

STATE OF NEW HAMPSHIRE
SUPERIOR COURT

Rockingham, ss.

STATE OF NEW HAMPSHIRE

v.

STEVEN BONACORSI

218-2014-CR-01357

STATE OF NEW HAMPSHIRE

v.

BRIAN MILLIGAN

218-2015-CR-868

ORDER

This order is issued in two factually unrelated criminal cases. Both of the defendants are charged with violating a provision of New Hampshire's sex offender registration statute that requires them to disclose and register all of their "online identifiers." RSA 651-B:4-a. Both defendants have moved to dismiss these charges, claiming that this statutory requirement violates the First Amendment to the United States Constitution and Part 1, Article 22 of the New Hampshire Constitution. The defendants thus challenge the facial constitutionality of RSA 651-B:4-a.

The court agrees with the defendants' argument that the obligation to pre-register an online identifier prior to use violates the First Amendment and Article 22. Because the pre-registration requirement is tangential rather than central to the statutory scheme,

it may be severed from the balance of the statute. Accordingly, the court concludes that a registrant must report new online identifiers within the same five day time frame that RSA 651-B:5 generally permits for changes in registration information. Because the lapse of the five day grace period is an element of the offense, it must be alleged by grand jury indictment and proven beyond a reasonable doubt.

The indictments in these cases do not allege that either defendant failed to report an online identifier prior to the lapse of the five day grace period. Therefore, the motions to dismiss are GRANTED and the indictments are DISMISSED WITHOUT PREJUDICE.

The order of dismissal is STAYED for thirty days to allow the State to appeal while all bail conditions remain in effect.

The court rejects the defendants' other constitutional challenges. The court will approve a motion from either or both defendants for an interlocutory appeal from the court's rulings on those challenges.

I. The Statute and The Defendants' Arguments Against It

RSA Chapter 651-B provides for the registration of sex offenders and offenders against children. All individuals convicted of certain specified offenses must register, in most cases for life. An offender who fails to comply with the requirements of the registration statute may be prosecuted for a felony.

Offenders must provide law enforcement with their names, aliases, social security numbers, permanent addresses, temporary addresses, school addresses, employment addresses, phone numbers, landlord's phone numbers, vehicle

registrations, professional licenses, passports and immigration documents. RSA 651-B:4. Offenders must report changes in this information within five days. RSA 651-B:5.

Since 2008 offenders have also been required to provide law enforcement with their "online identifiers." RSA 651-B:4-a. The statute provides as follows:

Registration of Online Identifiers. – In addition to any other information a person who is required to register is required to provide pursuant to RSA 651-B:4, such person shall report any online identifier such person uses or intends to use. For purposes of this section, "online identifier" 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. Such person shall report any changes to an existing online identifier, or the creation of any new online identifier to law enforcement before using the online identifier.

RSA 651-B:4-a.

The defendants challenge the constitutionality of the RSA 651-B:4-a on the following grounds:

1. They argue that the requirement of pre-registering online identifiers violates their State and Federal constitutional rights to speak and listen;
2. They argue that the definition of "online identifier" is vague and overbroad, thereby unconstitutionally burdening and chilling protected speech;
3. They argue that because registration of online identifiers is required regardless of the offender's actual dangerousness, the statute is too over-inclusive to survive constitutional scrutiny;
4. They argue that because (a) the statute requires registrants to disclose their participation in online communities and (b) there is no statutory prohibition on law enforcement disclosure of online identifiers, their right to engage in anonymous speech is unconstitutionally burdened and chilled; and

5. They argue that the statute infringes their freedom of association.

II. The First Amendment Rights Of Registrants

As any prison inmate can attest, a criminal justice sentence may carry with it profound restrictions on the exercise of constitutional rights. But registration is not a component of a criminal justice sentence. Registration is not a criminal penalty, sanction or forfeiture at all. As our Supreme Court has said, registration was intended by the Legislature to be a civil, “regulatory and non-punitive” means of furthering public safety. Doe v. State, 167 N.H. 382, 401 (2015). See also, Smith v. Doe, 538 U.S. 84, 96 (2003) (upholding a sex offender registration scheme because it was “a civil, non-punitive regime”).

New Hampshire’s statutory registration requirements apply to offenders, such as the defendants in these cases, who have completed their terms of confinement, criminal justice supervision and conditional liberty. Put another way, offenders must continue to register, usually for life, even after they have paid their debt to society and regained their status as free men and women.

“[R]egistered sex offenders who have completed their terms of probation and parole enjoy the full protection of the First Amendment.” Doe v. Harris, 772 F.3d 563, 572 (9th Cir. 2014) (striking down portions of a statute that requires the registration of internet identifiers); See also, White v. Baker, 696 F.Supp. 1289 (N.D.Ga. 2010) (striking down a statute that required the registration of internet identifiers because it was overbroad); Doe v. Snyder, 101 F. Supp. 3d 672, 690 (E.D. Mich. 2015) (narrowly construing an internet identifier registration requirement to avoid a First Amendment vagueness and overbreadth problem); Doe v. City of Albuquerque, 667 F.3d 1111, 1128

(10th Cir. 2012) (striking down an ordinance that prohibited registrants from entering public libraries where children congregate); Doe v. Jindal, 853 F. Supp. 2d 596, 605 (M.D. La. 2012) (striking down a statute that largely prohibited registrants from using social networking sites, internet chat rooms and peer-to-peer networks); Doe v. Prosecutor, Marion County, Indiana, 705 F.3d 694, 703, (7th Cir. 2013) (same); Harris v. State, 985 N.E.2d 767, 781 (Ind. Ct. App. 2013) (same); But see, State v. Packingham, 777 S.E.2d 738, 746 (N.C. 2015) (upholding a prohibition on registrants' use of social media services that permit participation by minors), petition for certiorari pending as U.S. Supreme Court No. 15-1194.

Of course, even those of us with full First Amendment and Article 22 protection face some limits on the exercise of our First Amendment and Article 22 rights. See e.g., Williams-Yulee v. Florida Bar, 135 S. Ct. 1656 (2015) (candidates for judicial office, in states where judges are elected, may be prohibited from personally soliciting campaign contributions); see also, N.H. Supreme Court Administrative Rule 38, Code of Judicial Conduct, Cannon 5(A) (prohibiting New Hampshire judges from making speeches for or endorsing political candidates and from engaging in most forms of political activity); N.H.R.Prof.C. 7.1 through 7.5 (governing attorneys' direct solicitation of prospective clients, attorney advertising, law firm names and letterhead). The same Constitutional framework that applies to judges, lawyers and everybody else applies to registered sex offenders as well. Those standards are addressed below.

III. The Applicable Level Of Constitutional Scrutiny

Subject to a handful of judicially recognized exceptions that are not applicable to these cases, restrictions on the content of speech are constitutional only if they survive

the most exacting scrutiny. See e.g., United States v. Playboy Entertainment Group, Inc., 120 S. Ct. 1878, 1886 (2000):

If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest. [citation omitted]. If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative.

See also, Doyle v. Commissioner, New Hampshire Department of Resources and Economic Development, 163 N.H. 215, 221 (2012) ("If a restriction is content-based, it must be narrowly tailored to serve a compelling government interest.").

