
February 5, 2018

VIA EMAIL

The Honorable Janet Ancel, Chair
House Committee on Ways & Means
Vermont State House
115 State Street
Montpelier, VT 05633-5301

**Re: Constitutional Problems with H.764**

Dear Madame Chair:

On behalf of the Software and Information Industry Association, I am writing to express our opposition to H. 764, entitled "An act relating to data brokers and consumer protection." The bill is constitutionally defective and violates both the First Amendment and the Commerce Clause of the U.S. Constitution.

SIIA is the principal trade association of the software and information industries and represents over 800 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment. SIIA's members range from start-up firms to some of the largest and most recognizable corporations in the world.

Our members include publishers of business-to-business and business-to-consumer products in both digital and print form, as well as financial news services, software companies, and database providers. Through their independent news-gathering and publishing activities, SIIA members inform businesses, journalists and governments on a wide variety of activities.

The bill requires "data brokers" to register with the state, and to comply with certain security standards. (H. 764, at 29-30 (registration); id. at 31-37 (security and notice). The legislation defines "data broker" as a "business that collects and sells to one or more third parties the personal information of a consumer with whom the business does not have a direct relationship." (page 9, lines 2-10). Personal information," in turn, is defined as digitally

stored elements, including name, address, family member, date of birth or other "indirect identifier," and other information "that is linkable to the consumer … that would allow a reasonable person to identify the consumer with reasonable certainty." (page 12 lines 1-13). The definition has no exclusion for public figures.

The bill deals with "personal information" in a few different ways. First, it forbids the acquisition of personal information by fraudulent means. (page 14). Second, it requires "data brokers" to register annually if they collect and sell "personal information" of "a Vermont consumer" (pages 29-31). As part of that registration, the data broker must provide information about: (a) the consumer's ability to opt-out of the collection or sale of personal information, (b) the data collection or data sales activities for which consumer cannot opt out from, (c) whether the data broker has a customer credentialing process, (d) the number of data broker security breaches (i.e., breaches involving the acquisition of personal information) the data broker experienced in the previous year, and (d) a separate statement identifying collection practices if personal information concerning minors is involved. (pages 29-31). Finally, the bill requires the data broker to implement operational and technical security measures to protect any personally identifiable information that holds (pages 32-37).

The practical operation of the statute is as follows. A person who lawfully acquires and sells the name—or other undefined and indeterminate kind of information--relating to a single "Vermont consumer" becomes a "data broker" and is required to register with the state. That "Vermont consumer" could either be a Vermont resident, or a non-resident who happened to purchase something in Vermont or, in the case of an online transaction, from Vermont. By its terms, the bill—including its notice and security provisions apply no matter where the "Vermont consumer" is located.

The bill has problems that will lead to litigation, uncertainty and—ultimately—judicial invalidation. First, the bill unconstitutionally burdens the publication of lawfully acquired, accurate information. Second, the bill improperly attempts to impose obligations based on conduct that occurs entirely outside the border of the state.

## I. The Bill Violates the First Amendment

SIIA members include a number of different business-to-business and specialized publications that, among other things, contain the "names" and other information of people with whom publishers and others have no business relationship. The same is true, of course, of online newspapers containing obituaries, online directories of lawyers, politicians, or Academy Awards winners as well as potentially any number of digitally published works—like an e-book of a biography. Any piece of information is "linkable" to a consumer. Under the plain language of the bill, publishers of such information must register with the government and provide a host of information about their business practices. If our members desire to sell a directory of the names of vending machine salesmen, or of Republican or Democratic politicians in the Northeast Kingdom, the Constitution does not require them to do that—before, during, or after that sale.

### A. "Personal Information" is protected speech.

Under the First Amendment, publishers of lawfully acquired factual information are not required to register with the government. The dissemination of lawfully acquired, factual information is protected speech. "[I]f the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of expressive conduct" (some internal quotation marks omitted)). Bartnicki v. Vopper, 532 U.S. 514, 527 (2001). The Court's decision in Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) rejected this State's argument that dry information lacks First Amendment protection, even when all that information consists of is marketing data. This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment. See also, e.g., Rubin v. Coors Brewing Co., 514 U.S. 476, 481 (1995) ("information on beer labels" is speech); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759 (1985) (plurality opinion) (credit report is "speech").

The speech covered in this legislation is broader than that covered by the statute invalidated in Sorrell. Examples of activity covered by the definition of "data broker" includes:

- A private investigator hired to determine who a particular subject of an investigation is meeting.

- Any website that sells directories of people who are not their "customers."

- Newspapers that publish pictures and descriptions of people who are "not their customers".

- Web sites that identify political donors from their lobbying registrations.

- Persons who sell access to directories of politicians, regulators and their staffs including names, emails, districts, and phone numbers for purposes of political activity.

