WILMERHALE

MEMORANDUM

+1 202 663 6800
+1 202 663 6363
seth.waxman@wilmerhale.com

Date February 27, 2023

To Christopher A. Mohr, President
Paul Lekas, Senior Vice President for Global Public Policy and Government Affairs
Software & Information Industry Association

From Seth P. Waxman

Re **Invalidity Under the First Amendment of Provisions of the Proposed American Data Privacy and Protection Act That Would Restrict Handling and Sharing of Publicly Available Information**

I. Executive Summary

The Supreme Court has made clear that "the creation and dissemination of information is speech for First Amendment purposes." *Sorrell v. IMS Health Inc*., 564 U.S. 552, 570 (2011). Although the proposed American Data Privacy and Protection Act ("ADPPA" or "HB 8152") addresses important privacy concerns, as currently drafted, certain of its provisions violate settled First Amendment principles by restricting the collection, retention, and dissemination of publicly available information.[1] These discrete provisions—which do not forward the Act's privacy goals—should be revised to avoid First Amendment violations, confusion, and litigation.

Speech restrictions that discriminate based on the identity of the speaker or the content of the speech are generally subject to strict scrutiny. Courts have acknowledged that there is generally no significant privacy interest in data that is in the public domain; as a consequence, laws that restrict the collection, retention, or dissemination of such information cannot survive that strict scrutiny because they are not narrowly tailored to advance a compelling government interest. Indeed, the provisions of HB 8152 that do so would fail even a less-restrictive "intermediate" level of scrutiny because they do not directly advance a substantial government interest.

As currently drafted, HB 8152 prohibits "covered entit[ies]" from collecting, processing, transferring, or even retaining over objection "covered data" other than to accomplish certain enumerated purposes. Sections 101(a)-(b); 203(a)(3). The bill's definition of "covered data," however, includes not just genuinely private, sensitive data but also, in some cases, inferences that are based exclusively on publicly available information. It also includes publicly available information that has been combined with covered data. And it appears to include information

[1] This white paper analyzes the version of the bill reported by the Committee on Energy and Commerce on December 30, 2022. H.R. Rep. No. 117-669.

based on aural observations of individuals in public. Individuals have no significant privacy interest in these categories of information that are known or knowable from information in the public domain. Yet HB 8152 would permit individuals to veto the inclusion of such information in databases and publications that businesses and non-profits provide to customers and others who use it for entirely legitimate purposes such as public safety, fraud detection, and public health. Congress should revise the definition of "covered data" to ensure that it does not include inferences drawn exclusively from publicly available information, public information that an entity at some point has been combined with nonpublic covered data, and information based on aural observations of individuals in public. Otherwise, these limitations on speech are all but certain to be struck down.

This paper first sets forth the background, purpose, and relevant provisions of the ADPPA as currently drafted. It then explains why the bill's burdening of speech would be subject to strict scrutiny and why several discrete provisions of the bill as currently drafted would not survive that scrutiny, or indeed even intermediate scrutiny. Next, it explains why these currently included provisions threaten important public interests and pose serious practical concerns for both the wide array of regulated entities and the multitudes of consumers, citizens, businesses, and other entities that they aid. Finally, it proposes modest revisions that would avoid these constitutional infirmities.

II. Background

The stated purpose of HB 8152 is to protect individual privacy rights. The preamble explains that it is intended "to provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement."[2] The bill seeks to "establish[] a

[2] The Committee on Energy and Commerce, which voted to advance the ADPPA to the full House of Representatives, issued a Memorandum stating that the Nation's current lack of a "comprehensive, national data privacy standard" means that it "relies on sector-specific privacy-related federal statutes that establish varying degrees of protection, impose different collection and use limitations on various entities, and provide consumers with varying degrees of individual rights." The memo states that the world has become "increasingly digital," companies have "increased their collection of personal consumer data," and Americans are concerned about "data privacy." It asserts that "data breaches," companies' provision of "data to third parties without knowledge, surreptitiously installing tracking software, misleading users about data harvesting, and more" constitute "[o]nline privacy harms" and "distress[] Americans." *See* Memorandum, Committee on Energy and Commerce Staff, *Hearing on "Protecting America's Consumers: Bipartisan Legislation to Strengthen Data Privacy and Security"* (June 10, 2022), https://tinyurl.com/bdz9jnuh.