Content-neutral restrictions are constitutional if they meet a slightly less rigorous test: (a) content-neutral restrictions must be narrowly tailored to promote a "significant" government interest, rather than a "compelling" government interest, and (b) content-neutral restrictions need not be the least restrictive alternative, but cannot burden substantially more speech than necessary to further the government's significant interest. See e.g., Doe v. Harris, 772 F.3d at 576-77:

Content-neutral restrictions on protected speech survive intermediate scrutiny so long as they are narrowly tailored to serve a significant governmental interest, and leave open ample alternative channels for communication of the information. [citations omitted]. To satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests. [citation omitted]. Rather, the test is whether the means chosen burdens substantially more speech than is necessary to further the government's legitimate interests. [citation omitted]. The government must also demonstrate that the recited harms are real and that the regulation will in fact alleviate these harms in a direct and material way. [citation omitted].

(internal quotation marks, bracketing and citations omitted); see also, McCullen v. Coakley, 134 S. Ct. 2518, 2529 (2014); Doyle, 163 N.H. at 215; State v. Bailey, 166 N.H. 537, 542 (2014).

The statute at issue in this case, RSA 651-B:4-a, restricts speech even though it does not flatly prohibit registrants from expressing, reading, listening to or viewing anything. See Doe v. Harris, 772 F.3d at 572, finding that a similar internet identifier registration statute restricted speech, thereby triggering First Amendment scrutiny:

...[A] a law may burden speech—and thereby regulate it—even if it stops short of prohibiting it. Indeed, the distinction between laws burdening and laws banning speech is but a matter of degree. [citations omitted].

There can be little doubt that requiring a narrow class of individuals to notify the government within 24 hours of engaging in online communication with a new identifier significantly burdens those individuals' ability and willingness to speak on the Internet. . . .

* * *

The Act also has the inevitable effect of burdening sex offenders' ability to engage in anonymous online speech.

RSA 651-B:4-a's restrictions on speech are content-neutral. The statute applies to the use of online identifiers in connection with all of the types of communication we see on the internet, ranging from serious political commentary (from left, right, center and other viewpoints) to posting and viewing cute pictures of cats. Therefore, to the extent that RSA 651-B:4-a restricts speech, it should be subject to intermediate level scrutiny.

The defendants nonetheless argue for the application of strict scrutiny. They concede that RSA 651-B:4-a is content-neutral. However, they claim that strict scrutiny should be applied to content-neutral statutes that are directed at a single class of disfavored speakers. They argue that because sex offenders are modern day pariahs, efforts to silence them (or chill their speech) ought to be subject to the most demanding level of scrutiny. This court rejects their argument because it goes further than either the U.S. Supreme Court or the New Hampshire Supreme Court has gone.

Defendants ground their argument in favor of strict scrutiny on the following passage from the U.S. Supreme Court's opinion in Citizens United v. Federal Election Commission, 130 S. Ct. 876, 898-99 (2010):

Premised on mistrust of governmental power, the First Amendment stands against attempts to disfavor certain subjects or viewpoints. [citation omitted]. Prohibited, too, are restrictions distinguishing among different speakers, allowing speech by some but not others. [citation omitted]. As instruments to censor, these categories are interrelated: Speech restrictions based on the identity of the speaker are all too often simply a means to control content.

Quite apart from the purpose or effect of regulating content, moreover, the Government may commit a constitutional wrong when by law it identifies certain preferred speakers. By taking the right to speak from some and giving it to others, the Government deprives the disadvantaged person or class of the right to use speech to strive to establish worth, standing, and respect for the speaker's voice. The Government may not by these means deprive the public of the right and privilege to determine for itself what speech and speakers are worthy of consideration. The First Amendment protects speech and speaker, and the ideas that flow from each.

(emphasis added).

However, the actual holding of Citizens United applies only to restrictions that are directed specifically at political speech:

We find no basis for the proposition that, in the context of political speech, the Government may impose restrictions on certain disfavored speakers.

The Citizens United case involved a federal statute that limited the ability of certain types of entities to engage in political speech in connection with federal elections.

Although the statute did not discriminate among political viewpoints, neither did it reach non-political speech.

The U.S. Supreme Court has not extended this holding in Citizens United to statutes that cover both political and non-political speech. Certainly, the risk of *sub rosa*

viewpoint discrimination is far more remote in cases such as this one, where the great bulk of the affected speech is likely to be non-political.

Every court that has considered the issue has found that content-neutral restrictions on sex offender registrants' use of the internet is subject to intermediate level scrutiny. See e.g., Doe v. Harris, 772 F.3d at 575 (distinguishing Citizens United and applying intermediate level scrutiny because "although it is true that the Act singles out registered sex offenders as a category of speakers, it does not target political speech content, nor is it a ban on speech."); Doe v. Prosecutor, 705 F.3d at 698; Doe v. Jindal, 853 F. Supp. 2d at 605; Doe v. Snyder, 101 F. Supp. 3d at 727; White v. Baker, 696 F.Supp. 2d at 1307–08; Doe v. Nebraska, 898 F. Supp. 2d 1086, 1107 (D. Neb. 2012).

Accordingly, the court rejects the defendants' argument in favor of strict scrutiny and finds that intermediate scrutiny applies. Thus, RSA 651-B:4-a can survive constitutional scrutiny if it is narrowly tailored to serve a significant government interest and if it allows for adequate alternative channels for speech.

IV. The Vagueness And Overbreadth Doctrines

The defendants challenge the facial validity of RSA 651-B:4-a on the grounds that it is unconstitutionally vague and overbroad. A brief summary of the vagueness and overbreadth doctrines follows.

A. Vagueness

A statute that restricts speech is unenforceable if it fails to provide reasonable clarity as to what it prohibits. Montenegro v. New Hampshire Division of Motor Vehicles, 166 N.H. 215, 221-22 (2014); State v. MacElman, 154 N.H. 304, 307 (2006). More

particularly, a statute is facially unconstitutional if it (a) fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits; or (b) authorizes or even encourages arbitrary and discriminatory enforcement. Montenegro, 166 N.H. at 215. See, Grayned v. City of Rockford, 408 U.S. 104, 108-09 (1972):

Vague laws offend several important values. First, because we assume that man is free to steer between lawful and unlawful conduct, we insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Second, if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them. A vague law impermissibly delegates basic policy matters to policemen, judges, and juries for resolution on an *ad hoc* and subjective basis, with the attendant dangers of arbitrary and discriminatory application. Third, but related, where a vague statute abuts upon sensitive areas of basic First Amendment freedoms, it operates to inhibit the exercise of those freedoms. Uncertain meanings inevitably lead citizens to steer far wider of the unlawful zone than if the boundaries of the forbidden areas were clearly marked.

(internal quotation marks, ellipsis, citations and footnotes omitted). The vagueness doctrine is applied “with special exactitude” when First Amendment and Article 22 interests are at stake. Montenegro, 166 N.H. at 222.

Nonetheless, “perfect clarity and precise guidance have never been required even of regulations that restrict expressive activity.” Montenegro, 166 N.H. at 222, quoting United States v. Williams, 553 U.S. 285, 304 (2008). “Condemned to the use of words, we can never expect mathematical certainty from our language.” Montenegro, 166 N.H. at 222, quoting Grayned, 408 U.S. at 110. Therefore, even a perfectly constitutional statute may harbor some degree of latent ambiguity.

