MAYER | BROWN

Mayer Brown LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071-1503
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 2, 2024

BY EMAIL

Senator Kesha Ram Hinsdale
115 State Street
Montpelier, VT 05633-5301
(802) 334-6302
mmarcotte@leg.state.vt.us

Re: House Bill 121/Vermont Data Privacy Act

Dear Senator Hinsdale:

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 House Bill 121, now pending before the Senate Committee on Economic Development, Housing and General Affairs which you chair, which would enact the Vermont Data Privacy Act (the "Act") and amend portions of the Data Broker Registry Law, 9 Vt. Stat. Ann. § 2446 (the "Registry Law"). We have no concerns with the proposed Act itself, but rather wish to address what we expect were unintended conflicts between the Act and the Registry Law amendments. We would welcome the opportunity to discuss these and any related issues.

I. Our clients. As noted, our clients provide background check, fraud detection, and other people search services. They do so, like others in the data industry, by collecting data mostly from publicly available sources, organizing the data into usable products (such as reports), and offering the reorganized data for sale to customers. Unlike businesses that collect personal information directly from consumers, our clients collect information only from third-party sources.

Our clients' services are widely used and highly valued by any array of public and private entities and individuals. Law enforcement agencies use the services to serve subpoenas and to identify and locate witnesses and suspects, for example, the prime suspect in the now-infamous Idaho university murders (see https://www.dailymail.co.uk/news/article-11592371/How-Idaho-cops-used-genetic-genealogy-trace-suspect-Bryan-Kohbgergers-distant-relatives.html, Part 4). Welfare agencies use the services to find parents evading child support awards. The Veterans Administration uses the services to locate next-of-kin of fallen soldiers. Businesses use the services to detect order fraud and update customer and prospect databases. And consumers use the services to find lost relatives and friends, plan family reunions, check out relationship and service-provider prospects, and root out scams.

II. Our concerns with the Registry Law amendments. Our clients support the enactment of privacy laws like the 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.

Consistent with this approach, our comments below are not meant to undermine the Act. Indeed and as mentioned, we have no quarrel with the Act itself. Rather, our comments are meant to ensure the Act and Registry Law amendments are compatible and that the resulting laws are legally compliant, operationally sound, and consistent with the laws of other states.

A. Individual Opt-Out. H121, at proposed Section 2448(a), would grant consumers a right of "individual opt-out" vis-à-vis data brokers, by which "[a] consumer may request that a data broker do any of the following: (A) stop collecting the consumer's data; (B) delete all data in its possession about the consumer; or (C) stop selling the consumer's data." This provision is both redundant of similar provisions in the Act and otherwise impossible to comply with. These flaws are not present in the Act, which mirrors other states laws by providing a workable deletion solution.

To understand the problems with the individual opt-out, it helps to understand the practice of indirect data collection and the history of state laws regulating the same. Companies that collect personal data directly from consumers can readily and confidently meet a deletion requirement. Upon receiving a consumer request, such companies can simply delete the consumer's data in its entirety from their databases and stop collecting from consumers. Since the consumer is the only source of the data, the companies need not worry about the consumer's data reappearing in their databases in the future, unless the consumer herself re-engages the company.

In contrast, companies that collect data from third party sources cannot fully, feasibly, or confidently comply with a deletion request. The reason is that such companies generally do not *collect* consumer data on a one-time-only basis. Instead, they *receive* data on an ongoing, repetitive basis from an array of sources to ensure that the data remains up-to-date and accurate (again, for the benefit of businesses and consumers). Typically, these sources send new, updated data flows to the company on a monthly, if not weekly, basis. Unless the sources themselves have deleted the consumer's data, the consumer's data is included in these new data flows.

Given these operational realities, it is *impossible* for indirect data collectors—data brokers—to "stop collecting the consumer's data," as H121 currently would require. Moreover, the requirement that a data broker "delete all data in its possession about the consumer" presents a Hobson's Choice for indirect collectors.

On the one hand, indirect collectors could honor a consumer's request when received by deleting the consumer's data entirely. However, within weeks, if not days, the consumer's data would once again be sent to their databases and companies like our clients, having deleted any prior

record of the consumer, would have no way to identify the new data for deletion. In this scenario, the companies would be technically compliant with the consumer's deletion request, but the impact would be only momentary. The consumers, meanwhile, would have no way to know their deletion was only temporary, making the deletion right illusory. If the consumer somehow learned the deletion was only temporary, the consumer would have to return to the indirect collectors, again and again, to ensure thorough and lasting deletion. Clearly, these are not consumer-friendly scenarios.

Alternatively, companies such as our clients could attempt to ensure ongoing deletion by retaining enough of the consumer's data to allow them to identify and re-delete the later-acquired data. That, or such companies could refrain from processing the received data in any way. But, in these scenarios, the companies would not have technically and fully complied with the consumer's deletion request and, thus, could be in violation of the law. Few companies would be willing to take on that risk, even if doing so better serves consumers and promotes consumer goodwill.