**B. The legislation is not tailored to any defined privacy interest.**

To the extent that the legislation covers public figures and other kinds of information, it is patently unconstitutional. Even assuming arguendo that the legislation could be tailored to involve only material about individuals not in the public eye, the transmission of such data still receives First Amendment protection. Accordingly, "it is the State's burden to justify its content-based law as consistent with the First Amendment," and the State must show at least that the statute directly advances a substantial governmental interest and that the measure is drawn to achieve that interest. Sorrell v. IMS Health Inc., 564 U.S. 552, 571–72 (2011) (internal citations and quotations omitted).

The legislation lacks the tailoring necessary to render it constitutional. The authors seem primarily concerned with the concept that some information may, at some unknown time and through an unknown means, be used for a purpose that the government finds undesirable—such as a privacy violation or identity theft. (H. 764, pp. 2-3). The government is then ostensibly deciding to impose not only a registration requirement, but make the registrant provide a number of items of information.

That background presents insurmountable problems for the constitutionality of this statute, as it cannot reasonably said to be narrowly drawn to the interests it ostensibly protects. First, vague claims of privacy will not sustain a statute from constitutional attack. E.g., U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999) (noting that the government cannot pass First Amendment scrutiny "by merely asserting a broad interest in privacy. … [Th]e specific privacy interest must be substantial, demonstrating that the state has considered the proper balancing of the benefits and harms

of privacy. In sum, privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.").

Even permitting the state to claim some vague and undefined interest in privacy, the bill's provisions lack tailoring as the definition is both heavily over-and-under inclusive. The definition of "personal information" excludes direct customer lists, which can be sold without registration and which contain information that actually identifies individuals—information that could be far more damaging to privacy. On the other hand, it sweeps in news stories, lists of politicians, and any other information that is "linkable" to an individual, even when the information is a matter of public interest. In addition to being overbroad, the bill provides no way for a First Amendment speaker to know when its responsibility begins and ends.

Finally, SIIA notes that the registration requirement's compelled disclosure of opt-out policies and similar requirements seem to be the first step towards even more broader and invasive legislation. There is no suggestion in the U.S. Supreme Court's case law that the First Amendment contains a "right to be forgotten," whereby the government can ban the publication of "personal information" and censor its transmission. Instead, the courts recognize a broad First Amendment right to transmit lawfully acquired, accurate information and the government may not generally censor the publication of particular kinds of information without meeting strict judicial scrutiny. See City of Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 429 (1993).

## II. The Bill Violates the Commerce Clause

The federal commerce clause (U.S. Const. Art. I, sec. 3., cl. 3) grants Congress the affirmative power to regulate interstate commerce. In addition to giving Congress an affirmative grant of power, the Commerce Clause also constrains the ability of the states to legislate across state lines. A state statute will fail Commerce Clause scrutiny if it directly regulates or discriminates against interstate commerce, or when it has a protectionist effect. See Brown-Forman Distillers Corp. v. New York State Liquor Auth., 476 U.S. 573, 579 (1986); Am. Booksellers Found. v. Dean, 342 F.3d 96, 102 (2d Cir. 2003).

The problem with H.B. 764 is not protectionism, but extraterritorial reach. "A statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature." Healy v. Beer Inst., Inc., 491 U.S. 324, 337 (1989) (citing Brown-Forman, 476 U.S., at 579). The key aspect is its "practical effect, which must be evaluated by "considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation." Id. at 336 (internal citations and quotations omitted).

Here, the bill's notice and registration requirements apply to the sale of the name "personal information" of a "Vermont consumer." The sale that triggers registration need not take place in the state—even one name or email triggers the obligation to register and provide notices. Indeed, it need not identify a particular consumer at all—it need only be "linkable" to the consumer. (H. 764, p.12, lines 12-13). Thus, companies could violate the statute by transferring "personal information" even without having any idea to whom the information actually belonged or their relationship with the State. First Amendment problems with this arrangement aside, the Commerce Clause problems with such a scheme are obvious and fatal. Were every state to pass such a law, publishers of information would be subject to competing and irreconcilable notice, security and other requirements. Under this bill, "the rest of the nation is forced to comply with its regulation or risk prosecution." Am. Booksellers Found, 342 F.3d at 103. The Commerce Clause prohibits exactly that result.

**Conclusion**

SIIA does not gainsay the state's ability to protect personal privacy in specific situations, especially when the misuse of specific information directly results in readily ascertainable tangible harm. The first line of defense (and one subject to lower levels of constitutional scrutiny) involves penalizing misuse. If personal information is being used to stalk individuals, then the state is well within its rights to prohibit stalking and information fraudulently acquired for that purpose.

But H.764 goes much further. In the name of protecting undefined privacy concerns, it unconstitutionally burdens SIIA members' dissemination of First Amendment-protected speech, and does so in a way that conflicts with Commerce Clause jurisprudence. We oppose its enactment, and urge members of the legislature to vote against the bill.

Should you wish to discuss the issues we have raised further, please do not hesitate to contact me.

Respectfully submitted,

Christopher A. Mohr

Vice President for Intellectual Property
and General Counsel

Cc: Hon. Maxine Grad, Chair, House Judiciary Committee and Committee Members

Hon. William Boztow II, Chair, House Committee on Commerce and Economic Development, and Committee Members.