

February 20, 2026

By Electronic Submission

Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, Maryland 21401

House Economic Matters Committee
231 Taylor House Office Building
Annapolis, Maryland 21401

Philip Recht
Partner

T: +1 213 229 9512
F: +1 213 576 8140
PRecht@mayerbrown.com

Re: Senate Bill 504/House Bill 711 re Data Privacy

To the members of the esteemed Senate Finance and House Economic Matters Committees:

Our firm represents a coalition of companies (i.e., Spokeo, PeopleFinders, BeenVerified, and People Connect) that provide background check, fraud detection, and other people search services. We write to address a single issue of concern in SB 504/HB 711, which would amend the Online Data Privacy Act (the “MODPA”), specifically its definition of “publicly available information.” The primary purpose of our comments is to ensure that the bills appropriately safeguard constitutionally-protected public data, consistent with the comprehensive data privacy laws enacted in numerous states and recommended by the Uniform Law Commission (ULC).

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. 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 investigate potential neighborhoods and neighbors, to plan family reunions, and to root out scams.

II. Our comments. Our clients support the enactment of comprehensive data privacy laws and rules. Clear and consistent data privacy practices not only protect consumers, but benefit businesses through enhanced consumer trust and stable compliance regimes. Even before the

Maryland Senate Finance & House
Economic Matters
February 20, 2026
Page 2

many state law enactments, our clients have long provided consumers with rights that laws such as the MODPA later made mandatory (e.g., opt-out rights). Indeed, when the MODPA was first proposed in 2024 (as SB541 and HB 567), we raised no objections. Our comments now are not meant to undermine the MODPA, but rather to ensure it remains constitutional and consistent with the laws of other states.

A. State law definitions of “publicly available information”

“In numerous cases the [United States 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.” *Barnicki v. Vopper*, 532 U.S. 514, 527 (2001).

The Supreme Court also 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) (holding that statute that restricts the commercial use of people’s personal identifying information “clearly restricts speech based upon its content”). “[T]hat 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), while 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). As a general matter, “state action to punish the publication of truthful information seldom can satisfy constitutional standards.” *Barnicki*, 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 20 comprehensive data privacy laws enacted in the United States in the past eight years, including the MODPA, as well as the model Uniform Personal Data Protection Act (UPDPA) drafted by the Uniform Law Commission (ULC), have come to exclude publicly available information, which has at least three components, rooted in Supreme Court jurisprudence: (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). *See*:

Maryland Senate Finance & House
Economic Matters
February 20, 2026
Page 3

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. Oregon [SB 619](#) § 1(13)(b);
16. Rhode Island [S2500](#) § 6-48.1-2(24);
17. Tennessee [HB 1181](#) § 47-18-3201(24);
18. Texas [HB 4](#) § 541.001(27);
19. Utah Code Ann. § 13-61-101(29).
20. Virginia Code § 59.1-571.

In addition to the state laws, the ULC (also known as the National Conference on Commissioners on Uniform State Laws), 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 publicly available data.¹ As the UPDPA’s drafters explained, “[t]he processing of publicly available information is excluded from the act[s]” because “[t]here are significant First Amendment implication for placing limits on the use of public information.” Sec. 3 cmt.

These state and model laws reflect a comprehensive, consistent commitment to protect public data in accordance with the First Amendment.

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).

Maryland Senate Finance & House
Economic Matters
February 20, 2026
Page 4

B. SB 504/HB 711's compatible use restriction on government records

SB 504 and HB 711 would deviate from the national standard, by amending the MODPA's definition of "publicly available information," at proposed section 14-4701(cc)(1), as follows:

"Publicly available information" means information that a person: (i) Lawfully obtains from a record of a governmental entity, **IF THE PERSON PROCESSES THE INFORMATION IN ACCORDANCE WITH EACH RESTRICTION OR TERM OF USE PLACED ON THE INFORMATION BY THE GOVERNMENTAL ENTITY**; (ii) Reasonably believes a consumer or widely distributed media have lawfully made available to the general public; or (iii) If the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

We presume that this "compatible use" restriction is based on nearly identical language in the nation's first comprehensive state data privacy law, the California Consumer Privacy Act or "CCPA." The original draft CCPA, first proposed as a ballot initiative in 2018, did not require government records data to be used for a compatible purpose to qualify as "publicly available." But when the ballot initiative was hurriedly converted to a bill, a compatible use restriction was added, premised on analogous language in the federal Privacy Act of 1974 (the "Privacy Act"), [5 U.S.C. § 552a](#).

The California legislature quickly came to understand that analogy to the 1974 Privacy Act was a mistake, however. That is because the Privacy Act, unlike the CCPA, expressly and exhaustively defines compatible uses, thereby avoiding fatal uncertainty under the First Amendment.

The Privacy Act primarily governs inter-agency transfers of *non-public* confidential information, such as an individual's education, financial, medical, criminal, and employment history. 5 USC § 552a(a)(2), (4). The Privacy Act sets the conditions under which one government agency can disclose its records to a "recipient agency" or otherwise, including "routine" or "compatible" use. *Id.* § 522a(a)(7), (a)(9), (b).

Crucially, the Privacy Act does not leave "routine use" undefined. Every agency to which the Act applies must "publish in the Federal Register," among other things, "each routine use of the records contained in [its recording] system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). These lists can and must be updated before a new routine use can be added. The Privacy Act itself lists twelve other conditions that authorize disclosure, such as a census or congressional hearing. *Id.* § 522a(b)

Here, as first in California, the compatible use restriction is being applied to information that has been made publicly available and, thus, is no longer confidential. Moreover, the restriction applies to data made available by all state and federal government agencies, including many in this and other states that will not have published (and are not required to publish) lists of routine

Maryland Senate Finance & House
Economic Matters
February 20, 2026
Page 5

and accordant uses. Controllers thus will be left to speculate as to both the restrictions placed on the use of government records and whether the controllers' uses are "in accordance" with such restrictions.

Such uncertainty (otherwise known as a prior restraint) "raises special First Amendment concerns because of its obvious chilling effect on free speech." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 871-72 (1997). Absent a list of acceptable uses, consumers, controllers, and other "[p]eople of common intelligence must necessarily guess at [the MODPA's] meaning and differ as to its application." *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 324, (2010). Moreover, because the "publicly available information" definition runs throughout the MODPA, the constitutional flaw puts the entire act 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.").

For these reasons, the California legislature amended the definition of "publicly available information" less than a year after the CCPA was enacted to remove the compatible use restriction (2019 Cal. AB 874). Since that time, nineteen other states have passed comprehensive data privacy laws. Some, copying the original CCPA, started out with "compatible use" restrictions. But, as in California, those bills were swiftly amended or superseded altogether and, to date, no state has passed or enacted a data privacy law with a compatible use limitation on its "publicly available information" definition.

We respectfully request that the same occur here and that the proposed compatible use restriction on the definition of publicly available information be removed from SB 504 and HB 711.

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