STATE OF NEW HAMPSHIRE

ROCKINGHAM, SS. SUPERIOR COURT

[redacted]

STATE OF NEW HAMPSHIRE

v.

[redacted]

DEFENDANT'S MOTION TO DISMISS
(ORAL ARGUMENT REQUESTED)

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

TABLE OF CONTENTS

INTRODUCTION

Defendant moves to dismiss all five (5) charges of knowingly violating RSA 651-B:4-a because this statute, on its face,[1] violates the First Amendment of the United States Constitution and Part I, Article 22 of the New Hampshire Constitution. RSA 651-B:4-a imposes burdensome reporting requirements on online speech—and even bans *all* online anonymous communications—engaged in by *all* persons convicted at any time of any offense that requires registration, including misdemeanors and convictions that occurred well before the registry went into effect ("registrants").

RSA 651-B:4-a came into effect on January 1, 2009 and expressly requires all of New Hampshire's approximately 2,700 registrants[2] to disclose to the police information about their use of "online identifiers" for expressive purposes. For example, this law requires registrants to provide information about online activities that are wholly innocent and have no possible relationship to criminality, such as the screen names and profiles they use (i) to post comments about articles on a newspaper's website, (ii) to access political discussion groups, (iii) to run their business, (iv) to sign up for health insurance online at www.healthcare.gov under the Affordable Care Act or to set up an online account with a health care provider, or (v) to provide comment to the President of the United States at www.whitehouse.gov. Even more problematic, when registrants want to engage in this innocent speech using a new screen name, they must now provide information about that name to the police *before engaging in this speech*. Put another way, under RSA 651-B:4-a, government disclosure is a necessary prerequisite to engaging in this

[1] If this Motion is denied, Defendant will argue that RSA 651-B:4-a is unconstitutional as applied to him and the online identifiers the State alleges he did not disclose. *See State v. Hollenbeck*, 164 N.H. 154, 159 (2012) (deciding facial challenge at motion to dismiss stage, and concluding that "to extent that as-applied challenge depends upon facts and evidence beyond those given in indictment, it must be denied before trial").

[2] *See* Lynne Tuohy, "Lawmakers Debate Lifting Sex Offender Residency Restrictions," *Associated Press* (Mar. 1, 2015), *available at* http://www.seacoastonline.com/article/20150301/NEWS/150309937/0/wap&template=wapart (noting that New Hampshire has 2,700 sex offender registrants).

form of innocent, protected speech, which clearly creates a chilling effect on innocent Internet activity. And, as the State's draconian charges demonstrate, the failure to disclose this online identifier to the government prior to engaging in this innocent speech is with real consequence—a "knowing" failure is a class B felony and a "negligent" failure is a misdemeanor offense.

The facts of this case further highlight the law's facial unconstitutionality. Defendant is being charged with five (5) separate counts of knowingly failing to disclose online identifiers, which could yield a maximum sentence of up to thirty-five (35) years in prison and fines of up to $20,000. Yet the alleged online identifiers at issue have no relationship to criminal conduct [redacted]

RSA 651-B:4-a is facially unconstitutional for at least five (5) independent reasons. ***First***, the law impermissibly makes disclosure of an online identifier a prerequisite for the registrant to use that online identifier to engage in innocent, protected speech. *See* RSA 651-B:4-a (disclosure required "before using the online identifier"). Indeed, this statute is far worse than a California law recently preliminarily enjoined by the Ninth Circuit Court of Appeals that required the disclosure of Internet identifiers "within 24 hours of using a new Internet identifier." *See Doe v. Harris*, 772 F.3d 563, 581 (9th Cir. 2014) (Bybee, J.). As the Ninth Circuit held there, "[t]he Act's 24-hour reporting requirement thus undoubtedly chills First Amendment Activity. Of course, that chilling effect is only exacerbated by the possibility that criminal sanctions may follow for failing to update information about Internet identifiers …." *Id.* RSA 651-B:4-a is no different, especially where it requires a registrant to constantly update the government ***before*** he or

she wants to engage in speech online.

Second, the law criminalizes far too much anonymous, constitutionally-protected speech by too many speakers and allows the information to be used for too many purposes. The statute, for example, requires disclose of online identifiers used for *all* online speech, even if the online identifier pertains to news, politics, and professional activity, and could not possibly be used to commit a crime. For example, the law requires disclosure of screen names registrants use to post comments about articles on a newspaper's website or names that they use to access political discussion groups. RSA 651-B:4-a also applies to *all* registrants, regardless of the severity, type, or age of the underlying offense and whether it had any connection whatsoever to the Internet or to children. Only 1% of sex-crimes against children involve any sort of technology, and even fewer involve the use of the Internet. Registered sex offenders make up only 2% to 4% of persons arrested for technology-facilitated sex crimes against youth. And after a number of years in the community without a new arrest, sex offenders are *less likely* to re-offend than a non-sexual offender is likely to commit an "out of the blue" sexual offense. Thus, RSA 651-B:4-a criminalizes many types of speech using undisclosed online identifiers—and the speech of many people—that do not pose the dangers with which the statute is concerned. RSA 651-B:4-a also contains no real restrictions on the purposes for which the information may be used by law enforcement, especially where the law expressly allows the police to make "any use or disclosure of any such information as may be necessary for the performance of a valid law enforcement function." RSA 651-B:7(I).

Third, RSA 651-B:4-a is not narrowly tailored and violates due process because it is impossibly vague. It requires registrants to immediately report all "online identifiers," but the definition of this term—particularly its examples of "user identification" and "chat or other

Internet communication name or identity information"—leaves it entirely unclear whether the law triggers reporting obligations for creating an account with, for example, a banking institution. This vague definition does not give registrants sufficient notice of what they need to report to comply with the law—a vagueness that is particularly intolerable given the free speech rights implicated and severe criminal penalties for lack of compliance. In interpreting an online identifier law in California that swept within its scope "similar Internet communications," the Ninth Circuit correctly held that such terminology was ambiguous and not susceptible of a narrowing instruction: "[W]hether narrowly construed or not, the ambiguities in the statute may lead registered sex offenders either to overreport their activity or underuse the Internet to avoid the difficult questions in understanding what, precisely, they must report. This uncertainty undermines the likelihood that the [Act] has been carefully tailored to the [State's] goal of protecting minors and other victims." *Harris*, 772 F.3d at 579. The same is true here. The phrases "user identification" and "chat or other Internet communication name or identity information" are indecipherable. Given this ambiguity and the criminal penalties RSA 651-B:4-a imposes, the law will cause registrants to either overreport their activity (either voluntarily or per the instruction of police) or to suppress their usage of the Internet—either of which intrude on registrants' speech rights.

Fourth, the State cannot show how RSA 651-B:4-a has achieved—and will achieve in the future—its objectives in preventing or detecting crimes. In response to Right-to-Know records requests submitted by the American Civil Liberties Union of New Hampshire, New Hampshire law enforcement agencies could not identify a single case in which an online identifier disclosed by a sex offender pursuant to RSA 651-B:4-a was used to uncover subsequent criminal activity that resulted in the filing of criminal charges against that sex offender. While it appears from over

6 years of data that the online identifiers disclosed under RSA 651-B:4-a have not been used to detect a single crime, more than 32 individuals—including the Defendant—have been charged for failing to disclose online identifiers pursuant to RSA 651-B:4-a from 2009 to 2014.

Finally, RSA 651-B:4-a is unconstitutional because it violates registrants' associational rights by potentially compelling disclosure of their participation in online forums organized by political and other groups and by compelling disclosure of the identity of other registrants with whom they discuss political issues.

At least five federal courts have invalidated or enjoined the enforcement of similar laws that require sex offenders to provide the government with identifying information about their online speech. *See Doe v. Harris*, 772 F.3d 563 (9th Cir. 2014)*; Doe v. Nebraska*, 898 F. Supp. 2d 1086 (D. Neb. 2012); *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010); *see also Doe v. Shurtleff*, No. 1:08-CV-64 TC, 2008 U.S. Dist. LEXIS 73787 (D. Utah Sept. 25, 2008), *vacated after law amended by* 2009 U.S. Dist. LEXIS 73955 (D. Utah Aug 20, 2009), *aff'd*, 628 F.3d 1217 (10th Cir. 2010); *Doe v. Snyder*, No. 12-11194, 2015 U.S. Dist. LEXIS 41681, at *63-79 (E.D. Mich. Mar. 31, 2015). These courts reached this conclusion, in part, because laws like RSA 651-B:4-a ignore the importance of the Internet in modern life. As the First Circuit Court of Appeals has explained, "[a]n undue restriction on internet use renders modern life—in which, for example, the government strongly encourages taxpayers to file their returns electronically, where more and more commerce is conducted on-line, and where vast amounts of government information are communicated via website—exceptionally difficult." *See United States v. Perazza-Mercado*, 553 F.3d 65, 72 (1st Cir. 2009) (quoting *United States v. Holm*, 326 F.3d 872, 878 (7th Cir. 2003)).