national standard to protect consumer data privacy" by regulating how an expansive array of specified entities may collect, use, share, and sell data.[3]

A. Speech Regulation

HB 8152 aims to regulate the conduct of numerous entities in a variety of ways, and many of its proposed regulations would limit speech. For example:

- Section 101, titled "Data Minimization," provides that "[a] covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to … provide or maintain a specific product or service requested by the individual to whom the data pertains" or to accomplish one of 17 enumerated purposes. Those purposes relate principally to provision of the requested products or services, preventing illegal activity and serious injuries, and complying with legal requirements. They include, for example, "authenticat[ing] users of a product or service," "fulfill[ing] a product or service warranty," "prevent[ing], detect[ing], protect[ing] against, or respond[ing] to a security incident," and "prevent[ing], detect[ing], protect[ing] against, or respond[ing] to fraud, harassment, or illegal activity" that can "directly harm." Covered entities would be prohibited from collecting, processing, or transferring covered data for any other purpose—for example, conducting internal research, non-peer-reviewed research, or research that is not viewed as being "in the public interest," *see* Section 101(b)(10) (setting forth requirements for permissible use of covered data in research); and "transfer[ring] covered data for payment or other valuable consideration to a government entity," Section 101(b)(15).
- Section 102 would further restrict covered entities' and service providers' abilities to collect, transfer, and process certain types "sensitive covered data." Among other things, it would require individuals' "affirmative express consent" to transfer "sensitive covered data" under some circumstances.
- Section 203 would require covered entities to correct, delete, or export covered data regarding an individual upon that individual's request.
- Section 204 would require covered entities to allow individuals to opt out of certain transfers of their covered data.

Because "the creation and dissemination of information is speech for First Amendment purposes," *Sorrell*, 564 U.S. at 570, HB 8152's provisions (1) restricting companies' ability to collect, process, and transfer data and (2) empowering individuals to opt out of data transfers and

[3] *Id.* at 2.

selectively require companies to delete data pertaining to them would significantly burden companies' protected speech rights.

B. Covered Data

HB 8152 defines "covered data" as "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers." Section 2(8). The definition excludes several categories of information, including "publicly available information" (as defined) and "inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual." Section 2(8)(B)(iii)-(iv).

1. "Publicly Available Information"

Under HB 8152, "publicly available information" is "any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from—

> (i) Federal, State, or local government records, if 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, for free or for a fee, can log in to the website or online service;[4]
>
> (iv) a disclosure that has been made to the general public as required by Federal, State, or local law; or
>
> (v) the visual observation of the physical presence of an individual or a device in a public space, not including data collected by a device in the individual's possession.

Section 2(27)(A).

[4] "[I]nformation from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience." Section 2(27)(B)(i).

2. Carve-Outs From "Publicly Available Information"

HB 8152 carves out exceptions to its definition of publicly available information, resulting in their reversion to "covered data," to which the bill's restrictions apply. Significantly, these carve-outs include: (1) "any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual"; and (2) "publicly available information that has been combined with covered data." Section 2(27)(B)(ii).

3. "Sensitive Covered Data"

The bill designates certain "types of covered data" as "sensitive covered data," Section 2(28)(A), subjecting them to additional restrictions.[5] And yet, anomalously, certain categories of "sensitive covered data" include information in which individuals do *not* have a reasonable expectation of privacy—precisely because that information can be inferred from "publicly available information." For example, "sensitive covered data" includes inferences regarding an individual's health status, race, or union membership even when that data can be derived from publicly available information.

C. Regulated Parties

HB 8152 regulates and restricts the speech of several groups, including "covered entit[ies]," "third part[ies]," and "third-party collecting entit[ies]."