B. Overbreadth

Under the familiar First Amendment and Article 22 overbreadth doctrine “a statute is facially invalid if it prohibits a substantial amount of protected speech.” United

States v. Williams, 553 U.S. 285, 292 (2008). See also, United States v. Stevens, 559 U.S. 460, 473 (2010); State v. Brobst, 151 N.H. 420, 422 (2004). A defendant has standing to challenge overbroad restriction on speech, even if the restriction could be applied to his own conduct without creating any constitutional ripple. This is so because an overinclusive statute will chill and deter others from exercising their constitutionally protected right to speak. Thus, “[t]he purpose of the overbreadth doctrine is to protect those persons who, although their speech or conduct is constitutionally protected, ‘may well refrain from exercising their rights for fear of criminal sanctions by a statute susceptible of application to protected expression.’” Brobst, 114 N.H. at 420, quoting New York v. Ferber, 458 U.S. 747, 768 (1982).

Of course, the constitutionally protected rights at issue include not only the right to propagate one’s thoughts, but also the right to read, hear and view what others have produced. “[W]here a speaker exists . . . the protection afforded is to the communication, to its source and to its recipients both.” Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 96 S. Ct. 1817, 1823 (1976) (discussing the right to advertise and the reciprocal right to receive advertising). See also, Red Lion Broad. Co. v. F.C.C., 395 U.S. 367, 390 (1969) (“It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas[.]”); Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 556 (1980) (noting “the First Amendment right to receive information and ideas.”).

Finally, protected “speech” includes not only oral and written expositions but also drawings, photographs, videos, music, dance, symbolic speech and all other forms of expression. See e.g., Texas v. Johnson, 109 S. Ct. 2533, 2539 (1989) (“The First

Amendment literally forbids the abridgment only of 'speech,' but we have long recognized that its protection does not end at the spoken or written word.”).

V. The Internet

This case requires the court to apply the foregoing legal doctrines and principles in the context of online speech. Before doing so, it is necessary to reflect on how deeply the internet has become larded into everyday life over the past two decades. Twenty-five years ago (circa 1991) a legal prohibition on using the internet altogether would have had no actual impact on the exercise of First Amendment/Article 22 rights by the vast majority of ordinary citizens. Twenty years ago, such a prohibition would likely be seen by all but a small minority as a hassle, but not as a meaningful impediment to speech.

The internet has since become an increasingly central means of communication in the lives of ordinary Americans. Perhaps the best milestone for this purpose is 1998, the year that Google first appeared on our screens. During the so-called dot.com boom, circa 1999 to 2000, we were told that the internet would change everything. Indeed it has. Take our profession, for example:

-We obtain New Hampshire Supreme Court slip opinions via a link to a webpage that the court supplies to us via its one-way listserv;

-If we don't choose to read the New Hampshire Supreme Court's opinions right away, we can read brief reviews written by quasi-anonymous third parties on Twitter;

-We obtain full text U.S. Supreme Court decisions within hours of their release, never bothering with the paper advance sheets that were such important reading in the past;

-Lawyers in virtually every niche of the profession have access to two-way listservs, computer bulletin boards and forums in which to discuss matters relevant to their practices;

-We pay our bar dues, look-up each other's office addresses and register for CLE's via the NH Bar's website;

-We sometimes attend CLE's by webinar, during which we may ask questions and interact with the presenters in real time;

-In small claims and guardianship cases, the parties submit most pleadings over the internet, as is done in virtually every federal civil and criminal case in the country;

When our workday is over, we read our newspapers online. We also read the comments left behind by previous readers and some of us add our own comments. We use the internet to browse, aided by ubiquitous professional and amateur reviews, and then shop for clothes, travel, housewares, hardware, insurance, new cars, new jobs, lawyers, doctors and home remodelers. We read and sometimes write and rate reviews of hotels, restaurants, shows and attractions. We communicate with our friends and colleagues by email, texts, Skype, Google Hangouts, Facetime, GoToMeeting, etc. We research everything from our medical symptoms to the causes of the First World War almost exclusively online. We join professional and avocational on-line communities. We remain in touch with friends and acquaintances via social networking sites and applications. There are those who search for romantic partners online. There are those who stream live video and those who consume live and stored video of the events of the day.

Most of us get our music online. Some of us review playlists prepared by others. Some of us share playlists with others. We take college level courses online and listen to podcasts relating to virtually any subject or discipline that suits us. We go online to play every kind of game from backgammon to bridge to so-called massive multiplayer games.

The significance of the internet for our nations' political process cannot be overstated. We have candidates who tweet and constituents who tweet back, joining and perhaps changing the conversation. A single video uploaded to the internet by a bystander can dominate the news cycle. There are those among us who cannot help but proclaim their political views and forward articles of interest via social media. Petitions are circulated online. Protests marches are planned online. Proposed legislation is published, circulated and critiqued online.

All of this is speech.

VI. RSA 651-B:4-a's Pre-Registration Requirement Is Unconstitutional But Severable

Defendants have one clearly meritorious, albeit limited challenge to RSA 651-B:4-a. The statute requires the pre-registration of new online identifiers prior to their use. Thus, for example, a registrant would be committing a felony if he or she responded to a political candidate's speech by establishing a Twitter account to either (a) immediately comment or (b) immediately follow the commentary of others. Likewise a registrant could not establish a new Periscope account to immediately live stream video from some newsworthy event or to view or comment on live video posted by others. A registrant with a recent medical diagnosis could not join an internet forum to

obtain immediate information from others with the same illness regarding his or her symptoms and treatment.

The U.S. Court of Appeals for the Ninth Circuit recently struck down a requirement that sex offender registrants report new online identifiers within 24 hours *after* establishing the identifiers. Doe v. Harris, 772 F.3d 563, 581-582 (9th Cir. 2014):

[T]he Act's 24-hour update requirement undeniably impedes protected First Amendment activity. [citation omitted]. Although registered sex offenders do not have to register before they communicate online, they must register within 24 hours of using a new Internet identifier—a shorter time than is given by registration laws in other jurisdictions. [citation omitted]. This burden is particularly onerous for sex offenders who live in remote areas or who, like other citizens, have multiple Internet identifiers. See Doe v. Nebraska, 898 F.Supp.2d. at 1122 (granting a preliminary injunction because a blog-reporting requirement that “[r]equir[ed] sex offenders to constantly update the government ... [wa]s unnecessarily burdensome and ... [wa]s likely to deter the offender from engaging in speech that is perfectly appropriate”).

Moreover, anytime registrants want to communicate with a new identifier, they must assess whether the message they intend to communicate is worth the hassle of filling out a form, purchasing stamps, and locating a post office or mailbox. The mail-in requirement is not only psychologically chilling, but physically inconvenient, since whenever a registered sex offender obtains a new ISP or Internet identifier, he must go somewhere else within 24 hours to mail that information to the State. [citation omitted]. The 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 or ISP accounts. [citation and parenthetical quotation omitted]

The 24-hour reporting requirement is not only onerous, it is also applied in an across-the-board fashion. 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. . . . In short, we have a hard time finding even an attempt at narrow tailoring in this section of the Act.

This court adopts the Ninth Circuit's reasoning and finds that New Hampshire's preregistration requirement violates both the First Amendment and Part 1, Article 22. To be sure, the court finds that the pre-registration requirement is designed to promote significant government interests. Those interests include (a) preventing convicted sex offenders from committing future offenses against children and other vulnerable victims and (b) investigating such offenses as may occur. As our Supreme Court observed in State v. White, 164 N.H. 418, 422 (2012):

Requiring a registered offender to report the creation of . . . [an online identifier] . . . promotes the investigatory purpose of the statute by providing law enforcement with the means to monitor and track the offender's online activities. Such a requirement also serves to discourage the use of social networking for predatory purposes because the offender knows he or she is under the watchful eye of law enforcement.