Like communists in the 1920s and 1950s and Jehovah's Witnesses in the 1930s and 1940s, sex offenders who have completed all conditions of their sentence are the political pariahs of our

day. This animus has led legislatures throughout the country to reflexively enact increasingly harsh laws like RSA 651-B:4-a specifically targeted at registrants that encroach on intimate aspects of their daily lives. Our courts are the public's last line of defense for civil liberties in such situations. This Court should view RSA 651-B:4-a with deep skepticism given its explicit targeting of a disfavored group. Here, RSA 651-B:4-a was enacted with little, if any, examination by the legislature as to how it would impact innocent speech and what its definitions even mean. The legislature did not even consider, as is constitutionally required, less intrusive means to address public safety, including the possibility of narrowing the law so it only impacted registrants who were convicted of offenses involving the Internet or who are at high risk of re-offending. *See McCullen v. Coakley*, 134 S. Ct. 2518, 2524 (2014) (striking down content-neutral 35-foot buffer zone around reproductive health care facilities as not narrowly tailored because the State had "not shown that it seriously undertook to address these various problems with the less intrusive tools readily available to it"). While perhaps politically expedient, this lack of tailoring renders RSA 651-B:4-a facially unconstitutional under the First Amendment and Part I, Article 22 of the New Hampshire Constitution. Accordingly, this Court should dismiss this prosecution in its entirety.

FACTUAL BACKGROUND

I. The New Hampshire Sex Offender Registry.

In New Hampshire, every person who has ever been convicted of a variety of offenses—including convictions occurring before the registry went into effect[3]—must register as a sex offender, with some being obligated to do so for the rest of their lives. *See* RSA 651-B:2. The requirement applies to persons convicted of a number of listed crimes, *see* RSA 651-B:1(V), (VII), as well as to persons who committed non-registerable offenses "as a result of sexual compulsion

[3] [redacted]

or for purposes of sexual gratification and [where] protection of the public would be furthered by requiring the person to register." *See* RSA 651-B:1(V)(c), (VII)(e). For example, registerable offenses include misdemeanor violation of privacy, *see* RSA 644:9 (III-a), or a second offense within a 5-year period for misdemeanor indecent exposure and lewdness, *see* RSA 645:1(I)—a statute which could be broadly construed to criminalize erotic dancing on a stage at a bar. *See* RSA 651-B:1(VIII)(a).

New Hampshire's registration law specifically requires that registrants provide local law enforcement with, among other things, their address, employer, professional licenses, social security numbers, landlord information, telephone numbers, and license plate numbers. *See* RSA 651-B:4(III). Registrants must provide this information "within 5 business days after the person's release, or within 5 business days after the person's date of establishment of residence, employment, or schooling in New Hampshire." *See* RSA 651-B:4(I). Moreover, "[w]hen there is a change to any of the information that a [registrant] is required to report …, the offender shall give written notification of the new information to the local law enforcement agency to which he or she last reported under RSA 651-B:4 within 5 business days of such change of information." *See* RSA 651-B:5(I).

Because New Hampshire's registration statute is so broad and because it fails to distinguish between sex offenders who pose a high risk to the public, there are currently more than 2,700 people required to register in New Hampshire.[4]

[4] In *Doe v. State*, 111 A.3d 1077 (N.H. 2015), the New Hampshire Supreme Court held that Chapter 651-B's lifetime registration requirements were unconstitutional under Part I, Article 23 of the New Hampshire Constitution's ban of retrospective laws as applied to a petitioner who (i) was convicted in 1987 but made subject to the registry in 1994, (ii) had not reoffended in nearly 30 years, (iii) had completed counseling, (iv) was discharged from probation early, and (v) was permanently disabled. *Id.* at 1100. The Court concluded that lifetime registration requirements could be enforced against the petitioner consistent with Article 23 only if he was promptly given an opportunity to demonstrate at a hearing that he is no longer dangerous sufficient to justify continued registration. *Id.* at 1101; *see infra* note 14.

II. The Requirements of RSA 651-B:4-a and Legislative Intent.

Effective January 1, 2009, RSA 651-B:4-a adds to the type of information an offender is required to disclose and supplement. In particular, registrants are now required to provide to law enforcement "any online identifier such person uses or intends to use." The statute further states that an "online identifier" broadly "includes all of the following: electronic mail address, instant message screen name, user identification, user profile information, and chat or other Internet communication name or identity information." RSA 651-B:4-a. This expansive language does not define, for example, the phrases "user identification" or "chat or other Internet communication name or identity information." RSA 651-B:4-a also requires that registrants provide this newly required information "*before using the online identifier*." (emphasis added).

As with the other registration requirements, a violation of this disclosure law is a crime with significant penalties. A "knowing" failure to disclose this information is a class B felony and a "negligent" failure to disclose is a misdemeanor offense. *See* RSA 651-B:9, I, II; *see also* RSA 651:2, II(c), IV(a) (misdemeanors punishable by up to one year in jail and a fine up to $2,000); RSA 651:2, II(b), IV(a) (class B felonies punishable by up to 7 years in jail and a fine up to $4,000).[5]

RSA 651-B:4-a was passed by the legislature in June 2008 and was signed by the Governor on July 2, 2008. RSA 651-B:4-a was packaged in Senate Bill 495—a bill styled as "prohibiting Internet solicitation and exploitation of children." This bill had little, if any, dissent, and was passed by voice vote in both the Senate and House of Representatives. Though most of the legislative history focusses on other aspects of the bill, the New Hampshire Attorney General's Office did provide a brief comment on the bill's requirement that online identifiers be disclosed:

[5] If a Tier I registrant who is only on the registry for 10 years is convicted of a "knowing" failure to disclose, he or she automatically "shall be required to register for an additional 10 years." RSA 651-B:9(II).

"This is a new section. It is necessary because social networking sites currently do not have identity verification, and sexual predators can log on anonymously to meet and lure minors. It will ensure that if a registered sex offender or offender against children is caught using the internet and he or she has not registered his or her online identity, that person can be prosecuted." *See* 2008 Senate Bill 495, and Attorney's General's Comments on Online Identifier Provisions Selected from House of Representatives Legislative History (Declaration of Gilles Bissonnette ("Biss. Dec."), ¶ 4, *Exhibit C*); *see also* 2008 Senate Bill 495 Complete Legislative History (Biss. Dec., ¶¶ 31-32, *Exhibit DD* at LEG-S 111-12, and *Exhibit EE* at LEG-H 105-06).

The intent behind Senate Bill 495 was also to make registrants' online identifiers publicly available on the online sex offender registry. *See* 2008 Senate Bill 495, Section 323:7 (amending RSA 651-B:7(II)(b)(1) to require public disclosure of online identifiers) (Biss. Dec., ¶ 4, *Exhibit C*). However, this intent was ultimately not effectuated because a separate 2008 bill—House Bill 1640—was passed by the legislature at the same time that substantially revised Chapter 651-B pursuant to the federal Adam Walsh Act, but did so without making online identifiers available on the online public registry under RSA 651-B:7(III)(a). *See* 2008 House Bill 1640, Section 334:4 (rewriting, among other things, RSA 651-B:7) (Biss. Dec., ¶ 5, *Exhibit D*). The following year, the legislature corrected this error and passed Senate Bill 142, which, effective July 1, 2009, added RSA 651-B:7(III)(a)(9) to require that online identifiers be published on the online public registry. *See* 2009 Senate Bill 142, Section 306:6 (Biss. Dec., ¶ 6, *Exhibit E*). However, effective January 1, 2011, the legislature repealed this language requiring that online identifiers be made available to the public on the online registry. *See* 2010 House Bill 1642, Section 78:8 (repealing RSA 651-B:7(III)(a)(9)) (Biss. Dec., ¶ 7, *Exhibit F*). In support of this repeal, the Attorney General's Office testified before the legislature that the disclosure of online identifiers on the public registry

resulted in harassment. As the Office explained: "It has really been discovered that putting that information on the public list results in a lot of harassment of sexual offenders through contact through those e-mails and on-line identifiers." *Id.*

III. Recidivism Rates Vary Among Sex Offenders in Predictable Ways.

By way of background, extensive research demonstrates that recidivism rates are not uniform across all sex offenders. Rather, the risk of re-offending varies based on well-known factors and can be reliably predicted by widely-used risk assessment tools such as the Static-99/Static-99R. *See* Dec. of R. Andrew Harris ¶¶ 2, 14-18.[6] In addition, outside of the sex offender registry context, states like New Hampshire and California frequently use these tools to distinguish between sex offenders who pose a high risk to the public and those who do not. For example, New Hampshire has relied upon Static-99/Static-99R scoring and interpretation in asking courts to civilly confine "sexually violent predators" under RSA Chapter 135-E. Indeed, in several Chapter 135-E cases, New Hampshire Superior Courts have deemed admissible expert testimony concerning Static-99 and Static-99R to assess a respondent's likelihood of recidivism. *See New Hampshire v. Ploof*, No. 07-E-0238 (Superior Court, Hillsborough County, Northern District) (Abramson, J.), *available at* http://www.static99.org/pdfdocs/daubert-order4-28-09.pdf (Biss. Dec., ¶ 2, *Exhibit A*); *New Hampshire v. Hurley*, No. 07-E-0236 (Superior Court, Hillsborough County, Northern District) (Abramson, J.), *available at* http://www.static99.org/pdfdocs/hurley-orderondaubert_nh.pdf (Biss. Dec., ¶ 2, *Exhibit B*).

