After Enactment Must Be Rejected.

A. The State's Narrowing Constructions Are Contrary To The Statute's Plain Terms.

While courts may adopt a narrowing construction to save a law from unconstitutionality if the law is "readily susceptible" to that limitation, *see Reno v. ACLU*, 521 U.S. 844, 884 (1997),

[2] The challenged law here is like the Utah statute originally enjoined as unconstitutional in *Shurtleff I*—not the amended statute at issue in *Shurtleff III*—because it lacks the protections against disclosure that led the Tenth Circuit Court of Appeals to uphold the amended statute. The district court in *Shurtleff I* originally enjoined the law because it did not specify that the government could "use internet information for criminal investigations only," or "prohibit[] dissemination of that information to the public." *See Doe v. Shurtleff*, No. 1:08-CV-64 TC, 2008 U.S. Dist. LEXIS 73787, at *24-26 (D. Utah Sept. 25, 2008). After the state legislature responded to the District Court's decision by amending the law to expressly address these flaws, the district court vacated its earlier injunction; it is that ruling that the Tenth Circuit affirmed in *Shurtleff III*. *Shurtleff III* is inapplicable for several other reasons. *First*, RSA 651-B:4-a is far more burdensome than the one held unconstitutional in *Shurtleff I* and the one deemed constitutional in *Shurtleff III* because RSA 651-B:4-a requires registrants to notify the police *before* they use the online identifier. At the time of *Shurtleff I and III*, Utah registrants were only required to report their online identifiers at their semi-annual registration. *See* UT ST § 77-41-105(3). *Second*, *Shurtleff III* attached great weight to the fact that registrants would not have to report their identifiers until long after they had finished speaking. 628 F.3d at 1225. Again, under RSA 651-B:4-a, registrants must disclose *before* they have even spoken. *Finally*, *Shurtleff III* is unpersuasive because, although it held that the law was subject to intermediate scrutiny, it never applied a narrow-tailoring test. The opinion contains no discussion of what websites were covered by the law, how many of those sites could be used for improper purposes, the likelihood that different categories of registrants would use the Internet to re-offend, or how the law would advance the government's interests. *Coppolino v. Comm'r of the Pa. State Police*, 102 A.3d 1254 (Pa. Commw. Ct. 2014) is similarly distinguishable. Setting aside the fact that *Coppolino* failed to engage in any meaningful narrow tailoring analysis, the Pennsylvania online identifier law upheld there is different from RSA 651-B:4-a because identifiers were to be disclosed within three days of use, rather than before their use.

courts "will not rewrite a … law to conform it to constitutional requirements." *Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 397 (1988); *see also Harris*, 772 F.3d at 578. As the United States Supreme Court has explained, "doing so would constitute a serious invasion of the legislative domain and sharply diminish [the legislature's] incentive to draft a narrowly tailored law in the first place." *United States v. Stevens*, 559 U.S. 460, 481 (2010) ("To read [the law] as the Government desires requires rewriting, not just reinterpretation."). The New Hampshire Supreme Court has embraced these principles. *See, e.g.*, *Montenegro v. N.H. DMV*, 166 N.H. 215, 220 (2014) (striking down regulation that encouraged "arbitrary and discriminatory enforcement," and declining to "add or delete text to the regulation" to save it); *State v. Brobst*, 151 N.H. 420, 422 (2004) (holding that a section of harassment statute was facially overbroad, and concluding that the Court could not envision a limiting construction "that would allow us to limit the scope of the statute without invading the province of the legislature"); *State v. Lukas*, 164 N.H. 693, 694 (2013) ("courts may not add words to a statute that the legislature did not see fit to include"); *Balke v. City of Manchester*, 150 N.H. 69, 73 (2003) ("We will not rewrite the statute; that is the province of the legislature."). Here, the State asks this Court to rewrite the law—and invade the province of the legislature—in two ways.