However, the nexus between preregistration and these laudable objectives is too weak to survive intermediate scrutiny. The preregistration requirement is not narrowly tailored and it burdens substantially more protected speech than is necessary to further the government's legitimate interest. The imposition of a waiting period for speech, effectively prohibits a substantial amount of protected speech.

Having determined that the preregistration requirement is unconstitutional, the next question is whether it may be severed from the balance the statute. See e.g., Deere & Company v. State, ___ N.H. ___, 130 A.3d 1197, 1214 (2015):

In determining whether the valid provisions of a statute are severable from the invalid ones, we presume that the legislature intended that the invalid part shall not destroy the validity of the entire statute. [citation omitted]. We then examine whether the unconstitutional provisions of the statute are so integral and essential in the general structure of the act that they may not be rejected without the result of an entire collapse and destruction of the structure" of the statute.

(internal quotation marks and citations omitted); Associated Press v. State, 153 N.H. 120, 141 (2005); Claremont School District v. Governor, 144 N.H. 210, 217 (1999).

The pre-registration requirement is tangential, rather than integral to RSA 651-B:4-a. It can be easily severed from the balance of the statute without significantly undermining the statutory scheme. RSA 651-B:5 provides a five day grace period for reporting all changes in registration information. This five day requirement period would apply to online identifiers if the preregistration language were stricken from RSA 651-B:4-a. A five day grace period would be perfectly constitutional and would be narrowly tailored to serve all of the State's legitimate interests. See e.g., White, 696 F.Supp 2d at 1294 (involving a similar statute with grace period of 72 hours); Doe v. Snyder, 101 F. Supp. 3d at 690 (involving a similar statute with a grace period of three business days).

Accordingly, the court concludes that (a) the pre-registration provision is unconstitutional on its face and (b) registrants have a five day grace period in which to report new online identifiers. The lapse of the five day grace period is an element of the offense that the grand jury must allege and the State must prove beyond a reasonable doubt. Because the indictments do not allege this element, they are DISMISSED WITHOUT PREJUDICE. Thus, the defendant's motion to dismiss is GRANTED IN PART WITHOUT PREJUDICE.

VII. RSA 651-B:4-a's Definition Of "Online Identifier" Is Neither Vague Nor Overbroad

A. The Issues And The Parties' Positions

The defendants argue that that RSA 651-B:4-a is unconstitutionally vague and overbroad. They first argue that the statute defines the term "online identifier" so poorly that they are left to guess at its meaning. Indeed, in defendant Bonacorsi's case, the

local police and the County Attorney's office were themselves of two minds about the scope of the statutory definition.¹ The defendants also claim that the statute requires the registration of online identifiers for important conduits of protected speech that are freakishly unlikely to be used for nefarious purposes. Therefore, they claim that it is not narrowly tailored and burdens a substantial amount of protected speech.

The statute applies not only to email addresses, instant message screen names, internet chat names and social media profiles, but also to all "internet communication names" and "internet . . . identity information." Defendants argue that this broad residual language could indeed be easily misread to apply to things like:

-IDs used for shopping, payment and account tracking (i.e. to access bank accounts, pay bills, book travel, interact with cable, electric, water and gas utilities and to make purchases);

-IDs used for commercial newspaper subscriptions (such as the *New York Times*, the *Wall Street Journal*, the *Union Leader*, etc.) and other informational websites and services;

-Names and "handles" used to post comments on articles published in the online versions of newspapers (such as the *Union Leader* or the *New York Times*) and on purely online publications (such as *Slate*, *Salon* and *CNET*) and blogs (such as *Sentencing Law and Policy* and *Crime and Consequences*);

¹The State not pressed an indictment against Bonacorsi for failing to report a "brandyourself.com" ID. Apparently, the State initially believed that it was a felony not to report the ID but later determined that it was no crime at all. The local police allegedly gave Bonacorsi inconsistent guidance concerning his need to report his ID for "healthcare.gov."

-Screen and account names for sites that allows users to comment on the quality and value of goods and services (such as Trip Advisor, Yelp, Amazon, LL Bean, etc);

-URLs and other information relating to websites authored or maintained by the registrant;

-Login IDs for cloud based services that store one's own information (such as Dropbox, Google Drive, iCloud, Evernote, etc.);

-Login IDs for wide area networks and intranets, such as those used by the judicial branch;

The State's position is that the residual language in the definition of "online identifier" is limited to "those services where [registrants] engage in person-to-person communications over the internet." See, State's Objection in Bonacorsi, p. 20. Thus, the State opines that the statute is sufficiently definite and narrowly tailored to survive constitutional scrutiny.

B. Analysis

(i) Statutory Construction—In General

The first step in the analysis of the defendants' vagueness and overbreadth arguments is to construe the statutory term "online identifier." The interpretation of a statute is a question of law. State v. Etienne, 163 N.H. 57, 71-72 (2011); State v. Breed, 159 N.H. 61, 64-65 (2009). The court's responsibility is to determine the intent of the legislature as expressed in the words of the statute considered as a whole. Etienne, 163 N.H. at 71-72; Breed, 159 N.H. at 64-65. In doing so, the court does not read statutory phrases and provisions in isolation, but rather "interpret[s] a statute in the

context of the overall statutory scheme.” State v. Kousounadis, 159 N.H. 413, 423 (2009).

The court must first look exclusively at the language of the statute itself, and, if possible, construe that language according to its plain and ordinary meaning. Etienne, 163 N.H. at 71-72; Breed, 159 N.H. at 64-65. The court’s inquiry is limited to “the statute as written and [the court] will not consider what the legislature might have said or add language it did not see fit to include.” Kousounadis, 159 N.H. at 423; see also, State v. Jennings, 159 N.H. 1, 3 (2009); State v. Hynes, 159 N.H. 187, 193 (2009); State v. Bernard, 158 N.H. 43, 44 (2008).

If the plain meaning of the statutory language can be determined from the black letter text, the analysis stops there. See, Etienne, 163 N.H. at 71-72. If, however, the statutory language is ambiguous, then—and only then—may the court may consider the statute’s legislative history. See, Matter of Lyon, 166 N.H. 315, 318 (2014) (“When the language of a statute is plain and unambiguous, we do not look beyond it for further indications of legislative intent. However, we review legislative history to aid our analysis when the statutory language is ambiguous or subject to more than one reasonable interpretation.”); State v. Spade, 161 N.H. 248, 251 (2010); Smith v. City of Franklin, 159 N.H. 585, 588 (2010).

In construing provisions of the Criminal Code, the court is mindful that “[t]he rule that penal statutes are to be strictly construed does not apply[,]” . . . [and] [a]ll provisions of this code shall be construed according to the fair import of their terms and to promote justice.” RSA 625:3. See, Breed, 159 N.H. at 64-65.

(ii) Statutory Construction—Ejusdem Generis

RSA 651-B:4-a's definition of "online identifier" includes three concrete examples followed by residual language creating a general category. The three specific examples of online identifiers are email addresses, instant messaging screen names and chat names. The residual categories include "user identification," "user profile information," and "other Internet communication name or identity information." The New Hampshire Supreme Court has already construed the category of "user profile information" to include social media profile pages. State v. White, 164 N.H. 418 (2012).