Research also contradicts the popular notion that sexual offenders remain at risk of re-

[6] In examining this Motion, this Court can consider the affidavits of R. Andrew Harris, David Finkelhor, and David Post, as well as the other extrinsic evidence accompanying this Motion, to the extent this evidence is not disputed. *See United States v. Levin*, 973 F.2d 463, 465-66 (6th Cir. 1992) (considering extrinsic evidence at motion to dismiss stage in criminal case to the extent the evidence is undisputed). In any event, even if any of this extrinsic evidence is disputed, the challenged law is unconstitutional on its face given its plain and overbroad terms and undisputed impact on innocent speech for all the reasons stated in this Motion.

offending throughout their lifespan. Most sex offenders do not re-offend. Harris Dec. ¶¶ 2, 19-25. The longer offenders remain offense-free in the community, the less likely they are to re-offend sexually. *See id*. ¶¶ 2, 26-40. On average, the likelihood of re-offending drops by 50% every five years that an offender remains in the community without a new arrest for a sex offense. *See id.* ¶ 27. Eventually, persons convicted of sex offenses are ***less likely*** to re-offend than a non-sexual offender is to commit an "out of the blue" sexual offence. *See id.* ¶¶ 2, 28. For example, offenders who are classified as "low risk" pose no more risk of recidivism than do individuals who have never been arrested for a sex-related offense but have been arrested for some other crimes. *See id.* ¶¶ 2, 30, 36. After 10 to 14 years in the community without committing a sex offense, medium-risk offenders pose no more risk of recidivism than individuals who have never been arrested for a sex-related offense but have been arrested for some other crimes. *See id.* ¶¶ 2, 30, 34. The same is true for high-risk offenders after 17 years without a new arrest for a sex-related offense. *See id.* ¶¶ 2, 35. Ex-offenders who remain free of any arrests following their release should present an even lower risk. *See id.* ¶ 28. Importantly, post-release factors such as cooperation with supervision and treatment can dramatically reduce recidivism, and monitoring these factors can be highly predictive. *See id*. ¶ 39.

Based on this research, criminal justice and recidivism experts recommend that "[r]ather than considering all sexual offenders as continuous, lifelong threats, society will be better served when legislation and policies consider the cost/benefit break point after which resources spent tracking and supervising low-risk sexual offenders are better re-directed toward the management of high-risk sexual offenders, crime prevention, and victim services." *See id.* ¶ 40.

IV. Sex Crimes are Overwhelmingly Committed by Family Members and Acquaintances, Not Strangers who Use the Internet to Meet Their Victims.

As further background, it should also be noted that in only very rare cases are sex crimes against children committed by strangers whom they have met on the Internet. In 2006, for example, arrests for *all* technology-facilitated sex crimes against minors (including those committed by acquaintances or family members) constituted only about 1% of all arrests for sex crimes against children. *See* Dec. of David Finkelhor ¶¶ 2, 13-14. In 2009, 46% of arrests for technology-facilitated child sexual exploitation were for child-pornography possession, with no additional sex crimes indicated, and thus did not involve an offender using the Internet to contact and victimize a child. *See id.* ¶¶ 2, 21.

Registrants constitute only a small percentage of those who commit technology-facilitated crimes against children. In 2006, for example, only 4% of persons arrested for technology-facilitated crimes against youth victims were registered sex offenders, and only 2% of those arrested for soliciting undercover investigators were registered sex offenders. *See id.* ¶ 19. And online targeting of children is decreasing, as are sex crimes against children in general. *See id.* ¶¶ 14-17. Studies show a 50% decline between 2000 and 2010 in sexual solicitation of youth on the Internet. *See id*. ¶ 14.

V. The Internet Is a Forum for Expression and Association.

At the same time, it can hardly be disputed that the role of the Internet as a forum for expression, communication, and association has continued to expand. There are millions, if not hundreds of millions, of web sites incorporating some form of communicative functionality, *e.g.*, the ability to create a profile and post some form of content. Dec. of David G. Post ¶ 23. While the total number of different websites continues to increase, so does the user base and usage of the most popular sites and services. For example, Facebook alone now has more than 1.44 billion

users worldwide, and Twitter users generate over 500,000,000 "tweets" per day. *Id.* ¶ 11.

Use of the Internet for a wide range of activities is also increasing. Most Americans use the Internet, and the average American spends more than an hour per day online. *Id.* ¶ 10. Roughly 76 percent of online adults obtain at least some news online. *Id.* ¶ 15. Approximately 39 percent of all Americans have engaged in some form of civic or political activity through social media beyond simply reading about political issues. *See id.* ¶ 16. And millions of Americans use the Internet to carry out their current employment, seek new employment, or further their education. *See id.* ¶¶ 18-19.

As a result, Americans visit a large number of different Internet sites, many of which require or permit the creation of user names, screen names, or similar identifiers, and engage in various expressive activities on these sites. The average Internet user visits well over 100 distinct web sites in a typical month, and prolific Internet users may visit far more. *See id.* ¶ 12. Using these sites and accounts, Internet users can and do post feedback on both recently-purchased items and their sellers, discuss news events, and advertise for and otherwise conduct their businesses. *See id.* ¶¶ 13, 15, 17, 23.

Defendant and other registered sex offenders wish to use the Internet like other Americans: to conduct business, communicate with friends and associates, engage in self-expression, comment on news articles, and participate in groups with political, religious, or recreational purposes.

VI. [redacted]

[redacted]

[7] [redacted]

[8] [redacted]

[redacted]

9 [redacted]

[redacted]

[redacted]

[10] [redacted]

[redacted]

LEGAL STANDARD

To sustain its burden in this case, the State is required to prove beyond a reasonable doubt that Defendant has violated RSA 651-B:4-a. Even assuming all facts in the State's indictments as true, the State cannot meet its burden because RSA 651-B:4-a, on its face, is unconstitutional. *See e.g., State v. Vaillancourt*, 122 N.H. 1153 (1982) ("an indictment must allege some criminal activity"; indictment is insufficient where "even if the facts alleged in it were true, they would not have satisfied the elements necessary"); *see also State v. Hollenbeck*, 164 N.H. 154, 159 (2012) (deciding facial challenge at motion to dismiss stage). Accordingly, all charges for violating RSA 651-B:4-a must be dismissed.

ARGUMENT

I. RSA 651-B:4-a Is Facially Unconstitutional.

At least five federal courts have invalidated or enjoined the enforcement of laws that require sex offenders to provide the government with identifying information about their online speech. *See Doe v. Harris*, 772 F.3d 563 (9th Cir. 2014); *Doe v. Nebraska*, 898 F. Supp. 2d 1086 (D. Neb. 2012); *White v. Baker*, 696 F. Supp. 2d 1289 (N.D. Ga. 2010); *see also Doe v. Shurtleff*,

No. 1:08-CV-64 TC, 2008 U.S. Dist. LEXIS 73787 (D. Utah Sept. 25, 2008) ("*Shurtleff I*"), *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); *Doe v. Snyder*, No. 12-11194, 2015 U.S. Dist. LEXIS 41681, at *63-79 (E.D. Mich. Mar. 31, 2015). Like those laws, RSA 651-B:4-a is facially unconstitutional because it criminalizes speech that the First Amendment and Part I, Article 22 of the New Hampshire Constitution protect and is not narrowly tailored to the government's interests of preventing and uncovering sex offenses.

A statute is unconstitutionally "'overbroad' in violation of the First Amendment if in its reach it prohibits constitutionally protected conduct." *Grayned v. City of Rockford*, 408 U.S. 104, 114 (1972). "The crucial question, then, is whether the ordinance sweeps within its prohibitions what may not be punished under the First and Fourteenth Amendments." *Id.* at 114-15; *see also Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 237 (2002) ("The overbreadth doctrine prohibits the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process."); *United States v. Stevens*, 559 U.S. 460, 473 (2010) (same); *Doyle v. Comm'r, N.H. Dep't. of Resources & Economic Dev*., 163 N.H. 215, 221 (2012) (under Part I, Article 22 of the New Hampshire Constitution, a law is facially overbroad where "a substantial number of its applications are unconstitutional, judged in relation to the [regulation's] plainly legitimate sweep"). An individual has standing to challenge a law as overbroad even if a more narrowly tailored law could properly be applied to him. *Parker v. Levy*, 417 U.S. 733, 759 (1974). Moreover, the Court's inquiry is not limited to the application of the challenged provisions to the particular litigant before it, as "[l]itigants … are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from

constitutionally protected speech or expression." *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). As the New Hampshire Supreme Court has also recently explained:

> In the First Amendment context, courts are especially concerned about overbroad and vague laws that may have a chilling effect on speech. Courts are suspicious of broad prophylactic rules in the area of free expression, and therefore precision of regulation must be the touchstone in an area so closely touching our most precious freedoms.

