Mayer Brown LLP
333 S. Grand Ave 47th Floor
Los Angeles, CA 90071-1575
United States of America

T: +1 213 229 9500
F: +1 213 625 0248

mayerbrown.com

**Philip Recht**
Partner
T: +1 213 229 9512
F: +1 213 576 8140
PRecht@mayerbrown.com

April 30, 2026

BY EMAIL

**Senate Committee on Economic Development, Housing and General Affairs**
c/o Ciara Mead, Committee Assistant
Ciara.Mead@vtleg.gov

**House Committee on Commerce and Economic Development**
c/o Kira Ecay, Committee Assistant
KEcay@leg.state.vt.us

115 State Street
Montpelier, VT 05633-5301
(802) 828-2228

Re: Senate Bill 71/House Bill 211

Honorable Committee Members:

Our firm represents a coalition of companies (i.e., Spokeo, PeopleFinders, BeenVerified, Truthfinder, Instant Checkmate, Classmates, Intelius) that provide background check, fraud detection, and other people search services.

We write regarding H211 (currently before the Senate Economic Development Committee), which would amend portions of the Data Broker Registry Law, 9 Vt. Stat. Ann. § 2446 (the "Registry Law") to, among other things, establish an accessible deletion mechanism by which consumers can request deletion of their personal data by registered data brokers. We have just one concern with H211, a limitation on the definition of "publicly available information" (PAI) that threatens the bill's constitutionality and creates (presumedly unintended) conflicts with S71 (currently before House Commerce), the proposed Vermont Data Privacy Act (the "Act"), and comparable laws in other states. These constitutional concerns would be resolved by harmonizing H211's definition of PAI with the definition in S71, as we explain below.

**I. Our clients.** Like others in the data industry, our clients collect data mostly from publicly available sources, such as phone books or directories, real property records, court records, consumer indices, and vital statistic. Our clients then organize the public data into usable products (such as reports), and offer the reorganized data for sale to customers.

Our clients' services are widely used and highly valued by an array of public and private entities and individuals. Welfare agencies use the services to find parents evading child support awards.

Mayer Brown is a global services provider comprising an association of legal practices that are separate entities including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian partnership).

Government and law enforcement agencies use the services to locate victims, suspects, constituents, beneficiaries, and witnesses, and to serve subpoenas. Businesses use the services to find, update, or verify contact information for prospective, current, or former customers, and to prevent e-commerce order fraud. Most of all, consumers use our clients' services for a wide range of reasons, for example: to locate lost friends and relatives, to reunite adoptees and birth parents, to verify the identity of persons met online, to identify who is behind unwanted calls or texts, to plan family reunions, and to root out scams.

**II. Our concerns with the Registry Law Amendments.** Our clients support the enactment of privacy laws like the Registry Law and Act. Clear and consistent data privacy practices not only protect consumers, but benefit businesses through enhanced consumer trust and stable compliance regimes. For these reasons, our clients have long voluntarily provided many of the consumer protections (e.g., opt out rights) that the Act would make mandatory and have been codified in a growing list of states beginning with California and Virginia, where we were involved in the generation of the laws.

Consistent with this approach, our comments are not meant to undermine the Registry Law or the Act, but rather to ensure the Act and Registry law amendments are compatible with one another, consistent with the laws of other states, and above all, constitutional.

"In numerous cases the [Supreme] Court has emphasized the importance to First Amendment values of a free flow of *public* information." *U.S. v. Jeter*, 775 F.2d 670, 678 n. 7(6th Cir. 1985) (emphasis in original) (citing cases). Both "the creation *and dissemination* of information are speech within the meaning of the First Amendment." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011) (emphasis added). Indeed, "if the acts of 'disclosing' and 'publishing' information do not constitute speech, it is hard to imagine what does fall within that category." *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001).

Sales plainly qualify as disclosures of free speech data, including sales of publicly available, personally-identifying information. The Supreme Court has held that "sales, transfer, and use of [personally]-identifying information are … speech for First Amendment purposes." *Sorrell*, 564 U.S. at 570; *see also Sarver v. Chartier*, 813 F.3d 891, 903 (9th Cir. 2016) (statute that restricts the commercial use of people's personal identifying information "clearly restricts speech based upon its content"). "[T]that circumstance is sufficient to justify applying heightened scrutiny, even assuming that [personally]-identifying information is a mere commodity." *Sorrell*, 564 U.S. at 570. The so-called "strict scrutiny test" requires that content-based restrictions of speech be narrowly tailored to promote a compelling government interest. *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000). As a general matter, "state action to punish the publication of truthful information seldom can satisfy constitutional standards." *Bartnicki*, 532 U.S. at 527 (quoting *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 102 (1979)).