1. Limitation To "Private Person to Person Communications"

Under the State's first construction, the State contends that RSA 651-B:4-a only applies to online identifiers used to engage in "private person to person electronic communications." *See* State's Br. at 8-9, 15. This construction is inconsistent with the statute's plain terms.

There is nothing in RSA 651-B:4-a's list of examples indicating that the law only encompasses online identifiers that allow private person-to-person communication. The terms "private" and "person-to-person" make no appearance in the statute. If the legislature wanted to limit RSA 651-B:4-a's scope only to these types of online identifiers, it could have done so. It did

not. Instead, as indicated by the statute's terms, the legislature intent's was to broadly "provid[e] law enforcement with the means to monitor and track *the offender's online activities*." *State v. White*, 164 N.H. 418, 422 (2012) (emphasis added); *see also Strike Four v. Nissan N. Am.*, 164 N.H. 729, 739 (2013) (noting the policy of interpreting "legislative intent from the statute as written," and the policy that courts "will not consider what the legislature might have said or add language that the legislature did not see fit to include").

When the New Hampshire Supreme Court had the opportunity in *White* to interpret RSA 651-B:4-a, it also made no reference to the State's current narrowing construction. Rather, the Court explained that RSA 651-B:4-a's examples of online identifiers must be read in isolation, independent of one another. *See White*, 164 N.H. at 422 (noting that the list in RSA 651-B:4-a contains "independent examples of online identifiers"). For example, when examining the term "user profile information" in isolation, the Court *did not* narrow it by requiring some sort of communicative functionality, let alone require private person-to-person communicative functionality. Instead, the Court simply explained that a "user profile" "refers to a set of personal facts that a person provides to a website in order to create an account"—a definition it concluded captured a social media account, but also would include a Dartmouth Hitchcock account or a profile at a website *without communicative functionality*. *Id.* at 423 (also referring to a "profile" as "a biographical account presenting [user's] noteworthy characteristics and achievements.").[3]

The federal law upon which the State heavily relies is also inconsistent with the State's narrowing construction. *See* State's Br. at 8-9. Under 42 U.S.C. § 16915a(e)(2), an "internet identifier" is defined as "electronic mail addresses and other designations used for self-identification or routing in Internet communication or posting." *See also* 73 Fed. Reg. 38030-01

[3] The State does not explain whether RSA 651-B:4-a requires registrants to disclose which "instant message screen names" or "user identifications" they use *and* where they use those online identifiers.

(July 2, 2008) ("The authority under section 114(a)(7) is accordingly exercised to require that the information included in the registries must include all designations used by sex offenders for purposes of routing or self-identification in Internet communications or postings."). As with RSA 651-B:4-a, this federal law does not use the terms "private" or "person-to-person." If the legislature wanted to adopt the language in this federal statute to capture any perceived limitations it contains, it could have. It did not. In any event, this federal law makes clear that a covered online identifier is not limited to those used to engage in "private person to person communications," but rather broadly includes all designations used for routing or self-identification in Internet *postings*. Thus, this law includes all online identifiers used to engage in any postings on the Internet, which captures both private and public posts, including (i) identifiers associated with comments on news websites, (ii) identifiers associated with feedback submitted sites like Yelp or Amazon, and (iii) even a personal blog.

The State's narrowing construction is also contradicted by its own statements to the New Hampshire Supreme Court in *White*. There, the Attorney General's Office offered an interpretation of RSA 651-B:4-a that is broader than the one it is currently presenting. Rather than arguing that covered online identifiers are limited to those used to engage in "private person to person communications," the Attorney General's Office explained that the law, consistent with federal guidance, included "*all designations* used by sex offenders for purposes of routing or self-identification *in Internet communications or postings.*" *See* State's Br. in White at 15 (Second Biss. Dec., ¶ 3, *Ex. JJ*) (emphasis added). The State is estopped from adopting this narrowing construction after having prosecuted defendants for seven years under this constitutionally overbroad interpretation. *See Pike v. Mullikin*, 158 N.H. 267, 270 (2009).