Montenegro v. N.H. DMV, 166 N.H. 215, 220 (2014) (quoting *Act Now to Stop War v. District of Columbia*, 905 F. Supp. 2d 317, 329-30 (D.D.C. 2012)).

A. RSA 651-B:4-a is unconstitutionally overbroad because its burdensome registration requirements are not narrowly tailored and chill protected innocent speech, whether anonymous or not.

Because RSA 651-B:4-a imposes burdensome registration requirements on all sorts of innocent online speech (whether anonymous or not), the law is unconstitutional.

1. RSA 651-B:4-a's registration requirements trigger strict scrutiny under the First Amendment and Part I, Article 22 of the New Hampshire Constitution.

The First Amendment and Part I, Article 22 of the New Hampshire Constitution take heed not only of flat prohibitions on speech, but also "statutes attempting to restrict or burden the exercise of [free speech] rights." *See Broadrick*, 413 U.S. at 611–12; *see, e.g.*, *Simon and Schuster, Inc. v N.Y. State Crime Victims Bd.*, 502 U.S. 105, 118 & 122 n.* (1991) (invalidating law that "establishe[d] financial disincentive" to certain speech by former offenders); *ACLU v. Reno*, 31 F. Supp. 2d 473, 493-95 (E.D. Pa. 1997), *aff'd* 542 U.S. 656 (2004). Because free speech rights are fragile, "the amount of burden on speech needed to trigger First Amendment scrutiny as a threshold matter is minimal." *American Legion Post 7 of Durham, N.C. v. City of Durham*, 239 F.3d 601, 607 (4th Cir. 2001).

RSA 651-B:4-a's reporting requirements are substantial and far exceed this minimal threshold for triggering scrutiny under the First Amendment and Part I, Article 22 of the New

Hampshire Constitution. The online identifier reporting requirement requires each registrant who is "no longer on the 'continuum' of state-imposed punishments," *see Harris*, 772 F.3d at 572, to document and report not only email addresses and social media accounts but also any "user identification," "user profile information," and "Internet communication name or identity information." This includes (i) online identifiers associated with comments on news websites and civil rights discussion fora, (ii) any identifier associated with feedback submitted to a review site like Yelp, (iii) affiliations with online government services, and (iv) even a personal blog or web page. *See* Post Dec. ¶¶ 23, 37-38. A registrant facing the possibility of arrest and serious criminal penalties if he fails to document and report each of these online activities may reconsider exercising free speech rights at all. *See Nebraska*, 898 F. Supp. 2d at 1121 (noting that the government reporting requirement "that puts a stake through the heart of the First Amendment's protection of anonymity … surely deters faint-hearted offenders from expressing themselves on matters of public concern"); *Harris*, 772 F.3d at 573 ("[T]he CASE Act directly and exclusively burdens speech, and a substantial amount of that speech is clearly protected under the First Amendment."). This is more than enough to trigger constitutional scrutiny.

And, here, the only appropriate form of review is strict scrutiny because RSA 651-B:4-a singles out the speech of Chapter 651-B registrants for differential treatment. There can be little doubt that registered sex offenders who have completed all aspects of their sentence are a disfavored group viewed with antipathy by both New Hampshire and American society. The Supreme Court has made it clear that the First Amendment generally prohibits laws that "impose restrictions on certain disfavored speakers." *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876, 888, 899 (2010); *see also Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 2663 (2011) (applying strict scrutiny to law that "disfavors specific speakers"). Such laws are akin to those that

discriminate by content, and are therefore subject to strict scrutiny, under which a law regulating speech is unconstitutional unless the government can "prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Citizens United*, 130 S. Ct. at 898 (citation omitted). In addition, in applying strict scrutiny review, the law must "choose[] the least restrictive means to further the articulated interest." *Sable Comm'ns v. FCC*, 492 U.S. 115, 126 (1989).

2. RSA 651-B:4-a is not narrowly tailored and therefore fails under either strict scrutiny or intermediate scrutiny.

But even content-neutral restrictions on speech must meet intermediate scrutiny, meaning that they must be "narrowly tailored to serve a significant governmental interest" and must "leave open ample alternative channels for communication of the information." *See McCullen v. Coakley*, 134 S. Ct. 2518, 2529 (2014) (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)); *see also Doyle*, 163 N.H. at 223 (a content-neutral law "must be narrowly tailored to serve a significant government interest"). To satisfy the narrow-tailoring requirement, the State bears the burden of showing that the remedy it has adopted does not "burden substantially more speech than is necessary to further the government's legitimate interests." *Ward*, 491 U.S. at 799-99.[11]

While RSA 651-B:4-a must satisfy strict scrutiny, it cannot even satisfy intermediate scrutiny because it is not remotely "narrowly tailored to further" the government's goals. *Grayned*, 408 U.S. at 119. Indeed, in at least four (4) independent ways, the law goes far beyond what is necessary to further the government's interest in preventing registrants from "log[ging] on anonymously [to websites] to meet and lure minors." *See* 2008 Senate Bill 495, and Attorney's

[11] Although this narrow-tailoring requirement is most often applied to speech that occurs in a public forum, as *Simon and Schuster* illustrates, it also applies to laws that generally restrict speech, including online speech. *See Golan v. Gonzales*, 501 F.3d 1179, 1196 (10th Cir. 2007); *see also Reno*, 521 U.S. at 868-870.

General's Comments on Online Identifier Provisions before House of Representatives (Biss. Dec., ¶ 4, *Exhibit C*); *see also* 2008 Senate Bill 495 Complete Legislative History (Biss. Dec., ¶¶ 31-32, *Exhibit DD* at LEG-S 111-12, and *Exhibit EE* at LEG-H 105-06).

First, the burdens imposed under the challenged law far exceed the government's stated interests because a registrant must disclose an online identifier to the police ***before*** he or she can use the online identifier to engage in online speech. Put another way, disclosure is compelled at the very moment the registrant wishes to be heard, which clearly creates a chilling effect on innocent Internet activity. Multiple courts have struck down or enjoined less extreme statutes that required the disclosure of online identifiers 24 and 72 hours ***after*** the online identifier was used. *See Harris*, 772 F.3d at 581 (law requiring disclosure of online identifier "within 24 hours of" use was unconstitutional because it "undoubtedly chills First Amendment [a]ctivity"); *White*, 696 F. Supp. 2d at 1310 (striking down Georgia statute requiring registrants to provide updated online identifier information within 72 hours). As the *Harris* Court explained in rejecting the law because of its 24-hour reporting requirement:

> The requirement applies to all registered sex offenders, regardless of their offense, their history of recidivism (or lack thereof), or any other relevant circumstance. And the requirement applies to all websites and all forms of communication, regardless of whether the website or form of communication is a likely or even a potential forum for engaging in illegal activity. (If for example a sex offender establishes a username on a news outlet's website for purposes of posting comments to news articles, it is hard to imagine how speedily reporting that identifier will serve the government's interests.) In short, we have a hard time finding even an attempt at narrow tailoring in this section of the Act.

Harris, 772 F.3d at 582. RSA 651-B:4-a's burdens far exceed the infringements that existed in *Harris* and *White* because it makes government disclosure a prerequisite to engaging in online speech, thus acting as a *de facto* prior restraint. And, to make matters worse, many registrants are also required to update any online identifiers "in person" at the offices of law enforcement agencies during semi-annual or quarterly reports. *See* 651-B:4(I)(a-b) (Tier III offenders must

report in person quarterly, and Tier I and II offenders must report in person semi-annually); *see also Doe v. Snyder*, No. 12-11194, 2015 U.S. Dist. LEXIS 41681, at *63-79 (E.D. Mich. Mar. 31, 2015) (noting that the "requirement to report 'in person'" renders Michigan's Internet identifier law not narrowly tailored and, therefore, unconstitutional).