In recognition of these principles, each of the 21 comprehensive data privacy laws enacted in the United States in the past decade have come to exclude PAI, which has at least three components grounded in First Amendment caselaw: (1) government records; (2) information made available to the general public by the consumer or from widely distributed media (e.g., a newspaper, TV or

radio program), and (3) information made available by a person to whom the consumer has disclosed the information without restriction to a specific audience (e.g., a public social media profile):

1. California Civ. Code § 1798.140(v)(2);
2. Colorado Rev. Stat. §§ 6-1-1303(17)(b), (23)(b)(V)(B);
3. Conn. Gen. Stat. § 42-515(33)
4. Delaware HB154 § 12D-102(28);
5. Florida SB 262 § 501.702(28);
6. Indiana SB 5, Ch. 2, § 1(26);
7. Iowa SB 262 § 1(24);
8. Kentucky HB 15 § 1(26);
9. Maryland SB541 § 14–4601(CC);
10. Minnesota HF4757 § 325O.02(p);
11. Montana SB 384 § (2)(22);
12. Nebraska § LB1074 2(28);
13. New Hampshire SB 255 §§ 507-H:1.XXVI, XXVII(e);
14. New Jersey S332 (definitions);
15. Oklahoma SB546 § 1.27;
16. Oregon SB 619 § 1(13)(b);
17. Rhode Island S2500 § 6-48.1-2(24);
18. Tennessee HB 1181 § 47-18-3201(24);
19. Texas HB 4 § 541.001(27);
20. Utah Code Ann. § 13-61-101(29).
21. Virginia Code § 59.1-571.

In addition to these state laws, the Uniform Law Commission, perhaps best known for developing the Uniform Commercial and Probate Codes, proposed its model privacy law in July 2021. The UPDPA contains a similar, though perhaps more illustrative, definition of PAI.[1] While Congress has not advanced a comprehensive data privacy law, federal proposals have contained similar definitions.[2] These various enacted, model, and proposed state and federal laws reflect a

[1] "'Publicly available information' means information: (A) lawfully made available from a federal, state, or local government record; (B) available to the general public in widely distributed media, including: (i) a publicly accessible website; (ii) a website or other forum with restricted access if the information is available to a broad audience; (iii) a telephone book or online directory; (iv) a television, Internet, or radio program; and (v) news media; (C) observable from a publicly accessible location; or (D) that a person reasonably believes is lawfully made available to the general public if: (i) the information is of a type generally available to the public; and (ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed." UPDPA § 2(15).

[2] "Publicly available information" means "any information that a covered entity has a reasonable basis to believe has been lawfully made available to the general public from (i) Federal, State, or local government records provided that the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity; (ii) widely distributed media; (iii) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public can log-in to the website or online service; (iv) a disclosure that has been made to the

comprehensive, consistent commitment to protect public data in accordance with the First Amendment. As the ULC explained, "[t]he processing of publicly available information is excluded from the act[s]" because "[t]here are significant First Amendment implications for placing limits on the use of public information." UPDPA, Sec. 3 cmt.

S71 is firmly in line with the national consensus,[3] and we have no quarrel with the Act. H211, however, diverges from consensus and thus from constitutional precedent. H211 would redefine the Registry Law's definition of "brokered personal information" (BPI) to exclude PAI, defined as "information that: (i) is made available: (I) through federal, state, or local government records; or (II) to the general public from widely distributed media; or (ii) a data broker has a reasonable basis to believe that the consumer has lawfully made available to the general public." Proposed Section 2430(16)(A). To that extent, H211 aligns with S71, other state laws, and the First Amendment.

But under H211, proposed Section 2430(16)(B), PAI would not include:

> "(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge; (iii) information that is made available for sale; (iv) an inference about a consumer that is generated from the information described in subdivision (ii) or (iii) of this subdivision (16)(B)."

Effectively, H211 would strip public information of its public character merely because the information is combined, collated, or sold—or inferred from otherwise public information combined, collated, or sold. Respectfully, there is no precedent for such a restriction in data privacy law or First Amendment jurisprudence. On the contrary, the Supreme Court has confirmed as recently as 2024 that the "First Amendment offers protection when an entity engag[es] in … compiling and curating" free-speech data, such as publicly available information. *Moody v. NetChoice, LLC*, 603 U.S. 707, 731 (2024).

Not only does public data retain its free-speech character when collated or compiled, but the "compilation … is expressive activity of its own," protected by the First Amendment. *Id.* This is "true [even] when the content comes from third parties." *Id.*; *see also Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557, 570 (1995) ("the presentation of an edited compilation of speech generated by other persons … fall[s] squarely within the core of

---

general public as required by Federal, State, or local law; or (v) a visual observation of an individual's physical presence in a public place by another person, not including data collected by a device in the individual's possession." ADPPA, H.R. 8152 § 2(23).