Finally, if this Court needs any further evidence demonstrating that this narrowing construction is untethered to RSA 651-B:4-a's plain terms, it need look no further than how the

State has interpreted and enforced RSA 651-B:4-a in this case. Here, one of the online identifiers that the State alleges Defendant did not disclose in the February 2015 indictments—a www.brandyourself.com account—may fall *outside* the very narrowing construction that the State has now proffered.[4] *See* Indictment (First Biss. Dec., ¶ 33, *Ex. FF* at BON003). Perhaps in recognition that this indictment would undermine this newfound construction, the State *nolle prossed* this charge on October 27, 2015—six (6) days before the State's Objection was due. Apparently, when this case was initially charged in February 2015, the State read RSA 651-B:4-a differently than it does today. If the State is having difficulty consistently interpreting RSA 651-B:4-a in this case, then how can registrants untrained in the law be expected to correctly interpret and comply with it terms? This proves the law's ambiguity. *See Nebraska*, 898 F. Supp. 2d at 1115-16 ("these proposed limiting constructions are good examples of the expansive and vague nature of the statute"; *see* discussion of Google+).

2. Limitation To "Investigations of Criminal Activity After It Has Occurred"

Though the State pays short shrift to RSA 651-B:7(I)'s broad terms, the State appears to argue that its language allowing law enforcement to "use or disclose" online identifiers "as may be necessary for the performance of a valid law enforcement function" should be limited to allowing the police to use online identifiers only "in furtherance of an investigation of criminal activity *after* it has occurred." *See* State's Br. at 14 (emphasis added).[5] The State makes little effort to argue that this construction has any foundation in the text of RSA 651-B:7. *See id.* Indeed, RSA 651-B:7 contains no such limitation.

It cannot seriously be disputed that, as a textual matter, the term "valid law enforcement

[4] And even if this www.brandyourself.com website does fall within the State's narrowing construction, this would demonstrate the law's unconstitutionality because this website has nothing to do with criminality.

[5] The State's interpretation of RSA 651-B:7 must also mean that *all* information disclosed by registrants—not just online identifiers—cannot be used by law enforcement until after criminal activity has occurred.

function" is not limited to investigating a crime after it has occurred, but rather includes a whole host of legitimate law enforcement activities occurring before a crime has been committed, including (i) actions designed to prevent future crimes before they happen, or (ii) the monitoring of online activity to seek out crimes as they occur in real time. *See Baker*, 696 F. Supp. 2d at 1311 ("While this monitoring could lead to the discovery of communications intended to harm children and thus would be a substantial benefit in identifying those making them, this section simply is too broad."). For example, under RSA 651-B:7(I)'s plain meaning, a police officer would be well within his right to disclose a registrant's online identifiers to the registrant's neighbors if the officer believed that doing so would prevent the registrant from engaging in future criminal activity over the Internet. Preventing future crime is undoubtedly a "valid law enforcement function." Under the RSA 651-B:7(I)'s plain meaning, a police officer would also be well with his right to take a registrant's online identifiers and then anonymously attempt to engage the registrant over the Internet in the hope of encouraging illegal activity that could then be prosecuted. Of course, catching a criminal in the act is a "valid law enforcement function."

The State's construction also runs contrary to the New Hampshire Supreme Court's decision in *White*. Again, as the *White* Court explained, the purpose of the online identifier statute, as indicated by its terms, was not simply to allow law enforcement to investigate crimes after they occurred, but to enable law enforcement "to monitor and track the offender's online activities," which includes in real time even in the absence of completed criminal activity. *White*, 164 N.H. at 422. Setting aside the fact that legislative intent is derived "from the statute as written"—not the legislative history—the legislative history does not suggest that online identifiers can only be used after criminal activity has occurred. *See Strike Four*, 164 N.H. at 739. The State has also produced no evidence indicating that law enforcement agencies have interpreted RSA 651-B:7 in this fashion since its inception.