A "covered entity" is "any entity or any person, other than an individual acting in a non-commercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data" and (I) is subject to the Federal Trade Commission Act; (II) is a common carrier subject to the Communications Act of 1934; or (III) is an organization not organized to carry on business for its own profit or that of its members. Section 2(9)(A). The definition excludes: (i) governmental entities and (ii) people or entities collecting, processing, or transferring covered data on behalf of a government entity, insofar as

[5] The bill defines sixteen separate categories of "sensitive covered data," including "[a]ny information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare condition or treatment of an individual," Section 2(28)(A)(ii), all "[i]nformation about an individual when the covered entity or service provider has knowledge that the individual" is under 17 years old, Section 2(28)(A)(xiii), and "[a]n individual's race, color, ethnicity, religion, or union membership," Section 2(28)(A)(xiv). The bill also empowers the Commission to commence rulemaking to include in that definition "any other type of covered data that may require a similar level of protection" as those already included "as a result of any new method of collecting, processing, or transferring data." Section 2(28)(B).

they are acting as a "service provider" to the government entity.[6] It also excludes entities that serve as congressionally designated nonprofits, national resource centers, or clearinghouses that provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues. Section 2(9)(B).

Broadly speaking, "third part[ies]" include persons or entities that collect, process, or transfer covered data that others have directly collected from the individuals linked to that data. Section 2(35). "Third-party collecting entit[ies]" are a subset of third parties whose "principal source of revenue," as defined by HB 8152, "is derived from processing or transferring covered data" that they did not collect directly from the individuals linked to that data. Section 2(36). HB 8152 would subject third-party collecting entities to additional requirements, including that they register to be included in a planned "central registry of third-party collecting entities." Section 206(b)(3). This registry would facilitate and streamline individuals' requests that third-party collecting entities delete or cease collecting covered data.

Many businesses—including members of the Software & Information Industry Association ("SIIA")—gather and sell information about people and thus would be covered by the ADPPA as currently drafted. Regulated parties include companies ranging from retailers, media platforms, publishers, consulting firms, industry analysts, marketing experts, executive search firms, agents, lobbyists, rating services, to private detectives.

III. HB 8152's Restrictions On Collection And Transfer Of Certain Forms Of "Covered Data" Would Violate The First Amendment

As currently drafted, three provisions of HB 8152 would violate the First Amendment because they would prohibit covered entities, like SIIA's members, from collecting, processing, or transferring three categories of "covered data" for reasons other than to accomplish statutorily enumerated permissible purposes: (1) inferences based exclusively on publicly available information, (2) publicly available information that at some point has been combined with covered data, and (3) information gleaned from aural observations of individuals in public

[6] A "service provider" is "a person or entity that—(i) collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity; and (ii) receives covered data from or on behalf of a covered entity or a Federal State, Tribal, territorial, or local government entity." Section 2(29)(A). The "service provider" exclusion is most naturally read to apply only when governmental entities like law-enforcement and public-health agencies outsource data management activities but retain full control and decision-making power over all data collected and used by the outside firm, including the ability to demand deletion of data. Accordingly, when an outside firm controls and manages its own data (often employing it to serve multiple governmental and non-governmental entities), ADPPA's "service provider" exclusion likely would not apply to it.

spaces. Under the current bill, individuals may veto the inclusion of those categories of information about themselves in the databases and publications that many businesses provide to customers who use them for important, entirely legitimate purposes. Individuals would also be able to demand that covered entities delete those categories of data from their possession. But individuals have no significant privacy interest in information that already is publicly available or is entirely derivative of publicly available information.

A. HB 8152 would restrict and limit speech

"[T]he creation and dissemination of information is speech for First Amendment purposes." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011). "Even dry information, devoid of advocacy, political relevance, or artistic expression," is speech guaranteed constitutional protection. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 446-447 (2d Cir. 2001). "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs." *Sorrell*, 564 U.S. at 570; *see also 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 First Amendment protects the right to receive information, as well as the right to create and disseminate it. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969). And courts have specifically held that "disclosure of … consumers' identities" "'to data miners and other third parties,' which allows for targeted marketing, advocacy, and solicitations from businesses, political groups, or non-profit organizations" is "protected speech." *Boelter v. Hearst Commc'ns, Inc.*, 192 F. Supp. 3d 427, 435, 444 (S.D.N.Y. 2016); *see also Trans Union Corp. v. FTC*, 267 F.3d 1138, 1140 (D.C. Cir. 2001) (targeted marketing lists comprise speech); *ACA Connects - Am.'s Commc'ns Ass'n v. Frey*, 471 F. Supp. 3d 318, 327 (D. Me. 2020) ("marketing of customer data … is sheltered by the First Amendment").