Second, RSA 651-B:4-a criminalizes far too much anonymous, constitutionally-protected speech by too many speakers and allows the information to be used for too many purposes. Where, as here, the State seeks to prevent sex offenses, the regulation must be targeted at "the means by which sex offenders may communicate with [their victims] and by which [their victims] may respond to offenders' sexual advances," which is "usually, but not exclusively, [in] interactive, and often real time" Internet communications that implicate children. *White*, 696 F. Supp. 2d at 1311. But rather than requiring disclosure of online identifiers only when used in this tailored context, RSA 651-B:4-a requires registrants to disclose to the police *all* online identifiers, including identifiers used innocently (i) to comment (whether anonymous or not) on articles published on websites like that of the *New York Times*, the *New Hampshire Union Leader*, or the ACLU, (ii) to participate in discussion groups pertaining to the civil rights of registrants, (iii) to sign up for health insurance online at www.healthcare.gov under the Affordable Care Act, (iv) to manage one's medical care through, for example, the Dartmouth-Hitchcock health care system, or (v) to provide political feedback to the President of the United States at https://petitions.whitehouse.gov or https://www.whitehouse.gov/contact/submit-questions-and-comments. *See* Post Dec. ¶¶ 23, 37, 40; *see also* Dartmouth-Hitchcock Health Care System's "Manage Your Health Care with myD-H" Brochure (Biss. Dec., ¶ 35, *Exhibit HH*) (noting that online account allows a patient to "[c]ommunicate with your health care team"); https://www.mydh.org/portal/faq.aspx. [redacted]

[redacted] All of these websites "are by their nature open to the public and pose no threat to children. That sex offenders—perhaps the most reviled group of people in our community—may 'blog' threatens no child. But the government reporting requirement (which puts a stake through the heart of the First Amendment's protection of anonymity) surely deters faint-hearted offenders from expressing themselves on matters of public concern." *Nebraska*, 898 F. Supp. 2d at 1121; *see also White,* 696 F. Supp. 2d at 1310 (predatory Internet communications "generally do not occur in communications that are posted publicly on sites dedicated to discussion of public, political, and social issues"); *Harris*, 772 F.3d at 582 (enjoining "Internet identifier" requirement where it makes no distinction as to whether a website is a "likely or even a potential forum for engaging in illegal activity"). Moreover, to the extent RSA 651-B:4-a requires disclosure of all websites where a registrant simply creates a "user profile"—regardless of whether the website allows users to communicate with third parties—this would include millions of websites, including entertainment, banking, shopping, and government websites.[12] *See* Post Dec. ¶ 23; *see United States v. Perazza-Mercado*, 553 F.3d 65, 72 (1st Cir. 2009) ("online banking or managing medical records are potentially important activities that one might not wish to conduct in public because of a legitimate interest in keeping the information private").

In light of these examples of innocent speech that RSA 651-B:4-a bans without

[12] This is not a hypothetical interpretation. While no court has decided whether RSA 651-B:4-a violates the free speech protections of the First Amendment or Part I, Article 22 of the New Hampshire Constitution, the New Hampshire Supreme Court in *State v. White*, 164 N.H. 418 (2012) did interpret the term "user profile" to include websites that "require[] the creation of a personal 'profile' or 'biographical account' information." *Id.* at 421. The Court later added that a "user profile" "refers to a set of personal facts that a person provides to a website in order to create an account." *Id.* at 423. The Court further explained, "[t]o the extent that our interpretation of the phrase 'user profile information' may require sex offenders to report a wide range of online activities, it does so as a reflection of legislative intent expressed in the statute's plain terms." *Id.* at 422. The statute's text and the New Hampshire Supreme Court's expansive interpretation of its plain terms only further demonstrate the law's substantial overbreadth under the federal and state constitutions.

government disclosure, its overbreadth—and thus facial unconstitutionality—is apparent. As the U.S. Supreme Court has explained, "[t]he Government may not suppress lawful speech as the means to suppress unlawful speech. Protected speech does not become unprotected merely because it resembles the latter. The Constitution requires the reverse." *Ashcroft*, 535 U.S. at 255 (Child Pornography Prevention Act of 1996's ban on virtual child pornography was unconstitutionally overbroad because it proscribed speech which was neither child pornography nor obscene); *see also State v. Brobst*, 151 N.H. 420, 422 (2004) (section of harassment statute facially overbroad because it "is not, however, limited in scope to … unreasonable, unwelcome and unwarranted activities or intrusions" but rather "applies to any call made to anyone, anywhere, at any time, whether or not conversation ensues, if the call is placed merely with the intent to annoy or alarm another, which means that the act constituting the offense is complete when the call is made, regardless of the character of conduct that ensues"; noting 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"); *Montenegro v. N.H. DMV*, 166 N.H. 215, 224 (2014) (striking down DMV vanity license plate regulation on its face as vague because it encouraged "arbitrary and discriminatory enforcement," and declining to "add or delete text to the regulation" to save the regulation); *Doyle*, 163 N.H. at 221 (holding that special-use permit regulation was facially unconstitutional and overbroad).[13] This is precisely why the overbreadth doctrine exists—to "prohibit[] the Government from banning unprotected speech if a substantial amount of protected speech is prohibited or chilled in the process." *Ashcroft*, 535 U.S. at 255.

RSA 651-B:4-a's application to <u>*all*</u> registrants—and only to registrants—is also both over-

[13] These requirements apply to laws such as this one that seek to protect children from criminal acts. *See Free Speech Coal.*, 535 U.S. at 252-53, 255 (where "the Government wants to keep speech from children not to protect them from its content but to protect them from those who would commit other crimes," it cannot employ a "restriction [that] goes well beyond that interest by restricting the speech available to law-abiding adults").

and under-inclusive. The law is woefully overinclusive because it applies to *all* registrants, regardless of the age of the conviction, whether they are at high or low risk of re-offending, and whether the registration-triggering conviction had anything to do with the Internet. *See Harris*, 772 F.3d at 582 (enjoining "Internet identifier" statute where "[t]he requirement applies to all registered sex offenders, regardless of their offense, their history of recidivism (or lack thereof), or any other relevant circumstance"); *see also United States v. Ramos*, 763 F.3d 45, 62 (1st Cir. 2014) ("[W]here a defendant's offense did not involve the use of the internet or a computer, and he did not have a history of impermissible internet or computer use, courts have vacated broad internet and computer bans regardless of probation's leeway in being able to grant exceptions."); *United States v. Perazza-Mercado*, 553 F.3d 65, 72 (1st Cir. 2009). Put another way, the law burdens speech by registrants, many of whom have no more chance of committing a future sex crime than a typical member of the population. *See* Harris Dec. ¶¶ 30, 34-36. Most sexual offenders do not re-offend. And the longer offenders remain offense-free in the community, the less likely they are to re-offend sexually. *See id.* ¶¶ 2, 14-25. Eventually, they are *less likely* to be arrested for a sex-related offense than individuals who have never been arrested for a sex-related offense. *See id*. ¶¶ 26-40; *see also United States v. T.M.*, 330 F.3d 1235, 1240 (9th Cir. 2003) ("The fact that T.M. has lived the last twenty years without committing a sex offense suggests that he no longer needs to be deterred or shielded from the public."). Using national data as a model, the vast majority of registrants were convicted of crimes that did not involve the Internet (more than 99% of national arrestees in 2006) but did involve victims who already knew the offender. *See* Finkelhor Dec. ¶¶ 13-14. Thus, RSA 651-B:4-a targets vastly more individuals than it needs to, as it "is not narrowly tailored to target those offenders who pose a factually based risk to children through the use or threatened use of the [specified] sites or services." *Nebraska*, 898 F.

Supp. 2d at 1111. This reality only highlights RSA 651-B:4-a's punitive effect when it comes to registrants who demonstrate no danger to society and who simply wish to engage in innocent speech on the Internet.[14]

Notably, RSA 651-B:4-a could achieve its goals if it applied only to those who have been convicted of offenses involving the Internet or who are at high risk of re-offending, or even by allowing persons with older or minor convictions or those who could otherwise demonstrate that they do not pose a risk and therefore should be excluded from this requirement. But the State has not even attempted to use less intrusive means as is constitutionally required. *See McCullen*, 134 S. Ct. at 2524 (state must show "that it seriously undertook to address these various problems with the less intrusive tools readily available to it"). For example, in 1996, the New Hampshire legislature repealed RSA 632-A:11-19 and replaced it with RSA Chapter 651-B containing certain due process safeguards with respect to the sex offender Act's requirements. *See* 1996 Version of RSA 651-B (Biss. Dec., ¶ 8, *Exhibit G*). Under these amendments, the legislature—while authorizing a law enforcement agency for the first time to notify organizations such as schools, youth groups, day care centers, summer camps, and libraries that certain sex offenders intended to reside in the neighborhood, *see id.*, RSA 651-B:7(II)(a)—also provided for such an offender to petition the Merrimack County Superior Court for a "qualifying order" exempting him from the restricted notification provision. *See id.*, RSA 651-B:7(II-III). Chapter 651-B then set out several criteria for the court to consider in deciding whether to grant the qualifying order including

[14] *See supra* note 4. In *Doe v. State*, 111 A.3d 1077 (N.H. 2015), the New Hampshire Supreme Court held that Chapter 651-B's lifetime registration requirements were punitive, and therefore unconstitutional under Part I, Article 23 of the New Hampshire Constitution's ban of retrospective laws, as applied to a petitioner who was convicted before the registry went into effect. The Court explained: "Although there is a regulatory purpose underlying this statute, we find that the act as currently constituted is excessive when compared with this purpose, and when compared with past versions of the act. Though many of the amendments serve a clear purpose to better the registry scheme or to make it more useful to the public, other aspects of the act serve no readily-apparent non-punitive purpose …. in fact there is no meaningful risk to the public, then the imposition of such requirements becomes wholly punitive." *Id.* at 1100.

whether the petitioner's physical condition minimized the risk of reoffending. However, when Chapter 651-B was next amended in 1998, the legislature repealed and did not replace those provisions that provided sexual offenders with the right to seek a qualified order. Despite the 1998 amendment, risk assessment tools like Static-99R—which have been developed based on decades of data and extensive research—are now widely available in the criminal justice field. *See* Harris Dec. ¶ 18. Indeed, New Hampshire has relied upon Static-99/Static-99R scoring and interpretation in asking courts to civilly confine "sexually violent predators" under RSA Chapter 135-E. The existence of feasible, readily identifiable, and less-restrictive means of addressing the State's concerns confirms that RSA 651-B:4-a is not narrowly tailored.[15]

At the same time, RSA 651-B:4-a is underinclusive because it only applies to registrants. *See Showtime Ent't, LLC v. Town of Mendon*, 769 F.3d 61, 73 (1st Cir. 2014) ("[W]here such secondary effects flow in equal measure from [alternative sources], which nonetheless are left untouched by the regulation in question, it stands to reason that such underinclusiveness raises questions as to whether the proffered interest is truly forwarded by the regulation, or is in fact substantial enough to warrant such regulation."). The overwhelming majority of technology-facilitated sex crimes are not committed by registered sex offenders. In 2006, only 4% of persons arrested for technology-facilitated sex crimes against youth were registered sex offenders, and only 2% of those arrested for soliciting undercover investigators were registered sex offenders.