Simply put, it is not the responsibility of this Court to "invad[e] the province of the legislature" and write a more carefully tailored time, place, and manner legislation that the legislature might have enacted but did not. *See Brobst*, 151 N.H. at 422.

B. The State's Narrowing Constructions Have Been Manufactured *Post Hoc* In Response To This Litigation.

After seven years of using a broader interpretation, the State simply "made up" these narrowing constructions in a pleading in direct response to Defendant's Motion to Dismiss. This behavior further demonstrates RSA 651-B:4-a's ambiguity and the fact that the law is not readily susceptible to these newfound constructions. *See City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 755-56 (1988) (narrowing constructions must "be made explicit by textual incorporation, binding judicial or administrative construction, or well-established practice," and declining to "write nonbinding limits into a silent state statute").

The Office of the Attorney General's litigation-driven interpretations are not the product of any prior practice, let alone a "well established" practice. *See id.* at 770 n.11. For the past seven years until the State's Objection was filed on November 2, 2015, no one knew that these constructions existed. This is because they did not exist. As Defendant's exhibits indicate, no law enforcement agency or administrative body has adopted such constructions in their policies or procedures. *See* Nineteen Right-to-Know Requests and Responses (Biss. Dec., ¶¶ 11-29, Exs. J-BB). There is no evidence that the Attorney General's Office has ever communicated these constructions to law enforcement or county prosecutors on the ground. There is no evidence that any prosecutor has ever communicated these constructions to a single judge. (To the contrary, the State argued for a broader interpretation before the New Hampshire Supreme Court in *White*.) There is no evidence that law enforcement have ever communicated these constructions to a single registrant. *See id.* The registration form itself makes no mention of these interpretations.

Until November 2, 2015, Defendant had never been informed that these constructions existed. These constructions are not in the police reports in this case. Indeed, contrary to these *post hoc* constructions, Defendant (i) was initially charged for allegedly not disclosing a www.brandyourself.com account by the [redacted] Police Department and Rockingham County Attorney's Office and (ii) was informed by the [redacted] Police Department that he needs to disclose any account with www.healthcare.gov. Either these law enforcement agencies are unsure about what the statute covers or they, at the time, disagreed with the Office of the Attorney General's new constructions. Either way, the State's own internal confusion shows the law's ambiguity. While a registrant is required to know RSA 651-B:4-a's terms, a registrant should not be required to be an expert in Chapter 651-B's legislative history or federal law and then guess how RSA 651-B:4-a's ambiguous terms will be construed by law enforcement in light of these texts—especially when guessing wrong and underdisclosing imposes criminal liability.

The Attorney General's Office does not have the authority to unilaterally narrow RSA 651-B:4-a under Chapter 651-B's terms. This is the legislature's role. The Attorney General's Office also cannot unilaterally relieve registrants of their legal obligation to report statutorily enumerated categories of information. Nor can the Attorney General's Office prevent local law enforcement or county prosecutors from demanding the categories of information that RSA 651-B:4-a expressly requires. In fact, local prosecutors and police must enforce the statute as written unless the legislature directs otherwise. *See* RSA 7:6 ("with the aid of the county attorneys, the attorney general shall enforce the criminal laws of the state"). The Office of the Attorney General's interpretations do not create a binding judicial or administrative construction. The Attorney General's Office can change these interpretations in the future at any time.