Under these precedents, various of HB 8152's provisions would restrict and limit covered entities' ability to create, receive, and disseminate information, thereby burdening their speech. *First*, as discussed, the bill would limit the purposes for which covered entities may collect, process, and transfer "covered data." *Second*, the bill would grant individuals the right to demand that covered entities delete certain information about them and prohibit those entities from transferring certain data about them. The bill would thereby restrict the creation and dissemination of information. These restrictions implicate the First Amendment.

B. HB 8152's limitations on speech are, at least in most respects, subject to strict scrutiny

1. The bill is subject to strict scrutiny because it imposes speaker- and content-based limits on non-commercial speech

Restrictions on speech that vary based on the identity of the speaker or the content of the speech are generally subject to the strictest form of First Amendment scrutiny, "which requires the Government to prove that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed v. Town of Gilbert*, 576 U.S. 155, 164 (2015). HB 8152's speech-restrictive provisions are both speaker- and content-based.

Speech restrictions are speaker-based when they treat distinct classes of speakers differently or regulate their speech to different degrees. *Turner Broadcasting Sys., Inc. v. FCC*, 512 U.S. 622, 658 (1994); s*ee Minneapolis Star & Trib. Co. v. Minnesota Com'r of Revenue*, 460 U.S. 575, 591 (1983) (state's "ink and paper tax," subjecting newspapers to a tax not imposed on other businesses, violates the First Amendment). Courts subject speaker-based restrictions on speech to strict scrutiny "when they reflect the Government's preference for the substance of what the favored speakers have to say (or aversion to what the disfavored speakers have to say)." *Turner Broadcasting*, 512 U.S. at 658.

HB 8152's "covered entity" definition makes clear that its limitations on speech depend on the identity of the speaker. For example, HB 8152 does not apply to "individual[s] acting in a non-commercial context," but does apply to entities subject to the Federal Trade Commission Act, common carriers, and non-profit organizations. Section 2(9)(A). HB 8152 also excludes from the definition of "covered entity" government entities, service providers to such government entities, and "congressionally designated nonprofit[s], national resource center[s], and clearinghouse[s]," but only those that "provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues." Section 2(9)(B)-(C). HB 8152's speaker-based restrictions demonstrate Congress's preference for speech unrelated to commerce and speech forwarding governmental aims over non-governmental aims. They also show Congress's preference for organizations addressing "missing and exploited children issues" over non-profits, national resource centers, and clearinghouses that address other social issues.

HB 8152's restrictions are also content-based in several ways, and thus also subject to strict scrutiny on that basis as well. *Reed*, 576 U.S. at 164. "A regulation of speech is facially content based under the First Amendment if it 'target[s] speech based on its communicative content'—that is, if it 'applies to particular speech because of the topic discussed or the idea or message expressed.'" *City of Austin v. Reagan Nat'l Advert. of Austin, LLC*, 142 S. Ct. 1464, 1471 (2022) (quoting *Reed*, 574 U.S. at 163) (alterations in original). That describes HB 8152, which targets only information that identifies an individual or a device reasonably linked to an individual. Moreover, the bill's inclusion within "covered data" of "[a]ny inference made exclusively from multiple independent sources of publicly available information that reveals

sensitive covered data with respect to an individual" is content-based because only inferences that reveal content specifically included within Section 2(28)'s enumeration of "sensitive covered data" qualify for the bill's limitations on speech.