Indulging the presumption that the legislature does not waste words and that it intends for every word in a statute to be given effect, Garand v. Town of Exeter, 159 N.H. 136, 140–41 (2009), In re Guardianship of Williams, 159 N.H. 318, 323 (2009); State v. Yates, 152 N.H. 245, 256 (2005), the court must read the statute in such a way that the specific examples are not are not pure surplusage. Yet, if the residual, catchall categories are read broadly enough, the specific examples would add nothing to the statute. Thus, the syntax of the statute suggests that the specific examples were intended, and should be read as guide posts that inform the meaning of the residual language.

This common sense reasoning is reflected in an oft-used canon of statutory construction known as *ejusdem generis* (Latin for "of the same kind"). "This doctrine provides that where general words follow an enumeration of persons or things, by words of a particular and specific meaning, such general words are not to be construed in their widest extent, but are to be held as applying only to persons or things of the same kind or class as those specifically mentioned." State v. Beckett, 144 N.H. 315, 318-19

(1999). See also, Breed, 159 N.H. at 65; Dolbeare v. City of Laconia, 168 N.H. 52 , 55 (2015); State v. Beauchemin, 161 N.H. 654, 658 (2011); In re Hennessey-Martin, 151 N.H. 207, 211 (2004); State v. Wilson, 140 N.H. 44, 45 (1995); State v. Meaney, 134 N.H. 741, 744 (1991); State v. Small, 99 N.H. 349, 350-52 (1955); see generally, CSX Transp., Inc. v. Alabama Dep't of Revenue, 131 S. Ct. 1101, 1113 (2011) ("We typically use *ejusdem generis* to ensure that a general word will not render specific words meaningless.); Yates v. United States, 135 S. Ct. 1074, 1086 (2015) (same); 2A Sutherland Statutory Construction §47:17 (7th ed.):

The doctrine of *ejusdem generis* seeks to reconcile an incompatibility between specific and general words in light of other rules of construction that all words in a statute and other legal instruments are to be given effect, if possible, that all parts of a statute are to be construed together, and that a legislature is presumed not to have used superfluous language. If the general words are given their full and natural abstract meaning, they would include the objects designated by the specific words, making the latter superfluous. If, on the other hand, the series of specific words is given its full and natural meaning, the general words are partially redundant. The rule accomplishes the purpose of giving effect to both the particular and the general words, by treating the particular words as indicating the class, and the general words as extending the provisions of the statute to everything embraced in that class, though not specifically named by the particular words. The resolution of this conflict by ascribing to the series its natural meaning and by restricting the meaning of the general words to things *ejusdem generis* with the series is justified on the ground that, had a legislature intended the general words to be used in their unrestricted sense, it would have made no mention of the particular words, but would have used only one compendious expression.

Ejusdem generis is a common drafting technique designed to save a legislature from spelling out in advance every contingency in which a statute could apply. When foreseeable circumstances are too numerous or varied for particular enumeration, a legislature may employ *ejusdem generis* principles and permissibly rely on courts to give content to a general statutory phrase. Consequently, courts may use *ejusdem generis* to avoid a finding of unconstitutional vagueness where an enumeration of unlawful conduct clarifies a subsequent general term enough to provide guidance to a person of reasonable intelligence, and the general term encompasses conduct a legislature intended to prevent.

In this case, the doctrine of *ejusdem generis* suggests that the general terms “user identification,” “user profile information,” and “other Internet communication name or identity information” should be read to include only those things that are similar to email addresses, instant message screen names and chat names. Email services, internet instant messaging services and internet chat services have the following common and essential attributes:

(A) They have a primary purpose of facilitating person-to-person, two-way communication (as opposed to one-way broadcasting or consumption);

(B) Over the internet (as opposed to over local or wide area networks, VPN’s and intranets, such as, for example the NH Judicial Branch network); and

(C) With persons other than the issuer of the email address, chat name or messaging name.

Therefore, the doctrine of *ejusdem generis* suggests that the general categories of “online identifiers” include only names, handles, IDs and profiles for websites sites and services that share these attributes. This is essentially the State’s construction with four clarifying tweaks to the concept of “person-to-person” communication.

First, the communication must be two-way. Otherwise, the definition would include websites and services that allow users to comment on and/or rate reviews left by other users (such as, for example, Amazon, LL Bean, Yelp and Trip Advisor). If user “A” gives five stars to a hotel review by user “B,” then user A should reasonably anticipate that user “B” will see this. Thus, user “A” would be having indirect, one-way person-to-person communication with user “B.” The same sort of one-way communication can be found in the user comments on *The Union Leader* website.

Commenters on *Union Leader* articles frequently applaud or disparage the comments of others. This is clearly not the type of online activity that falls within the scope of RSA 651-B:4-a.

Second, the communication must be with a third party, i.e. somebody other than the person or entity that issued the online identifier. Otherwise, the definition would cover virtually every website and service that allows the transaction of business over the internet (such as Verizon, Eversource, Xfinity, Citizens Bank, Amazon, etc.). Many commercial websites and services allow registered users to chat or otherwise communicate with customer service representatives.

Third, the communication must be over the internet and not on a private network. Otherwise, the statute would apply to IDs that are used solely within personal or business networks. For example, many N.H. Judicial Branch employees have IDs that are used to access the court's wide area network based Odyssey case management system and JMS jury management system. Although both of these applications allow for communication, they do not each beyond the virtual four walls of the network.

Fourth, the website, application or service must have as a primary purpose the facilitation of communications (i.e. person-to-person, two way, over the internet communications with third parties). The facilitation of these communications need not be the sole purpose for the website and it need not be the primary purpose. But it must be a primary purpose rather than a purely incidental purpose. Otherwise, the definition of online identifier would include sites like Trip Advisor and the Union Leader, because users can comment on the reviews and comments of other users. Likewise, without a primary purpose limitation the statute would reach auction sites such as EBay because

buyer and seller can communicate. Indeed, the Uber iPhone application allows communication between passenger and Uber driver. None of these types of incidental communications is likely to be exploited for nefarious, sexual purposes.

These four tweaks to the State's definition are necessary not only because they are inherent in a reasoned examination of the statute's specific examples (i.e. email address, internet messaging name and internet chat name), but also because without these limits RSA 651-B:4-a might very well be unconstitutionally vague overbroad. See, White v. Baker, 696 F. Supp. 2d 1289, 1309-1310 (N.D. Ga. 2010) (holding that Georgia's internet identifier registration statute was unconstitutionally vague and overbroad because it could be read to apply to blogs, publicly posted comments directed to the world and retail and banking sites). Statutes must be construed to avoid conflict with constitutional rights wherever reasonably possible. See e.g., State v. Ploof, 162 N.H. 609, 620 (2011); Opinion Of Justices, 162 N.H. 160, 164 (2011); State v. MacElman, 154 N.H. 304, 307 (2006); State v. Pierce, 152 N.H. 790, 791 (2005); Opinion of the Justices, 140 N.H. 22, 26 (1995); State v. Smagula, 117 N.H. 663, 666 (1977).