The State's apparent promise to only enforce the law consistent with these constructions does not save the statute. As the Ninth Circuit Court of Appeals explained in *Harris*, this Court

"cannot assume that, in its subsequent enforcement, ambiguities will be resolved in favor of adequate protection of First Amendment rights." *Harris*, 772 F.3d at 579, 580-81 (citing *Lakewood*, and noting that "the promise from the State that it will use the power appropriately is not sufficient"); *see also United States v. Stevens*, 559 U.S. 460, 480 (2010) ("The Government's assurance that it will apply [the challenged law] far more restrictively than its language provides is pertinent only as an implicit acknowledgment of the potential constitutional problems with a more natural reading."). This is especially true here where the State has demonstrated a willingness both historically and in this case to enforce RSA 651-B:4-a more broadly than its newfound interpretations. As in *Stevens*, "[t]his prosecution is itself evidence of the danger in putting faith in Government representations of prosecutorial restraint." *Id.*

III. Even If The State's Narrowing Constructions Are Reasonable (Which They Are Not), They Do Not Cure The Statute's Constitutional Defects.

Even if these constructions are reasonably tethered to Chapter 651-B's terms—which they are not—they do not cure RSA 651-B:4-a's constitutional infirmities.

A. Investigating Criminal Conduct

The State contends that RSA 651-B:4-a is necessary because "online identifiers can be a crucial tool in law enforcement investigations into criminal conduct and can even be used to locate victims based on their last known internet communications." *See* State's Br. at 13. However, under any construction of the law, the law is still not narrowly tailored.

First, even assuming that RSA 651-B:4-a only requires the disclosure of online identifiers with communicative functionality—regardless of whether the communication is private or public—this would compel registrants to provide information about screen names and profiles that have no nexus to criminality. For example, the law would encompass identifiers used (i) to post comments about articles on a newspaper's website, (ii) to blog, or (iii) to comment on Yelp.com or

Amazon.com. And, even if the Court accepts the State's *post hoc* narrowing construction that the law only applies to online identifiers allowing private person-to-person communications, the law would still be overbroad. It goes without saying that not all websites that allow private communications have any nexus to criminality. For example, this construction would capture identifiers used to access: (i) the website www.whitehouse.gov (which allows members of the public to privately send a message the President), (ii) Dartmouth Hitchcock (which allows a patient to "[c]ommunicate with your health care team"), (iii) www.att.com (which has "chat" functionality for customer support), (iv) www.llbean (which has "chat" functionality for customer support), and (v) TurboTax (which can connect a person preparing his or her taxes to someone for assistance). This case brings this reality close to home. If a www.brandyourself.com account has private person-to-person chat functionality, it too would be subsumed by the State's construction notwithstanding the fact it would be virtually impossible to use this commercial website to commit a registerable offense. Another indictment in this case also alleges that Defendant failed to disclose a LinkedIn account—a networking website for business professionals that has person-to-person communicative functionality. *See* Indictments (First Biss. Dec., ¶ 33, *Ex. FF* at BON004). It is difficult to imagine a LinkedIn account, even with its private messaging functionality, being used to illegally solicit minors. *See Harris*, 772 F.3d at 579 (even narrowing construction "would not necessarily alleviate the chilling effect caused by the ambiguities in the Act").

Second, even under the State's construction, the law is also overbroad in addressing criminal conduct because it applies to registrants who have never committed an Internet crime.

Finally, after seven years of collecting online identifiers and enforcing RSA 651-B:4-a, the State still has provided no evidence indicating that, since 2009, previously unknown online identifiers disclosed under RSA 651-B:4-a have been used to apprehend a perpetrator or find a victim. This lack of evidence demonstrates that the challenged law is far more likely to impact

innocent expression than assist law enforcement in addressing criminal behavior. *See Rideout*, 2015 U.S. Dist. LEXIS 105194, at *30 ("For an interest to be sufficiently compelling, the state must demonstrate that it addresses an actual problem.").

B. Tracking Missing Registrants

The State also contends that RSA 651-B:4-a is designed to assist law enforcement "[i]n the event that a registered sex offender fails to report or goes missing." *See* State's Br. at 12-13.