2. HB 8152 would not avoid strict scrutiny merely because some of the speech it regulates is sold

Regulations of "commercial speech" are subject to intermediate scrutiny. *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 562 (1980); *see also Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66 (1983). But "commercial speech" does not include all speech that is sold. Rather, the core of commercial speech is speech that "proposes a commercial transaction," typically understood as advertising. *Central Hudson*, 447 U.S. at 562; *Bolger*, 463 U.S. at 66. *See also Spirit Airlines, Inc. v. DOT*, 687 F.3d 403, 412 (D.C. Cir. 2012); *U.S. Healthcare, Inc. v. Blue Cross of Greater Phila.*, 898 F.2d 914, 933 (3d Cir. 1990); *Greater Baltimore Ctr. for Pregnancy Concerns, Inc. v. Mayor & City Council of Baltimore*, 721 F.3d 264, 285 (4th Cir. 2013); *Bad Frog Brewery, Inc. v. N.Y. State Liquor Auth.*, 134 F.3d 87, 97 (2d Cir.1998).

Most of the information collection and transfer that would be regulated by HB 8152 does not propose a commercial transaction or refer to a specific product. For example, firms regularly gather information about individuals' demographics, preferences, and practices and pass that information to other firms that make use of that information. That some of this speech is sold does not make it commercial speech. The mere fact that a business may have an economic motivation for collecting and disseminating information does not transform that speech activity into commercial speech. *See, e.g., City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 756 n.5 (1988) ("[T]he degree of First Amendment protection is not diminished merely because . . . speech is sold rather than given away."); *Bolger*, 463 U.S. at 67 ("the fact that [a speaker] has an economic motivation for [his speech] would clearly be insufficient by itself to turn the materials into commercial speech"); *Sorrell*, 564 U.S. at 567 ("a great deal of vital expression" "results from an economic motive"). Moreover, HB 8152 clearly limits non-economically motivated collection and dissemination of information, too, because it also applies to "organization[s] not organized to carry on business for [their] own profit or that of [their members]." Section 2(9)(A)(i)(III).

Accordingly, a court evaluating HB 8152's speaker- and content- based speech-regulating provisions would apply the demanding strict scrutiny standard, at least in the vast majority of instances. *See Sarver v. Chartier*, 813 F.3d 891, 903, 905-906 (9th Cir. 2016) (applying strict scrutiny to prohibition on disseminating personal information about an individual in speech that does not "propos[e] a commercial transaction").

3. Even if some of the speech HB 8152 regulates were deemed to be "commercial speech," its restrictions of such speech would be tested under intermediate scrutiny

Were a court to determine that certain speech the bill regulates is "commercial speech," as the Supreme Court has narrowly defined it, the restricting provisions would be evaluated under an "intermediate" standard that is heightened, although less exacting than strict scrutiny. *See Retail Digital Network, LLC v. Prieto*, 861 F.3d 839, 847-848 & n.9 (9th Cir. 2017) (subjecting "undisputedly speaker-based" and "content-based" law regulating commercial speech to intermediate scrutiny); *United States v. Caronia*, 703 F.3d 149, 165 (2d Cir. 2012) (same). If commercial speech concerns lawful activity and is not misleading, the government may restrict it only if the government proves it has "a substantial interest to be achieved by restrictions on commercial speech" and the restriction "directly advance[s] the [government] interest involved." *Central Hudson*, 447 U.S. at 564. "If the governmental interest [that the law purports to advance] could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive." *Id.*

C. HB 8152's restrictions on collection, processing, and transfer of certain forms of "covered data" would fail both strict scrutiny and intermediate scrutiny

While HB 8152 is animated by broad privacy concerns regarding the collection, use, and sale of private personal consumer data by companies, neither the bill nor its legislative history provide any rationale for regulating speech involving three categories of information in which individuals have no significant privacy interest: (1) inferences made based solely on information that is already publicly available; (2) publicly available information that has at some point been combined with covered data; and (3) information gleaned from aural observations of individuals in public spaces.[7] These provisions would fail strict scrutiny because they are not "narrowly tailored to promote a compelling Government interest." *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000). Indeed, they would fail even intermediate scrutiny because they do not "'directly advance[]'" a "substantial" interest and in any event are "more extensive than

[7] As the bill is currently drafted, its definition of "publicly available information" may also present constitutional concerns. "Publicly available information" includes "any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from . . . Federal, State, or local government records, *if 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*," Section 2(27)(A) (emphasis added). To the extent that the "restrictions or terms of use" referenced in this provision are themselves constitutionally infirm, that infirmity would also impact the legitimacy of the bill's attempt to regulate collection, processing, and transfer of "information … lawfully made available to the general public from . . . Federal, State, or local government records."

necessary to serve [the asserted] interest." *Vugo, Inc. v. City of New York*, 931 F.3d 42, 51 (2d Cir. 2019) (quoting *Central Hudson*, 447 U.S. at 566).