[3] S71 excludes from the definition of personal data "publicly available information," defined as: "information that: (A) is lawfully made available through federal, state, or local government records or widely distributed media; or (B) a controller has a reasonable basis to believe that the consumer has lawfully made available to the general public." Proposed Section 2415(33). The "sale of personal data" likewise is defined to exclude "the disclosure of personal data that the consumer: (I) intentionally made available to the general public via a channel of mass media; and (II) did not restrict to a specific audience." Proposed Section 2415(37)(B)(v).

First Amendment security"). "When the government interferes with such … compilation," it "confronts the First Amendment" and must satisfy strict scrutiny. *Moody*, 603 U.S. at 731-32.

A general interest in privacy cannot justify limiting First Amendment rights. *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999) (compelling government interest cannot simply be a general interest in privacy). More emphatically, "the government cannot get its way just by asserting an interest in improving, or better balancing, the marketplace of ideas." *Moody*, 603 U.S. at 732. As the Supreme Court has explained, "it is critically important to have a well-functioning sphere of expression, in which citizens have access to information from many sources," particularly, public sources. *Id.* "That is the whole project of the First Amendment." *Id.*

When regulating free speech data, therefore, the government must specifically articulate, and then justify, the goals it is trying to achieve. H211 does not specify its goals. We presume both H211and H71 aim to give consumers enhanced control and choice regarding their private data and to prevent identity theft and other misuse—laudable goals all. But those aims do not and cannot justify the blanket regulation of non-confidential, public-domain data, whether compiled, collated, sold, or inferred therefrom.

Indeed, indirect data collectors such as our clients do not exploit customer relationships or confidences when they organize data acquired from public phone directories, media outlets, search engines, and other widely available sources. Nor do they imperil an individual's safety, security, or reputation by redistributing data that is already in the public domain.

But by including public data in its broad sweep—simply because the data is combined, collated, sold, or inferred—H211 is not narrowly tailored to promote any legitimate and justified goals. This failure puts the entire bill at risk of invalidation. *See United States v. Stevens*, 559 U.S. 460, 473 (2010) ("In the First Amendment context, … a law may be invalidated as overbroad if a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly legitimate sweep.").

Removing proposed Section 2430(16)(B)(ii)-(v), or substituting S71's PAI definition, would address this legal deficiency without leaving consumers unprotected. H211's definition of "brokered personal information" covers an array of data that generally is not publicly available and, as such, would still be subject to regulation. Moreover, consumers who wish to keep their data confidential, particularly on social media sites, still could do so by marking their posts and profiles private. And S71, if passed, would give consumers even more rights with respect to their personal data.

In the end, companies like our clients simply allow data already in the public domain to be used more efficiently by consumers, businesses, news organizations, law enforcement, governments, and others—that is to say, *by the public*. The First Amendment protects such dissemination and so too must laws and rules respecting data privacy. We presume H211 was modeled on California's recently enacted Delete Act (CA 2023 SB 362), which amended the California Data Broker Registry law (Cal. Civ. Code § 1798.99.80 *et seq.*) to include an accessible deletion mechanism (referred to as "DROP"). The California Delete Act, however, incorporates the

California Privacy Rights Act's full definitions of personal and publicly available information, without any limitation on data combined, collated, sold, or inferred. *See* Cal. Civ. Code § 1798.99.80(a).

Respectfully, H211 should do the same. The constitutional infirmity in H211 can be addressed in one of three ways:

1. Strike subdivisions (ii), (iii), and (vi) from proposed subdivision 2430(16)(B):

   (B) "Publicly available information" does not include:
   (i) biometric data collected by a business about a consumer without the consumer's knowledge;
   ~~(ii) information that is collated and combined to create a consumer profile that is made available to a user of a publicly available website either in exchange for payment or free of charge;~~
   ~~(iii) information that is made available for sale;~~
   ~~(iv) an inference about a consumer that is generated from the information described in subdivision (ii) or (iii) of this subdivision (16)(B);~~
   (~~v~~ii) any obscene visual depiction, as defined in 18 U.S.C. § 1460; (vi) brokered personal information that is created through the combination of brokered personal information with publicly available information;
   (~~vi~~iii) genetic data, unless otherwise made publicly available by the consumer to whom the information pertains;
   (~~vii~~iv) information provided by a consumer on a website or online service made available to all members of the public, for free or for a fee, where the consumer has maintained a reasonable expectation of privacy in the information, such as by restricting the information to a specific audience; or
   (v~~ix~~) intimate images, authentic or computer-generated, known to be nonconsensual.

2. Substitute S71's definition of PAI (proposed § 2415(33)) for H211's definition; or

3. Incorporate S71's definition of PAI into H211 by reference.

The latter approach has the added benefit of ensuring maximum consistency between the two data privacy laws and other state enactments, including in the event the Act is ever amended in the future.

**III. Conclusion.** We hope this information is helpful. Please let us know if you have any questions about it. Otherwise, we would welcome the opportunity to speak to you further about the issues discussed herein.

Yours sincerely,

Philip Recht
Partner