First, this was not the rationale used by the legislature to justify RSA 651-B:4-a, and thus must be discarded. *See Guare v. State*, 117 A.3d 731, 740 (N.H. 2015) (*quoting Cmty. Res. for Justice, Inc. v. City of Manchester*, 154 N.H. 748, 762 (2007) ("To meet this 'demanding' burden [applying intermediate scrutiny], the government must demonstrate that its justification is genuine, not hypothesized or invented post hoc in response to litigation.")). Rather, the legislative history addressing the challenged law simply states that the law is necessary because sex offenders "can log on anonymously [to social networking sites] to meet and lure minors." *See* Legislative History (First Biss. Dec., ¶¶ 31-32, *Ex. DD* at LEG-S 111-12, and *Ex. EE* at LEG-H 105-06). This *post hoc* justification is also inconsistent with the New Hampshire Supreme Court's pronouncement that the challenged law is more broadly designed to "provid[e] law enforcement with the means to monitor and track the offender's online activities." *White*, 164 N.H. at 422.

Second, RSA 651-B:4-a is not narrowly tailored to this purported interest in tracking missing registrants. This is because RSA 651-B:4-a applies to *all* registrants, not just those who (i) have in the past failed to comply with their reporting obligations or (ii) are, by some principled measurement, likely to not comply with their reporting obligations in the future. While most registrants may naturally dislike Chapter 651-B's onerous reporting obligations that subject them to forced interactions with the police, the State's assumption that *all* registrants "pose[] the same risk of evading their registration requirements" is unsupported and wrong. *See* State's Br. at 14.

Registrants are motivated to comply with Chapter 651-B's obligations in full. If they do not, they will be subjected to severe criminal penalties. Even if a registrant's failure to report information is negligent, prosecutors routinely charge "failure to report" offenses as "knowing" violations subject to Class B felony penalties under the premise that registrants have filled out a form acknowledging that they are subject to Chapter 651-B's terms.[6] This case is an example of this type of prosecutorial zeal that has transformed "failure to report" charges into strict liability offenses. *See, e.g.*, Reports (First Biss. Dec., ¶ 33, Ex. FF at BON074). Here, RSA 651-B:4-a would more narrowly achieve its goal of tracking missing registrants if it applied only to those registrants who are likely to go missing—namely, registrants who have failed to comply in the past. The legislature never considered this more narrowly tailored approach.

Third, to the extent RSA 651-B:4-a is aimed at addressing registrants' purported "incentive[s] to avoid using [their] real name[s] or identit[ies] over the internet," *see* State's Br. at 14, the law is not narrowly tailored even under the State's construction because it sweeps within its scope online identifiers where registrants are *not* shielding their identities. *See White*, 164 N.H. at 422 (social media page using registrant's actual name was encompassed under challenged law).

Fourth, if the purpose of RSA 651-B:4-a is to allow law enforcement to track missing registrants, then the State's narrowing construction is not tailored to this interest. If, as the State contends, only online identifiers used to engage in private communications must be disclosed, then it is difficult to imagine how law enforcement would find such online identifiers useful in tracking down a missing registrant because the communications would not be public. Here, the State has

[6] The police have gone so far as to interrogate one registrant—Michael Daley—when he voluntarily self-reported an email account in an effort to determine whether the account was created before the disclosure. When the registrant admitted that the account was created approximately five to six months prior to the disclosure, he was charged. *See* Concord Documents, Michael Daley Police Reports (First Biss. Dec., ¶ 23, Ex. V, pages 37-45). However, Mr. Daley had never used the email account to send a message, and the account was previously disclosed to his Probation Officer. This type of enforcement after as registrant voluntarily reports an online identifier will only deter the voluntary reporting of online identifiers, which runs counter to the goals of Chapter 651-B.

not shown "that the regulation will in fact alleviate [these] harms in a direct and material way." *Turner Broad. Sys. v. FCC*, 512 U.S. 622, 664 (1994) (plurality). In any event, the fact that such identifiers "may" be helpful in abstract hypotheticals is insufficient to satisfy narrow tailoring. *See Santa Monica Food Not Bombs v. City of Santa Monica*, 450 F.3d 1022, 1041 (9th Cir. 2006) ("The term 'may,' in other words, simply takes in too many circumstances that do not, as matters actually turn out, implicate the governmental interests justifying the permitting requirement.").