States enacting comprehensive data privacy laws such as the Act have generally adopted one of two solutions to problem. Several states have limited deletion obligations to direct collection ("data collected from the consumer"). See Cal. Civil Code sec. 1798.105(a); Iowa SB 262 § 3(1)(b); Utah Code Ann. § 13-61-201(b)(2).[1] Other states addressed the deletion issue by providing indirect collectors two separate compliance options: retain, but do not otherwise use, minimal data to ensure deletion of later-received data (often called "suppression") or opt the consumer out of processing for all but exempted purposes. See Virginia Code § 59.1-577.B.5; Connecticut Public Act No. 22-15 § 4(a)(5); Colorado Rule 904-3-4.06(E); Montana SB 384 § (1)(e); Tennessee HB 1181 § 47-18-3203(a)(2)(C); Florida SB 262 § 501.706(6); Texas HB 4 § 541.052(f); Oregon SB619 § 4(7)).

This alternative provision was a classic win-win. It resolved the Hobson's Choice discussed above by allowing indirect collectors to retain enough data to perpetually and perennially delete a consumer's data or to opt that data out of processing. At the same time, it ensured that the consumer's desire to stop the further use and circulation of his/her data was honored, within the reality that indirect collectors cannot stop collecting since they do not collect directly in the first place.

Indeed, the Act portion of H121 includes the alternative adopted in the majority of states and thus addresses the concerns outlined above. But H121 goes further and provides the individual opt-out in the Registry Law amendments, without any corresponding alternatives. Put simply, the individual opt-out is redundant and unnecessary, given that rights of deletion and opt-out exist in

[1] The Uniform Law Commission (ULC)—the collection of retired judges, law professors, and practicing attorneys best known for developing the Uniform Commercial and Probate Codes—omitted a deletion requirement altogether from its model state privacy law, the Uniform Personal Data Protection Act (UPDPA), citing "a wide range of legitimate interests on the part of collectors that require data retention" and the fact that it is "difficult given how data is currently stored and processed to assure that any particular data subject's data is deleted." UPDPA § 4, cmt.

the Act, which would apply to all data brokers. All the individual opt-out adds is the right to request data brokers "stop collecting" data, but as explained, that right is inapposite and impossible to perfect when applied to data brokers, who by their very definition and practice do not collect data directly from consumers.

For all of these reasons, we respectfully request that the individual opt-out be stricken from H121 or, at the least, that proposed Section 2448(a) be amended to conform to the Act as follows:

> § 2448(a) Individual opt-out.
>
> (1) A consumer may request that a data broker do any of the following:
>
> (A) ~~stop collecting the consumer's data;~~
>
> ~~(B)~~ delete all data in its possession about the consumer **in accordance with Subdivision 2418(c)(5) of Chapter 61A**; or
>
> (~~C~~B) stop selling the consumer's data.

C. Publicly Available Information. In addition to the individual opt-out, H121 also includes a "General Opt-Out," by which consumers may file a request with the Secretary of State, who will create an opt-out list to be regularly accessed and honored by all registered data brokers. Proposed Section 2448(b). In effect, the general out-out (like the individual opt-out) adds new restrictions on dissemination and sale to the Registry Law, which previously had required registration only. In this way, the Registry Law amendments are similar to 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 a general deletion mechanism to be administered by state agency and regularly accessed by data brokers.

The amendments to Section 2448, however, continue to rely on the Registry Law's original definition of "brokered personal information" (BPI), creating a constitutional and potentially fatal flaw in the individual and general opt-outs. Specifically, the BPI definition, unlike the Act's proposed definition of "personal information," fails to exclude publicly available information, which is free speech protected by the First Amendment. This flaw, if left unattended, could render not only the BPI definition, but the entirety of H121 vulnerable to challenge and invalidation.

The First Amendment prohibits laws that abridge freedom of speech. Commercial speech—i.e., speech that proposes a commercial transaction (e.g., a billboard advertisement)—may be limited by laws that are necessary to directly advance a substantial government interest. *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566 (1980). However, content-based restrictions on non-commercial speech, such as H121's proposed limitations on the use of consumers' personal information (including the data reports provided by our clients), are presumptively unconstitutional and may only be allowed if they meet the so-called "strict

scrutiny test"—i.e., are narrowly tailored to promote a compelling government interest. *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000); *see also Sarver v. Chartier*, 813 F.3d 891, 903 (9th Cir. 2016) (holding that statute that restricts the commercial use of people's personal identifying information "clearly restricts speech based upon its content"). Special First Amendment protection is afforded speech involving truthful information on matters of public concern. *See*, *e.g.*, *Connick v. Myers*, 461 U.S. 138, 147 (1983); *New York Times Co. v. Sullivan*, 376 U.S. 254, 279-80.

The Act recognizes these principles but excluding from the definition of personal data, proposed Section 2415(18)(B), "publicly available information," defined as: "information that: (A) is lawfully made available through federal, state, or municipal government records or widely distributed media; and (B) a controller has a reasonable basis to believe a consumer has lawfully made available to the general public." Proposed Section 2415(43). 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(48)(C)(v).