[15] The procedures currently provided by the State for the civil commitment of sexually violent predators under RSA Chapter 135-E also demonstrate the existence of less burdensome alternatives. Under Chapter 135-E, the agency with custody of an inmate whom the government believes is a sexually violent predator is required to give notice of his impending release to the county attorney or attorney general. If there is an articulable basis to believe that the inmate is likely to engage in acts of sexual violence, the prosecutor may request an assessment by a multidisciplinary team to determine whether the inmate meets the definition of sexually violent predator. The inmate is entitled to counsel. If the multidisciplinary team finds that the inmate meets the definition of sexually violent predator, the prosecutor may file a petition with the superior court alleging that the inmate is a sexually violent predator and stating facts sufficient to support that allegation. The court must then determine whether there is probable cause to believe that the inmate is a sexually violent predator. If the court finds probable cause then there is a hearing on the merits to determine whether the inmate is a sexually violent predator. The inmate has the right to a jury trial.

See Finkelhor Dec. ¶¶ 2, 19. Here, "the fact that [the statute] is both overinclusive and underinclusive would lead to the conclusion that it is not narrowly tailored to serve the governmental interest at stake." *Ohio Citizen Action v. City of Mentor-On-The-Lake*, 272 F. Supp. 2d 671, 684 n.2 (N.D. Ohio 2003).[16]

RSA 651-B:4-a also does not meaningfully restrict potential uses by law enforcement or public disclosure of online identifiers—a reality which further compounds the law's chilling effect. Release of this information is governed by existing law. *See also* Chapter Saf-C 5500, Sex Offender Registration Rules (Biss. Dec., ¶ 9, *Exhibit H*). RSA 651-B:7(I) states that "the records established and information collected pursuant to the provisions of this chapter"—which includes online identifiers collected under RSA 651-B:4-a—"shall not be considered 'public records' subject to inspection under RSA 91-A:4." However, the statute goes on to make clear that "nothing in this chapter shall be construed to limit any law enforcement agency from making any use or disclosure of any such information as may be necessary for the performance of *a valid law enforcement function*." RSA 651-B:7(I) (emphasis added). Thus, any police officer is expressly permitted by statute to disclose a registrant's online identifier to another officer—or perhaps even to a social media company or member of the public—if that officer, in his or her unfettered discretion, feels that the disclosure would "be necessary for the performance of a valid law enforcement function."[17] It can hardly be said that the phrase "valid law enforcement function" cabins the discretion of law enforcement agencies. *See Montenegro*, 166 N.H. at 220 (striking

[16] RSA 651-B:4-a is also underinclusive because it applies only to *Internet* speech, and thus excludes all analogous communications that take place over cellular networks or other communications channels with the same characteristics. *See* Post Dec. ¶ 29.

[17] Policies and procedures obtained by the American Civil Liberties Union of New Hampshire in response to Right-to-Know records requests confirm the fact that law enforcement agencies have unbridled discretion in disclosing online identifiers. For example, the policy of the Derry Police Department simply states that "[t]he release of sexual offender information shall be in accordance with RSA 651-B:7" and that "[t]he Chief of Police or his designee shall be consulted in all cases prior to 'affirmative public notification' of a registered offender in accordance with any section of RSA 651-B." *See* Derry Policy (Biss. Dec., ¶ 24, *Exhibit W*). Nashua Police Department's policy simply restates the terms of RSA 651-B:7. *See* Nashua Policy (Biss. Dec., ¶ 27, *Exhibit Z*).

down DMV vanity license plate regulation as vague because it allowed for unfettered discretion in enforcement). As one court explained in striking down a similar Georgia online identifier statute where online identifiers could be disclosed to law enforcement agencies for "law enforcement purposes":

> "Law enforcement purposes" can have many meanings. To some, it is the investigation of suspected or identified criminal conduct. To others, "law enforcement purposes" encompasses the development of investigative leads. To still others, it is the prevention of crime. It may mean any purpose determined appropriate by law enforcement personnel to prevent criminal conduct. The free speech implication is obvious. A law enforcement agency could deem it necessary to begin monitoring internet sites, blogs, or chat rooms it believes may or could be used by predators to induce minors into sexual encounters because the monitoring may provide investigative leads. An agency could decide to create a list of registrant user names for use in monitoring targeted internet sites, blogs, or chat rooms to review what registrants are saying in their communications on those internet locations. Using Plaintiff's Internet Identifiers in this way would disclose protected speech he chose to engage in anonymously and thus would chill his right to engage in protected anonymous free speech.

White, 696 F. Supp. 2d at 1310-11 (also noting as problematic the fact that the law "allows the Internet Identifiers to be released to the community by law enforcement 'to protect the public'"); *see also Harris*, 772 F.3d at 581 ("[S]ex offenders' fear of disclosure in and of itself chills their speech. If their identity is exposed, their speech, even on topics of public importance, could subject them to harassment, retaliation, and intimidation."); *Nebraska*, 898 F. Supp. 2d at 1111 ("[T]he requirement that offenders report to the police regarding the material they post to Internet sites they operate will surely deter offenders in business from maintaining such sites."). Troublingly, under this language, law enforcement can use online identifiers to investigate actions that having nothing to do with sex crimes or the Internet, or even to pierce the veil of anonymity before an alleged crime has ever been committed.[18] Moreover, there are no limits on the ability of

[18] The lack of sufficient limits on the governmental use of the information or public disclosure distinguishes RSA 651-B:4-a from the Utah law that was upheld in *Shurtleff II*, after it was amended to permit use of the information only "to assist in investigating kidnapping and sex-related crimes." *See Shurtleff II*, 2009 U.S. Dist. LEXIS 73955 (D. Utah Aug 20, 2009); *see also Coppolino v. Comm'r of the Pa. State Police*, 102 A.3d 1254, 1283 (Pa. Commw. Ct. 2014)

law enforcement to disclose online identifiers to the public. For example, officers' release of registrants' online identifiers to social networking sites in the interest of "public safety"—which reasonably may be viewed as a "valid law enforcement function"—could result in registrants being cut off not only from these services but from the increasingly wide range of activities that require a Facebook or similar account, including participation in online discussions of news articles, political and social issues, and more. *See* Post Dec. ¶ 41.

Third, the vagueness of RSA 651-B:4-a's definitions of what registrants must disclose—particularly its examples of "user identification" and "chat or other Internet communication name or identity information"—as coupled with the serious punishment for failure to provide the correct information, renders it "problematic for purposes of the First Amendment" narrow tailoring test, regardless of whether it is so vague as to violate due process. *Reno v. ACLU*, 521 U.S. 844, 870-72 (1997); *see also Montenegro*, 166 N.H. at 220. As a practical matter, vague criminal laws regulating speech are nearly always overinclusive because the "severity of criminal sanctions may well cause speakers to remain silent rather than" risk prosecution for "arguably unlawful" activity. *Reno*, 521 U.S. at 872; *see also Harris*, 772 F.3d at 578-79 (striking down Internet identifier law because it "does not make clear what sex offenders are required to report"). As discussed in more detail below, the law's examples of "online identifier" are incomprehensible. *See infra* Part I.C;

(not engaging in tailoring analysis as required under First Amendment and concluding, in error, that "the determining factor is whether a given statute permits or makes likely disclosure of a registrant's Internet identifiers to the public"). But even with these limits, RSA 651-B:4-a would be not tailored, and thus is unconstitutional, because it (i) requires disclosure of online identifiers as a precondition to engaging in speech using the online identifier, (ii) still requires speakers, including those who did not commit an Internet offense or who pose no danger, to disclose their identities to the State, (iii) is hopelessly overbroad in that it requires disclosure of online identifiers that bear no nexus to the State's purported public safety interests, and (iv) is so vague that it will cause offenders to overreport their activity and to underuse the Internet given the risk of criminal prosecution. Indeed, unlike the challenged law, the Utah law did not require disclosure as a precondition to expression. *See Shurtleff II*, 628 F.3d 1217, 1225 (10th Cir. 2010) (noting that "[s]peech is chilled when an individual whose speech relies on anonymity is forced to reveal his identity as a pre-condition to expression," and explaining that the law there was constitutional because "disclosure would generally occur, if at all, at some time period following Mr. Doe's speech and not at the moment he wished to be heard") (quotations omitted); *see also Coppolino*, 102 A.3d at 1277 (upholding online identifier statute where identifiers are to be disclosed three days after use).

see also Post Dec. ¶¶ 23-34, 37-39. Given this ambiguity, a registrant who would like to use an "online identifier" to engage in Internet speech in a way that only "arguably" falls within the law's purview would be reckless indeed to risk arrest and imprisonment by doing so without first disclosing the online identifier. Thus, the likely result is that a registrant will either overreport his activity (either voluntarily or per the instruction of police) or self-suppress his Internet usage in order to avoid the difficult questions in understanding what precisely he must disclose. Even construing these examples as narrowly as possible, the law's requirements are not narrowly tailored; that they are potentially much broader in scope due its vague definitions only magnifies this constitutional infirmity. *See Snyder*, 2015 U.S. Dist. LEXIS 41681, at *63-79 (ambiguities in reporting requirements rendered Internet identifier requirement "not narrowly tailored and, therefore, unconstitutional").