Finally, the State has presented no evidence demonstrating that, since 2009, (i) all registrants are likely to fail to comply with Chapter 651-B and "go missing" and (ii) previously-unknown online identifiers disclosed under RSA 651-B:4-a have assisted law enforcement in successfully finding missing registrants. The State has also not presented evidence demonstrating that, without online identifiers, it has found it difficult to track down missing registrants despite all the other information registrants must disclose. Thus, the challenged law is far more likely to impact registrants who are fully compliant with Chapter 651-B's reporting obligations, than registrants who have gone (or are likely to go) missing.

C. The Law Is Substantially Overbroad

The State believes that RSA 651-B:4-a's broad application to *all* registrants (including those who are not a danger and who have no history of failing to comply) and to speech that has no nexus to criminality is necessary because (i) *some* registrants may engage in misconduct on the Internet or may go missing and (ii) access to online identifiers may make it easier for the police to respond effectively. However, this sort of justification for restricting speech is alien to First Amendment values. The First Amendment is a bulwark against not only legislative suppression of speech, but also legislative indifference and expedience. *See McCullen*, 134 S. Ct. at 2540. The First Amendment ensures that the government may not unduly burden free expression by choosing to restrict speech as its first option to prevent crime or achieve some other goal, rather than as a

last resort. *See Ashcroft v. Free Speech Coalition*, 535 U.S. 234, 245 (2002) ("The prospect of crime … by itself does not justify laws suppressing protected speech."); *Thompson v. W. States Med. Ctr.*, 535 U.S. 357, 373 (2002) ("If the First Amendment means anything, it means that regulating speech must be a last—not first—resort."); *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973).

But this is precisely what the legislature did here. The legislature failed to consider applying the law only to those registrants who were convicted of offenses involving the Internet or who are at high risk of re-offending. The legislature failed to consider applying the law to only online identifiers that have a nexus to criminality. And the legislature failed to consider applying the law to only registrants who previously were convicted of not complying with Chapter 651-B's reporting obligations. *See McCullen*, 134 S. Ct. at 2524 (the State had "not shown that it seriously undertook to address [its] various problems with the less intrusive tools readily available to it").

Finally, unlike the laws upheld in *Shurtleff III*, 628 F.3d 1217, 1225 (10th Cir. 2010) and *Coppolino v. Comm'r of the Pa. State Police*, 102 A.3d 1254, 1283 (Pa. Commw. Ct. 2014), RSA 651-B:4-a requires a registrant to disclose to the government an online identifier ***before*** he can use that identifier to engage in speech.[7] This reality, which the State acknowledges but then ignores, chills innocent Internet activity.[8] *See* State's Br. at 4 (admitting that "[a]ny changes or new online identifiers must be reported prior to their use"); *see also Harris*, 772 F.3d at 581 (preliminarily enjoining similar, but less restrictive, Internet identifier law that required the disclosure of Internet identifiers "within 24 hours of using a new Internet identifier"). And even if the State's tortured construction of RSA 651-B:7 limiting the police's usage of online identifiers until after a crime has been committed were read into the law, this too would not cure RSA 651-B:4-a's lack of

[7] *See supra* note 2.

[8] Defendant has been informed by the [redacted] Police Department that ***all*** amendments, including to his online identifiers, must be done in person.

tailoring for all the reasons above—namely, because it criminalizes far too much anonymous, constitutionally-protected speech by too many speakers and requires disclosure as a prerequisite to using an online identifier to engage in speech.[9]

Accordingly, even under the State's constructions, RSA 651-B:4-a is unconstitutional because "it applies in numerous circumstances that have no relation to [the State's] significant interests." *See Doyle v. Comm'r, N.H. Dep't. of Res. & Econ. Dev.*, 163 N.H. 215, 228 (2012).[10]

WHEREFORE, for these reasons and the reasons in Defendant's Motion to Dismiss, Defendant respectfully requests that this Court grant his Motion.