These definitions are in line with each and every other comprehensive data privacy law passed in the United States in the past five years—fifteen bills total. See **California** Civ. Code § 1798.140(v)(2); **Colorado** Rev. Stat. § 6-1-1303 (23)(b)(V)(B); **Connecticut** Public Act No. 22-15 §§ 1(25)-(26); **Delaware** HB 154 § 12D-102(28); **Florida** SB 262 § 501.702(28); **Indiana** SB 5, Ch. 2, § 1(26); **Iowa** SB 262 § 1(24); **Montana** SB 384 § (2)(22); **New Hampshire** SB 255 §§ 507-H:1.XXVI, XXVII(e); **New Jersey** S332; **Oregon** SB 619 § 1(13)(b); **Tennessee** HB 1181 § 47-18-3201(24); **Texas** HB 4 § 541.001(27); **Utah** Code Ann. § 13-61-101(29); **Virginia** Code § 59.1-575.[2]

In addition to the state laws, the ULC's UPDPA contains a similar, though perhaps more illustrative, definition of publicly available data.[3] The UPDPA's drafters explained in comments to the model law that "[t]he processing of publicly available information is excluded from the act" because "[t]here are significant First Amendment implication for placing limits on the use of public information." Sec. 3 cmt. In additional, the recently proposed bipartisan American Data

[2] A sixteenth bill, Kentucky HB 15, awaits signature by the governor and treats publicly available information in like fashion.

[3] "'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).

Privacy and Protection Act (ADPPA), H.R. 8152, similarly exempted and defined "publicly available information."[4]

These various enacted, model, and proposed state and federal laws reflect a comprehensive, consistent commitment to balance legitimate privacy interests with paramount First Amendment freedoms.

The Registry Law's definition of BPI excludes publicly available information (undefined therein), but only "to the extent that it is related to a consumer's business or profession." 9 Vt. Stat. Ann. § 2430(2)(B). That approach may have been appropriate in a registration-only law. But H121's Registry Law amendments go beyond mere registration, restricting the collection, processing, and sale of personal data through individual and general opt-outs. In so doing, H121 triggers constitutional strict scrutiny (*see Sarver*, 813 F.3d at 903), as did California's Delete Act. The Delete Act, however, incorporates the definitions of personal and publicly available information in the California Privacy Rights Act, cited above. *See* Cal. Civ. Code § 1798.99.80(a).

Respectfully, we recommend and request that H121's Registry Law amendments be revised in like fashion, eliminating the "business or profession" proviso and incorporating the Act's definition of publicly available information. This simple yet meaningful change would align the Registry Law with the Act and align both laws with all other states to have passed or enacted comprehensive data privacy laws. More importantly, it would eliminate a significant and potentially fatal legal risk inherent in H121.

H121 did not specify its goals or purposes, but 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; rather, the government must specifically articulate, and then justify, the goals it is trying to achieve). Even assuming H121 aims to give consumers enhanced control and choice regarding their private data, and to prevent identity theft and other misuse—laudable goals all—those aims do not justify the regulation of non-confidential, public-domain data.

Indeed, indirect data collectors such as our clients do not exploit customer relationships or confidences by acquiring data from public phone directories, media outlets, search engines, and other widely available sources. Nor do they imperil an individual's safety, security, or reputation

[4] Publicly available information includes "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 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 § 2(23).

by redistributed data that is already in the public domain. But by including public domain data in its broad sweep, H121 is not narrowly tailored to promote its legitimate and justified goals, putting the entire bill at risk. *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.").

While updating the BPI definition will address this legal deficiency, it will not leave consumers unprotected. H121's definition of "personal information" covers an array of data that generally is not publicly available and, as such, would still be subject to regulation. Further, even with an expanded scope of exempt public data, consumers who wish to keep their data confidential, on social media sites, for example, still would be able to do so by designating their profiles and posts as private, as opposed to public.

In the end, companies like our clients that redistribute data that already is public simply allow that data to be used more efficiently by consumers, businesses, news organizations, law enforcement, governments, and others. The First Amendment protects such dissemination. H121's failure to fully exempt publicly available data threatens this protection and puts the entire bill at risk of invalidation.

For all these reasons, we urge that H121 be amended as follows. Proposed Section 2430(2)(B) should be amended to read:

> "Brokered personal information" does not include publicly available information**, as that term is defined in section 2415(25) of this title** ~~to the extent that it is related to a consumer's business or profession~~.

And proposed Section 2430(7)(D) should be revised to read:

> The phrase "sells or licenses" does not include:
>
> (i) a one-time or occasional sale of assets of a business as part of a transfer of control of those assets that is not part of the ordinary conduct of the business; ~~or~~
>
> (ii) a sale or license of data that is merely incidental to the business~~.~~**; or**
>
> **(iii) the disclosure of brokered personal information 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.**

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