To see how the ambiguities in RSA 651-B:4-a impact the daily lives of registrants, this Court need look no further than the Defendant and the State's overaggressive prosecution in this case. [redacted] These charges highlight the State's overzealous strategy of charging even "honest mistakes" as "knowing" violations under RSA 651-B:4-a. [redacted] Unfortunately, as this prosecution makes clear, the State will engage in law enforcement practices using the law's ambiguities to bludgeon registrants

who make honest mistakes while trying to comply with the law. This will only further chill registrants' usage of the Internet. *See Doe*, 772 F.3d at 579 (rejecting State's "assurances that it will not prosecute 'honest mistakes'" because the Court "cannot assume that, in its subsequent enforcement, ambiguities will be resolved in favor of adequate protection of First Amendment rights").

Finally, the State cannot show how RSA 651-B:4-a has achieved—and will achieve in the future—its objectives in preventing or detecting crimes. In January 2015, the American Civil Liberties Union of New Hampshire submitted Right-to-Know records requests to all ten County Attorney offices in New Hampshire, the police departments of the seven largest cities in New Hampshire (Concord, Derry, Dover, Manchester, Nashua, Rochester, and Salem), the New Hampshire Division of the State Police, and the New Hampshire Attorney General's Office concerning the enforcement of RSA 651-B:4-a and the use by law enforcement of online identifiers disclosed by registrants. *See* Nineteen Right-to-Know Requests and Responses (Biss. Dec., ¶¶ 11-29, *Exhibits J-BB*); *see also* Summary of Nineteen Right-to-Know Responses (Biss. Dec., ¶ 30, *Exhibit CC*). In response to these nineteen (19) records requests, each of these law enforcement agencies in New Hampshire could not identify a single case in which an online identifier disclosed by a sex offender pursuant to RSA 651-B:4-a was used to uncover subsequent criminal activity that resulted in the filing of criminal charges against that sex offender. *Id.* But even if the State could produce isolated cases where online identifiers have been used to prevent a crime, the challenged law is still facially overbroad because it creates a chilling effect by sweeping within its scope innocent online speech. *See Broadrick*, 413 U.S. at 612 ("The possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted ….''). In short, while it appears from over 6 years of

data that the online identifiers disclosed under RSA 651-B:4-a have not resulted in the detection of a single crime, more than 32 individuals have been charged for failing to disclose online identifiers pursuant to RSA 651-B:4-a from 2009 to 2014, including the Defendant.

RSA 651-B:4-a is facially unconstitutional because it imposes burdensome reporting requirements on online speech without being tailored to address the State's asserted interests in preventing sex offenses. Even if its vague terms are construed as narrowly as possible, it is not limited to the speech or speakers that give rise to the purported dangers the statute seeks to address, and thus fails to prohibit law enforcement from using the information for purposes unrelated to the prevention or investigation of sex offenses.

B. RSA 651-B:4-a is unconstitutionally overbroad because it effectively criminalizes all online anonymous communications engaged in by registrants and is not narrowly tailored.

Because RSA 651-B:4-a requires registrants to disclose ***all*** their online identifiers to law enforcement, the law also effectively bans ***all*** registrants from engaging in online anonymous communications. For example, RSA 651-B:4-a prohibits registrants from using a pseudonymous screen name to participate in online speech without disclosing their real identity to the government.

"Under our constitution, anonymous [speech] … is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent." *McIntyre v. Ohio Elections Comm.*, 514 U.S. 334, 357 (1995) (law prohibiting anonymous leafletting unconstitutional); *see also Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 166 (2002); *Talley v. California*, 362 U.S. 60, 64-65 (1960). And it cannot be disputed that the right to engage in anonymous speech extends to the Internet. "As with other forms of expression, the ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals

to express themselves freely without fear of economic or official retaliation or concern about social ostracism." *In re Anonymous Online Speakers*, 661 F.3d 1168, 1173 (9th Cir. 2011) (internal quotes omitted).

Given RSA 651-B:4-a's outright ban on registrants' anonymous online speech, it must satisfy strict scrutiny because it targets a disfavored group. *See supra* Part I.A.1. However, RSA 651-B:4-a cannot even satisfy intermediate scrutiny because the law is not narrowly tailored for the same reasons stated above. *See supra* Part I.A.2; *see also McCullen*, 134 S. Ct. at 2524. The fact that the law requires disclosure as a prerequisite to using an online identifier to engage in speech on the Internet creates a massive chilling effect on anonymous speech. As *Harris* and *White* make clear, the loss of anonymity deters speech regardless of when the coerced identification of the speaker occurs. *Harris*, 772 F.3d at 579 (striking down Internet identifier law because "the Act burdens registered sex offenders' ability to engage in anonymous online speech"); *White*, 696 F. Supp. 2d at 1308-12 (noting that Internet identifier disclosure requirement created a chilling effect on an offender's right to anonymous free speech). The online identifier registration requirement—which applies even to participation in an online political forum—is also dramatically overinclusive because it covers a great deal of innocent anonymous speech that could not possibly be used to facilitate a crime. Moreover, the law places these burdens on all registrants rather than just those individuals (whether registrants or not) who are likely to commit future sex crimes involving the Internet. And the law fails to limit law enforcement's disclosure and use of the information obtained to furthering the statute's stated goals of preventing and investigating sex offenses. Its vague definitions and requirements, even if not rising to the level of a constitutional defect, increase the overbreadth of its impact on anonymous speech. In short, the law's ban on innocent anonymous online speech "suppress[es] lawful speech as the means to

suppress unlawful speech." *Ashcroft*, 535 U.S. at 255. Thus, RSA 651-B:4-a therefore cannot survive intermediate scrutiny, much less strict scrutiny, under the First Amendment and Part I, Article 22 of the New Hampshire Constitution.

C. RSA 651-B:4-a is unconstitutionally vague.

The definition of "online identifier"—particularly its inclusion of the phrases "user identification" and "chat or other Internet communication name or identity information"—is unconstitutionally vague, thus rendering RSA 651-B:4-a unconstitutional on its face.[19] And this ambiguity is with real consequence. Given the criminal penalties under the challenged law, registrants are likely to "either to overreport their activity or underuse the Internet to avoid the difficult questions in understanding what, precisely, they must report." *See Harris*, 772 F.3d at 579 (striking down similar Internet identifier law on vagueness grounds because it was "unclear as to what it requires registered sex offenders to provide," thus creating a chilling effect on innocent online speech). Thus, RSA 651-B:4-a's ambiguities create an unconstitutional chilling effect on innocent online speech.