[9] The State's attempt to distinguish the cases cited by Defendant fails. *See* State's Br. at 17-19. In *Doe v. Harris*, 772 F.3d 563 (9th Cir. 2014), the legal issue was the same as in this case—namely, whether an online identifier law is facially unconstitutional under the First Amendment. The *Harris* Court concluded that the "necessary to ensure the public safety" language in the California law did not meaningfully constrain law enforcement's ability to use and disclose online identifiers. *Id.* at 579-81. RSA 651-B:7's "valid law enforcement function" language is no different. *White v. Baker*, 696 F. Supp. 2d 1289, 1294 (N.D. Ga. 2010) is similarly indistinguishable. Just as the language "necessary to protect the public concerning sex offenders" did not cabin law enforcement's discretion in how identifiers can be used, the same is true here under RSA 651-B:7. This case is also indistinguishable from *Doe v. Nebraska*, 898 F. Supp. 2d 1086 (D. Neb. 2012). There, the law covered blog posts. Similarly, RSA 651-B:4-a, even when applying the federal requirements as the State suggests, captures postings, which includes blog postings.

[10] The State suggests that, if RSA 651-B:4-a is struck down, New Hampshire would lose federal funds under the Sex Offender Registration and Notification Act ("SORNA") because New Hampshire currently "substantially complies" with SORNA. *See* State's Br. at 4. However, as of April 2014, the federal government's own website does not list New Hampshire as one of the 17 states that has been found to be in substantial compliance with SORNA. *See* SORNA Website (Second Biss. Dec., ¶ 4, *Ex. KK*); *see also* http://www ncsl.org/research/civil-and-criminal-justice/adam-walsh-child-protection-and-safety-act.aspx. The Attorney General's Office acknowledged this lack of substantial compliance in 2013. *See* sos.nh.gov/WorkArea/DownloadAsset.aspx?id=46872. This is perhaps due to the fact that the cost of SORNA compliance is considerable. New Hampshire has apparently applied for reallocation of the funding penalty in 2015 to work solely towards furthering SORNA implementation activities and efforts. *See* http://www.smart.gov/newsroom.htm. In any event, to the extent New Hampshire currently receives SORNA funds, it is difficult to imagine that the federal government would withhold funds if this Court, like the multiple courts before it, enforced the First Amendment by striking down a "online identifier" statute. The State has produced no evidence indicating that it would lose a single dollar if RSA 651-B:4-a was struck down. And even it could, the State's desire to obtain federal funds does not trump the First Amendment.

Respectfully submitted,

[redacted]

Gilles R. Bissonnette (N.H. Bar No. 265393)
AMERICAN CIVIL LIBERTIES UNION OF NEW HAMPSHIRE
18 Low Avenue
Concord, NH 03301
Tel.: 603.224.5591
gilles@aclu-nh.org

John M. Greabe (N.H. Bar No. 18706)
296 Gage Hill Road
Hopkinton, NH 03220
Tel.: 603.513.5191
john@greabe-law.com

Mark Sisti (N.H. Bar No. 2357)
SISTI LAW OFFICES
387 Dover Road
Chichester, NH 03258
Tel.: 603.224.4220
msisti@sistilawoffices.com

Dated: November 20, 2015

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing has this day been mailed to the following:

Matthew Broadhead
Rebecca Woodard
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Annalise H. Wolf, Esq.
Rockingham County Attorney's Office
P.O. Box 1209
Kingston NH 03848
E-mail: awolf@rcao.net

Gilles Bissonnette, Esq.