The court notes that RSA 651-B:4-a's definition of "online identifier" is not limited to identifiers used in connection with websites and services that are used by children. Thus, for example, the indictment in Bonacorsi's case for failure to register a LinkedIn ID states a crime even though children are unlikely to join and use LinkedIn. Likewise, a registrant would need to disclose IDs used for internet bulletin boards that are devoted to topics unlikely to interest children, such as for example, retirement planning or living with cancer. This is so because the text of RSA 651-B:4-a does not contain any

language suggesting an intent to limit the reach of the statute to websites and services that cater to children. The court cannot rewrite the statute under the guise of construing it.

It comes as no great surprise that the statute includes identifiers used in connection with websites that cater exclusively to adults. Sex offender registrants include those who have committed sex crimes against adults through such means as force, threats, extortion, kidnapping, false imprisonment, surprise, incapacitation by alcohol or drugs, coercion through the use of certain defined positions of authority, and the exploitation of victims who are physically or mentally incapable of giving consent. See, RSA 632-A:2. The goal of the online identifier statute is to protect all potential victims including vulnerable adults. Adults, no less than children, may be exploited by those who abuse dating sites such as Tinder or OKCupid, or via online social communities through which adults meet and congregate.

Finally, the court notes that its construction of the residual language in RSA 651-B:4 is supported by the U.S. District Court's decision in Doe v. Snyder, 101 F. Supp. 3d 672, (E.D. Mich. 2015). In Snyder the court construed an internet identifier registration statute that required sex offender registrants to disclose "electronic mail or instant message address[es], [and] any other designations used in internet communications or postings." Snyder, 101 F. Supp. 3d at 690. The plaintiff in Snyder argued that the residual phrase "any other designation used in internet communications or postings" was unconstitutionally vague. The court responded to this argument as follows:

While the phrase uncontroversially includes social media aliases and other aliases used for the primary purpose of exchanging information with other Internet users, there are many Internet aliases that individuals use that involve some degree of Internet communication but do not clearly fall

within [the Michigan statute]. Plaintiffs ask, "Must an individual report when setting up a new on-line bank account, Amazon account, Mlive account, gaming account, etc.?" . . . In the broadest sense, virtually all online accounts are Internet designations used for some sort of communication.

In order to alleviate ambiguity and in light of the rule of lenity, the court interprets [the Michigan statute's] catch-all Internet designation phrase to apply to Internet designations that are primarily used in Internet communications or postings. This construction is consistent with a plain reading of the statute. Under the established interpretive canons of *noscitur a sociis* and *ejusdem generis*, where general words follow specific words in statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words. [citations omitted]. "Any other designation used in internet communications or postings" is a general phrase which follows the more specific terms "electronic mail" and "instant message address[.]" . . . E-mail and instant message addresses are used primarily for the purpose of communicating with other individuals online. Therefore, applying the canon of *ejusdem generis*, the court construes "other designations used in internet communications or postings" to refer only to designations used primarily for the purposes of Internet communications or postings.

This construction excludes designations used primarily to engage in e-commerce and online banking, or to read content like online newspaper accounts even though registrants may post comments at the end of online newspaper articles or "chat" with Amazon representatives. Meanwhile, a MMORPG [massively multiplayer online role-playing games] alias is created for the primary purpose of interacting with other online gamers and engaging in a substantial amount of communications. Such aliases are "similar in nature" to e-mail and instant message addresses and fall within the Internet designation provision.

* * *

In sum, using this narrowing construction, [the Michigan statute] is sufficiently clear to provide fair notice to registrants and adequate guidance to law enforcement.

To be sure, this court's construction of RSA 651-B:4-a is more wordy than the pithy construction that the U.S. District Court gave to the Michigan statute in Snyder. However, the examples in Snyder suggest that the U.S. District Court's laconic

language was intended to convey the same concepts as those set forth above. In this court's view the extra words are necessary to clarify the reach of the New Hampshire statute.

(ii) Vagueness

As construed by the court, the statutory concept of an "online identifier" is not unconstitutionally vague. The requirements that the website or service (a) facilitate two-way, person-to-person communication, (b) over the internet, and (c) with persons other than the issuer of the identifier, are all bright lines.

Concededly, the "primary purpose" requirement is less exact. There may well be some cases in which reasonable minds can disagree as to whether a particular website or service has a primary purpose of facilitating two-way, person-to-person communication. However, such a primary purpose will usually be found if a website or service offers a forum, bulletin board, chat service, two-way listserv or similar means of promoting discussions among users. Conversely, the primary purpose requirement will usually not be met by the comment and review functions of blogs, newspapers, ratings sites, auction sites, and commercial sites. Without the "primary purpose" requirement the statute would be unconstitutionally overbroad. The slight amount of grey that it introduces does not make the statute unconstitutionally vague.²

²It is perhaps also worthwhile to note that if the statute were limited to websites and services that attract children, that limitation would have created a much more serious vagueness concern. Clearly, the applicability of such a statute could not depend on a website's formal terms of service. Many websites have policies forbidding minors to enter—including, for example the N.H. Liquor Commission Outlet website—but anybody old enough to use a keyboard can put in a random birthdate and use virtually all of these sites. As any middle school student can attest, young teens are among the most frequent users of social networks, messaging services, chat services

Continued on next page

(iii) Overbreadth

As explained above, a statute is overbroad and facially invalid if prohibits a substantial amount of protected speech. Defendants concede that RSA 651-B:4-a does not prohibit registrants from saying or listening to anything, anywhere, at any time, for any reason, by any means.³ Registrants are free to join social networks, use instant messaging services, engage in real time internet chats, play internet based games, use dating sites and services, post to internet bulletin boards, etc. The statute does not prohibit them from engaging in two-way, person to person communication with minors or from joining social networks that attract minors. It only requires the registration of certain online names, handles and IDs.

Furthermore, as construed by the court, those registration requirements apply only to the particular types of websites and services that are the most likely to be used (a) to establish a confidential personal relationship with another person, and (b) in secrecy from the other person's family and real life friends. To the extent there is a substantial risk that registrants will re-offend by abusing such relationships (see, below), the definition of "online identifier," as construed by the court, is narrowly tailored to promote significant State interests. The court rejects defendants' argument that this definition is overbroad.

Continued from previous page

and the like, regardless of the terms of service. The alternatives to relying on the terms of service are to consider (a) whether the website or service appears to be attractive to children and (b) whether the website or service actually attracts children. Appearance is very often in the eye of the beholder and actual user demographics are hard to come by.

³As noted above, the statute's pre-registration is unconstitutional, unenforceable and severable.

VIII. RSA 651-B:4-a Does Not Unconstitutionally Limit Anonymous Speech

Defendants argue that RSA 651-B:4-a unconstitutionally burdens anonymous speech.⁴ There is no doubt that the First Amendment and Article 22 provide solicitous protection for anonymous and pseudonymous speech. See e.g., Buckley v. American Constitutional Law Foundation, Inc., 525 U.S. 182 (1999) (striking down a statute that required persons circulating petitions to wear a name badge); Mortgage Specialists, Inc. v. Implode-Explode Heavy Industries, Inc., 160 N.H. 227, 237 (2010) (holding that the authors of internet posts and communications have a First Amendment right to retain their anonymity). This is so because anonymous and pseudonymous speech is necessary to maintain a free society. It will be recalled that the The Federalist Papers were published under the pseudonym "Publius." See also, Talley v. California, 362 U.S. 60, 64-65 (1960):

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . It is plain that anonymity has sometimes been assumed for the most constructive purposes.