"It is a basic principle of due process that an enactment is void for vagueness if its prohibitions are not clearly defined." *Grayned*, 408 U.S. at 108; *see also Montenegro*, 166 N.H. at 220 ("The vagueness doctrine, originally a due process doctrine, applies when the statutory language is unclear, and is concerned with notice to the potential wrongdoer and prevention of arbitrary or discriminatory enforcement.") (internal quotations omitted). A law may be void for

[19] Again, in *State v. White*, 164 N.H. 418 (2012), the New Hampshire Supreme Court held that a Myspace account constitutes "user profile information," and that this specific statutory example of an "online identifier" is not vague. The Court did not address whether RSA 651-B:4-a violated the First Amendment, as such an argument was not raised by the defendant. Nor did the Court address whether the other "online identifier" examples at issue in this lawsuit were vague. *See id.* 424 ("[W]e need not address the defendant's argument that the phrase 'chat or other Internet communication name or identity information' is also unconstitutionally vague."). This Motion does not contend that the term "user profile" is vague—a question answered in *White*—but rather challenges as vague the terms "user identification" and "chat or other Internet communication name or identity information"—a question that the *White* Court explicitly declined to address.

vagueness if it fails to give a "person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly." *Grayned*, 408 U.S. at 108; *see also Montenegro*, 166 N.H. at 221-22. Indeed, the vagueness doctrine serves to "[rein] in the discretion of enforcement officers." *See Montenegro*, 166 N.H. at 222 (quoting *Act Now to Stop War & End Racism Coal. v. District of Columbia*, 905 F. Supp. 2d 317, 330 (D.D.C. 2012)). As the New Hampshire and U.S. Supreme Courts have stated, "if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them." *See Montenegro*, 166 N.H. at 222 (citing *Grayned*, 408 U.S. at 108). When First Amendment interests are at stake, "[c]ourts apply the vagueness doctrine with special exactitude." *Montenegro*, 166 N.H. at 222 (quoting *Act Now to Stop War*, 905 F. Supp. 2d at 351). This exactitude is necessary to avoid chilling lawful, constitutionally-protected speech, as "[u]ncertain meanings inevitably lead citizens to steer far wider of the unlawful zone than if the boundaries of the forbidden areas were clearly marked." *Grayned*, 408 U.S. at 109.[20]

An "online identifier" is defined, in part, as an "electronic mail address, instant message screen name, *user identification*, user profile information, and *chat or other Internet communication name or identity information*." RSA 651-b:4-a (emphasis added). However, the law provides no further definition of the phrases "user identification," "chat," or "other Internet communication name or identity information" used in stating the contours of this requirement, thereby leaving it unclear as to what is required to be disclosed under the law. For example, a simple blog could qualify as "Internet communication name or identity information," as a blog is used to communicate with third parties—namely, members of the public who elect to visit this public website. Then again, as a blog does not necessarily contain an interface where the blogger

[20] For example, the U.S. Supreme Court has invalidated as vague a law that required door-to-door canvassers to identify themselves to the police. *See Hynes v. Mayor and Council*, 425 U.S. 610, 620-623 (1976).

can communicate privately with another individual, a blog may not satisfy the "online identifier" definition. Moreover, even if one were to assume that communicative functionality was the prerequisite for disclosure—which is far from clear under the statute's "user profile" and "user identification" language—an increasing number of sites incorporate some communicative functionality that arguably are encompassed by this "online identifier" definition, such as the use of mechanisms for communicating and linking with other users. *See id.* ¶ 36. The total number of sites incorporating communication functionality, and thus potentially qualifying as "online identifier" sites under the law, is estimated to be in the millions if not hundreds of millions. *Id.* ¶¶ 23, 26, 37. Wikipedia, for example, permits users to establish a profile and communicate directly and indirectly with each other. Is this required to be disclosed under the law? *See Harris*, 772 F.3d at 579 (in interpreting an online identifier law in California that swept within its scope "similar Internet communications," holding that such terminology was ambiguous); *White*, 696 F. Supp. 2d at 1310 (holding that a similar Georgia statute using the term "interactive online communication" chilled a sex offender's right to anonymous free speech because the term is too ambiguous). This ambiguity is highlighted by the registration form itself which, when requiring the disclosure of "online identifiers," simply tells registrants that it includes "e-mail addresses, instant message screen names, etc." *See* Sex Offender Registration Form (Biss. Dec., ¶ 10, *Exhibit I*).

RSA 651-B:4-a is unclear as to what a registrant is actually required to report. While the language of the law only requires registrants to report the "online identifier" (*e.g.*, "JohnDoe")—and not the site on which that identifier was used—obtaining an identifier without the associated site is frequently of no practical value. *See* Post Dec. ¶ 27. As a result, law enforcement agencies may demand that registrants provide the online identifier associated with a specific site or the site

associated with each online identifier. *See id.* ¶¶ 27, 40. *In fact, this appears to be occurring in New Hampshire according to the former New Hampshire State Trooper who managed the Sex Offender Registry.*[21] Similarly, under one plausible reading of the law, a registrant would be required to report only once that he has created the new screen name "JohnDoe" and may then use that identifier on as many sites as he chooses; under another, he must report this screen name for every site he uses. *See id.* ¶ 28(a).

RSA 651-B:4-a also requires reporting of certain online identifiers that "such person uses or intends to use." Again, the precise meaning is unclear: Is this "such person uses or intends to use" definition satisfied if the online identifier's creation *permits* communication, or only if the creator actually uses the online identifier to *engage* in communication? *See id.* ¶ 28(a). For example, an account on youtube.com allows a user both to watch videos and to post feedback on videos. Assuming that posting feedback constitutes participating in an "Internet communication," it is unclear whether a registrant is required to report the creation of an account on Youtube even if she never intends to post feedback.

Regulations that impact "sensitive areas of basic First Amendment freedoms" must be particularly clear to avoid chilling legitimate speech. *Baggett v. Bullitt*, 377 U.S. 360, 372 (1964). RSA 651-B:4-a is rife with imprecise definitions and uncertain requirements. The law is

[21] On March 31, 2009, Jill Rockey—then a member of the New Hampshire State Police who managed New Hampshire's sex offender registry—testified before the Senate Judiciary Committee in support of Senate Bill 142, which, among other things, made registrants' online identifiers available on the public registry (such language has since been repealed). She explained that law enforcement was asking for this information, though it may not be required under RSA 651-B:4-a. She stated:

> When offenders use instant message screen names or other chat names, the service they are using is not identified [under RSA 651-B:4-a]. In fact, right now, there is nothing in [RSA 651-B:4-a] that requires them to report that to law enforcement …. So, if they give you their screen name, if the offender's name is John Smith and that is the actual screen name he is using, you don't know if that is in Myspace; you don't know if that is in Facebook; you don't know if it is in eHarmony; you don't know if it is allthefish.com. There are several different chat rooms, different sites where people go to meet each other and, by clarifying not only the chat name they are using or electronic identifier, *but also the site at which they are using it* [sic]. Again, most sex offenders are registered offenders, offenders against children *are giving that information because law enforcement is asking for it*.

See 2009 Senate Bill 142 Testimony (Biss. Dec., ¶ 6, *Exhibit E*).

unconstitutionally vague because it fails to provide guidance to a person of ordinary intelligence as to what information he is required to report about her online speech, and the penalty for getting it wrong is prison.

D. RSA 651-B:4-a violates the right of association by requiring the compelled disclosure of membership in online communities.

Requiring registrants to disclose the online communities or groups of which they are a member implicates their "right to be protected from compelled disclosure by the State" of their associations and affiliations, and thus the freedom of association. *NAACP v. Alabama*, 357 U.S. 449, 458 (1958). RSA 651-B:4-a would require the disclosure of all such groups, including groups advocating dissident beliefs where "privacy in group association may … be indispensable to preservation of freedom of association." *Id.* at 462 (citation omitted); *see also Brown v. Socialist Workers*, 459 U.S. 87, 91 (1982). Even a legitimate purpose "cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved." *Shelton v. Tucker*, 364 U.S. 479, 488 (1960); *see NAACP*, 357 U.S. at 463, 464-65.

RSA 651-B:4-a could effectively require every registered sex offender to disclose her relationship with online organizations regardless of type, purpose, or membership, if those organizations have websites that allow members to create user profiles or have a functionality enabling a user to communicate with a third party. *See* Post Dec. ¶¶ 23, 37. Because "[m]any such relationships could have no possible bearing" on the State's interest in deterring and investigating Internet sex crimes and the law's "comprehensive interference with associational freedom goes far beyond what might be justified in the exercise of the State's legitimate" interest, this requirement violates the First Amendment. *Shelton*, 364 U.S. at 487-88, 490.

CONCLUSION

RSA 651-B:4-a fails to recognize the critical importance of online speech under the Federal and State Constitutions as well as to American culture. "Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer." *Reno*, 521 U.S. at 870. Now, more than ever, "[t]he content on the Internet is as diverse as human thought." *Id.* (internal quotation marks and citation omitted). If free speech protections are to enjoy enduring relevance in the twenty-first century, they must apply with full force to speech conducted online. *See United States v. Ramos*, 763 F.3d 45, 60 (1st Cir. 2014) ("There is ample reason to believe that it will become harder and harder in the future for an offender to rebuild his life when disconnected from the internet at home."); *United States v. Perazza-Mercado*, 553 F.3d 65, 72 (1st Cir. 2009). Moreover, RSA 651-B:4-a targets the online speech of a group widely reviled by most in New Hampshire and American society in general. When disfavored groups are targeted during the political process, this is precisely when the courts must give a skeptical gaze to the legislature's actions to ensure that civil liberties are respected. In this case, the legislature failed to even consider more narrowly tailored alternatives, let alone consider what the law's terms mean and how it would impact innocent online speech. Thus, the challenged law fails under any level of scrutiny.

WHEREFORE, the Defendant respectfully requests the following: (a) dismissal of all charges against Defendant for violating RSA 651-B:4-a; (b) a declaration that RSA 651-B:4-a is facially unconstitutional in violation of the First and Fourteenth Amendments to the United States Constitution, as well as Part I, Articles 22 and 15 of the New Hampshire Constitution; and (c) any other relief as may be just and equitable.

[redacted]

[redacted] B[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: August 7, 2015

CERTIFICATE OF SERVICE

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

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

Gilles Bissonnette, Esq.