See also, McIntyre v. Ohio Elections Commission, 514 U.S. 334, 341-42 (1995):

⁴The court understands that, absent burdensome and deliberate precautions, virtually none of what we do on the internet is truly anonymous. Law enforcement may obtain user account profile information, IP addresses and non-public content by warrant, judicial order or, in some cases, subpoena. Parties in civil litigation may be required to disclose the same information, to the extent it is in their possession, in discovery. Data brokers are aware of the details of our browsing history. Google is virtually omniscient as to our online comings, goings and doings. Nonetheless, through the use of pseudonyms and other online identifiers people can speak and listen over the internet in quasi-anonymity.

Great works of literature have frequently been produced by authors writing under assumed names. Despite readers' curiosity and the public's interest in identifying the creator of a work of art, an author generally is free to decide whether or not to disclose his or her true identity. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.

However, not all restrictions on anonymous speech violate the First Amendment and Article 22. See e.g., Mortgage Specialists (balancing the rights of defamation plaintiffs to seek redress for relief against the rights of internet posters to remain anonymous); John Doe No. 1 v. Reed, 561 U.S. 186, 218 (2010) (upholding a statute that made the identities of signers of a petition for a referendum a public record); Doe v. Shurtleff, 628 F.3d 1217 10th Cir. 2010) (upholding a statute that requires sex offender to disclose internet identifiers even though it placed some burdens on anonymous speech); But see, White v. Baker (holding that an overly broad internet identifier registration statute placed an unconstitutional burden on registrants' right to anonymous speech).

To apply these constitutional principles in this case the court must carefully analyze how RSA 651-B:4-a's provisions, as construed by the court, burden anonymous speech. The statute's restrictions on anonymity are subtle:

-RSA 651-B:4-a does not require disclosure of static IP addresses. Additionally, under the court's construction of the statute, registrants need not share online identifiers for websites or services that broadcast information, even if user comments are allowed.

Thus, registrants can anonymously read virtually any newspaper or blog and they can leave comments on any publication that allows the public to do so. Registrants can also anonymously read posts on bulletin boards that do not require a user account.⁵

-Under the court's construction of the statute, registrants do not have to disclose online identifiers for their own blogs or websites. Thus, they can quasi-anonymously publish and republish to the world whatever verbal, audio or video information they please. (However, if a registrant creates an online community that has, as a primary purpose, the facilitation of two-way, person to person communication, the registrant must report his online identifier for that website or service.)

- Further, registrants can restrict access to their websites to approved users. By doing so, registrants can stop the government from gaining access to the content posted on the website or service absent (a) probable cause and a warrant, (b) a judicial order or (c) an approved user who chooses to share.

-Registrants are free to anonymously visit public social media sites, to the extent that such websites or service allows for public browsing. For example, registrants need not sign up for a Twitter account in order to read Tweets.

-Registrants who report online identifiers for their social media accounts may, in most cases, either (a) restrict access to those accounts to the account holders'

⁵Web browsing is, for most of us, at best quasi-anonymous. Anybody who accesses a website shares certain information, such as his or her IP address, with the website operator. When combined with other information obtained by many websites via cookies, the website operator and/or third party data brokers may be able to presumptively identify the user or the user's online identifiers. This is why we see ads that are targeted to our browsing history when we read certain online publications. Yet, the government does not have access to this information without a warrant, judicial order or cooperation of the website operator/data broker.

approved “friends,” “followers,” or “network” and/or (b) block access to specified users. Thus, a registrant who does not want the government to see his Facebook page or Twitter feed, can make his accounts private.

- Nonetheless, RSA 651-B:4-a imposes some restraints on anonymous speech:

(A) By reporting their social media IDs, registrants effectively invite the government to review any social media postings that registrants make public. Thus, registrants cannot use social media to anonymously communicate with the world.

(B) Many social media accounts allow the public to view some limited information relating to non-public accounts. Thus, a registrant who places his Facebook page beyond the reach of anybody except for “friends,” still exposes to the government his list of “friends.” Therefore, RSA 651-B:4-a allows the government to keep track of registrants’ social media “friends,” “followers” and “network”

(C) If a government agent knows a registrant’s social media name, ID or handle, he can send the registrant a pseudonymous “friend” or “follower” request. A less than vigilant registrant could thus unwittingly allow the government agent into his non-public social media network.

(D) Registrants will need to disclose their membership or participation in online communities (if those communities have, as a primary purpose, the facilitation of two-way, person to person communication). Thus, registrants will need to let their local police department know if they join online communities devoted to controversial but lawful causes and pursuits, such as, by way of illustration, libertarian or socialist political beliefs, or efforts to reform marijuana laws, or non-mainstream religions.

(E) Government agents could use Google and/or private data brokers to search for any publicly available information connected to a registrant's email address and other online identifiers.

(F) Law enforcement may disclose a registrant's online identifiers to third parties or to the public for "a legitimate law enforcement purpose." RSA 651-B:7,1.

The court finds that RSA 651-B:4-a's restrictions on anonymous speech are narrowly tailored to promote significant government interests. The statute, as construed by the court, largely preserves rather than burdens the ability to speak and listen anonymously. Indeed, registrants who are subject to the statute have profoundly greater opportunities for anonymous speech than every human being who has lived prior to the late 1990s. As noted above, as construed by the court RSA 651-B:4-a's reach limited only to those spaces on the internet which are most likely to be used to

create person-to-person relationships. To the extent that registrants are significantly more likely than the general public to abuse such person-to-person relationships for criminal purposes (see, below), the requirement that registrants report online identifiers places no greater burden on anonymous speech than is necessary to further the State's legitimate interests.

The fact that law enforcement may disclose online identifiers to third parties or the public "for a valid law enforcement function," RSA 651-B:7, does not overburden anonymous speech. It is true that the statute does not define what constitutes "a valid law enforcement function." It is also true that the statute immunizes law enforcement agencies and officers from civil and criminal liability for good faith disclosures. RSA 651-B:7. However, registrants' online identifiers are not public records and are not published on the State's offender registry website. Id.

Nothing in RSA Chapter 651-B does—or could—allow law enforcement agencies and officers to retaliate against registrants for exercising their First Amendment rights. To establish a claim of First Amendment retaliation under 42 U.S.C. §1983 a plaintiff must show "(1) that the speech or conduct at issue was protected, (2) that the defendant took adverse action against the plaintiff, and (3) that there was a causal connection between the protected speech and the adverse action." Cossette v. Poulin, 573 F. Supp. 2d 456, 459 (D.N.H. 2008). See also, Gagliardi v. Sullivan, 513 F.3d 301, 306 (1st Cir. 2008); Pollack v. Regional School District Unit 75, 12 F. Supp. 3d 173, 188 (D. Me. 2014). In this context, "an adverse action . . . one that viewed objectively would have a chilling effect on the plaintiff's exercise of First Amendment rights[.]"

Pollack, 12 F. Supp. 3d at 188 (internal quotation marks, bracketing and ellipsis omitted), quoting Barton v. Clancy, 632 F.3d 9, 29 and n. 19 (1st Cir.2011). See also, D.B. ex rel. Elizabeth B. v. Esposito, 675 F.3d 26, 43 (1st Cir. 2012).

The First Amendment retaliation doctrine, which may be enforced by registrants under §1983, thus limits law enforcement discretion under RSA 651-B:7. Neither the First Amendment nor Article 22 requires anything more limiting than this.

For all of these reasons the court concludes that RSA 651-B:4-a not unconstitutional to the extent that it restricts anonymous speech.

IX. RSA 651-B:4-a Might Be Unconstitutional As Applied
To Particular Registrants But The Only Remedy
For Such Registrants Is Individualized Prospective Judicial Relief

Defendants next argue that RSA 641-B:4-a violates the First Amendment and Article 22 because it applies across the board to all persons convicted of specified offenses, without any individualized determination of actual dangerousness. Defendants have a point. An 18 year old who committed a felonious sexual assault against a peer in 2009 will be subject to the internet identifier registration statute in 2059, even though by then he may be an aging, long married accountant far more preoccupied with his mortgage bills and 401(k) than with anything of a sexual nature. A 21 year old who today has a non-forcible sexual relationship with a 15 year old, will still be subject to the registration in 2075, long after his own children first turned 15, then turned 21 and then turned 60 and retired. Defendant Bonacorsi proffered, but did not present expert testimony subject to cross-examination, the following facts:

. . . [E]xtensive 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. . . . [O]utside of the sex offender registry context,

states like New Hampshire . . . frequently use these tools to distinguish between sex offenders who pose a high risk to the public and those who do not. . . .

. . . Research also contradicts the popular notion that sexual offenders remain at risk of reoffending throughout their lifespan. Most sex offenders do not re-offend. . . . The longer offenders remain offense-free in the community, the less likely they are to re-offend sexually. . . . 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. 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 offense. 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. . . . The same is true for high-risk offenders after 17 years without a new arrest for a sex-related offense. . . . Ex-offenders who remain free of any arrests following their release should present an even lower risk. . . . Importantly, post-release factors such as cooperation with supervision and treatment can dramatically reduce recidivism, and monitoring these factors can be highly predictive.

Bonacorsi’s Motion To Dismiss, p. 11 (citations to affidavits omitted; emphasis in original).

At the oral argument on Bonacorsi’s motion to dismiss, the court opined that New Hampshire’s blanket, lifetime registration scheme might create haystacks with buried needles. The statute provides no means to differentiate between those who are actually dangerous (i.e. the needles in the haystacks) and those who statistically present no greater danger to the community than a group of non-sex offenders randomly selected from the phone book. As Bonacorsi suggested, without any dispute from the State, there are validated risk assessment tools that separate the needles from the hay, both with respect to an offender’s “static factors” (i.e. the unchangeable, historical facts relating to the offender) and the offender’s “dynamic factors” (i.e future-looking possibilities such as sex offender treatment).

However, even if these defendants proved beyond cavil that the internet identifier registration statute violated the First Amendment and Article 22 rights as applied to some registrants, this would not support a facial overbreadth challenge. As explained above, a statute may be successfully challenged as overbroad if it prohibits or unduly restricts a substantial amount of protected speech. In other words, an overbreadth challenge looks to the varieties of speech that are prohibited or burdened. The specific challenge here has nothing to do with the varieties of speech covered by RSA 651-B:4-a, but is rather limited to who may constitutionally fall within the statute's reach.

More important, the New Hampshire Supreme Court has already determined that, to the extent RSA Chapter 651-B cannot be constitutionally applied to a particular person, that person's sole remedy is to request prospective judicial relief from the statute's obligations. In Doe v. State, 167 N.H. 382 (2015), the Supreme Court held that RSA Chapter 651-B's registration requirements violated Part 1, Article 23 of the New Hampshire Constitution (which prohibits retrospective or *ex post facto* laws) to the extent that the statute applies to certain persons who were convicted of qualifying offenses prior to the effective date of various registration requirements. Thus, the court recognized that the registration statute could not be constitutionally applied to at least some registrants. Nonetheless, the court declined to simply release a class of registrants from their statutory obligations. Doe, 167 N.H. at 411. The court noted that such a blanket remedy "would produce unwarranted consequences" given the "legitimate and important public safety concerns" that underlie the registration statute. Id. Instead, the court held that an affected registrant must be "promptly given an opportunity for either a court hearing, or an administrative hearing subject to judicial

review, at which he is permitted to demonstrate that he no longer poses a risk sufficient to justify continued registration.” Doe, 167 N.H. at 411-412.

To the extent that the defendants may be correct in their belief that the First Amendment and Article 22 entitle some registrants to relief from the online identifier registration requirements in RSA 651-B:4-a, a Doe remedy would be appropriate. The alternative, baby-with-the-bath-water remedy proposed by defendants would nullify RSA 651-B:4-a with respect to all registrants, including recent high risk offenders who used online identifiers to commit multiple offenses against multiple victims.

A Doe remedy would give every registrant the opportunity to “opt-in” for a prompt due process hearing. This “opt-in” approach would ensure the procedural and substantive rights of any registrant who asks for a hearing. An “opt-out” regime, under which the State would be required to provide hearings to all registrants except those who waive the right to a hearing, would provide no greater protection to those who want hearings. At the same time an “opt-out” regime would place an enormous burden on the State.

Needless to add, a Doe hearing can only grant prospective relief. Therefore, until a registrant receives Doe-style relief from the obligations in RSA 651-B:4-a, he must continue to report his online identifiers. Put another way, neither of the defendants in these cases can litigate the issue of their own dangerousness in the context of these criminal enforcement proceedings.

X. RSA 651-B:4-a Does Not Infringe Registrants Freedom Of Association

Defendants argue that RSA 651-B:4-a unduly burdens their First Amendment and Article 22 right to association. Defendants rely primarily on NAACP v. Alabama, ex

rel. Patterson, 357 U.S. 449 (1958) which held that compelled disclosure of the NAACP's membership lists violated the constitutional right of its members to associate with each other for social advocacy. As the Supreme Court noted "Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." NAACP, 357 U.S. at 462. See also, Bates v. City of Little Rock, 361 U.S. 516 (1960); Gibson v. Florida Legislative Investigation Committee, 372 U.S. 539 (1963).

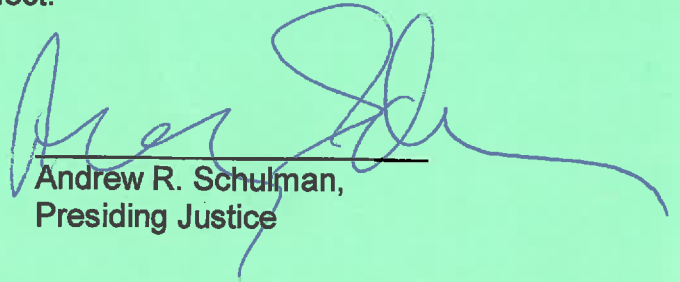
This case presents markedly different facts than the civil rights era cases cited above. RSA 651-B:4-a is not directed at any organization, type of organization or viewpoint. It is viewpoint neutral. Also, the statute does not require the disclosure of any organization's membership list. That said, by forcing registrants to disclose their affiliation with various online communities, RSA 651-B:4-a does impose a burden on their right to association.

However, for the reasons set forth above, as construed by the court RSA 651-B:4-a's compelled disclosure of online identifiers used for associational purposes is narrowly tailored to the government's significant interest. Therefore, the statute survives intermediate scrutiny with respect to defendant's freedom of association claims.

XI. CONCLUSION

For the reasons set forth above, the indictments in these cases are **DISMISSED WITHOUT PREJUDICE**. The order of dismissal is **STAYED** for thirty days to allow the State to appeal while all bail conditions remain in effect.

May 18, 2016



Andrew R. Schulman,
Presiding Justice