1. Restricting the collection and dissemination of information reflecting inferences drawn from publicly available information that reveal "sensitive covered data" with respect to an individual does not materially advance any significant privacy interest

Limitations on the collection, processing, and dissemination of inferences drawn exclusively from publicly available information would fail any applicable First Amendment test, even if the information reveals "sensitive covered data."

An inference drawn exclusively from publicly available information reveals no private information, regardless of whether the information is "sensitive." For example, "sensitive covered data" is defined to include "[i]nformation identifying an individual's online activities over time and across third party websites or online services." Section 2(28)(A)(xv). Take, for example, an individual making and selling custom quilts advertised and sold to the public over third party websites like Etsy. Information regarding the individual's public online business activities would qualify as "sensitive covered data." This would be true even though the quiltmaker intentionally utilized these websites in a public manner to gain exposure and business, and though any member of the public could perform a Google search that would reveal the various online platforms through which her quilts could be purchased.

Limitations on the collection and dissemination of such inferences cannot survive First Amendment scrutiny because there is no substantial, much less a compelling, government interest in restricting information that is already available to the public via other means. Courts have repeatedly held that there is significantly less of a privacy interest in information that is already available to the public. *See Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 494-495 (1975) ("even the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record"); *Oklahoma Publishing Co. v. District Court*, 430 U.S. 308, 311 (1977) (court violated First Amendment by enjoining dissemination of truthful information that had been "publicly revealed" and was "in the public domain"), *Trans Union*, 267 F.3d at 1140 (there is less of a privacy interest in "names, addresses, and financial circumstances" of "companies whose articles of incorporation and financial statements are generally available for inspection" than in the non-broadly available names, addresses, and financial circumstances of private individuals); *see also In re Application of New York Times Co. for Access to Certain Sealed Ct. Recs.*, 585 F. Supp. 2d 83, 91 (D.D.C. 2008) (because some assertedly private information was "*already known by the public*," "disclosure . . . does not present the risk that [information] will be *newly disclosed* to the media) (emphasis added)*; Application of WP Co. LLC*, 201 F. Supp. 3d 109, 130 (D.D.C. 2016) (evaluation of privacy interest taking into account that documents newspaper seeks are

"not publicly available" and the newspaper's "reporting to date offers scant information regarding their supposed contents"); *cf. Cottone v. Reno*, 193 F.3d 550, 554 (D.C. Cir. 1999) ("Under our public-domain doctrine, materials normally immunized from disclosure under FOIA lose their protective cloak once disclosed and preserved in a permanent public record.").

As the Tenth Circuit has explained, "[i]n the context of a speech restriction imposed to protect privacy by keeping certain information confidential, the government must show that the dissemination of the information desired to be kept private would inflict *specific and significant harm* on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity." *U.S. West, Inc.*, 182 F.3d at 1235 (emphasis added). But where the information in question is already publicly available, the interests protected diminish substantially. "Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of a substantial state interest." *Id.* at 1235.

Indeed, *U.S. West* highlighted the corresponding downsides of privacy-motivated speech restrictions, which "facilitate[] the dissemination of false information by making it more difficult for individuals and institutions to discover falsities"; "protect[] the withholding of relevant true information, such as when an employee fails to disclose a medical condition that would affect his or her job performance"; "interfere[] with the collection, organization, and storage of information which can assist businesses in making rapid, informed decisions and efficiently marketing their products or services," thereby "lead[ing] to reduced productivity and higher prices for those products or services"; and "may even threaten physical safety by interfering with the public's ability to access information needed to protect themselves, such as whether an individual has a history of child abuse or molestation, sexual offenses, or communicable diseases." 182 F.3d at 1235 n.7 (quotation marks and internal citations omitted).

Here, the restrictions on covered entities' dissemination of inferences drawn solely from publicly available information would impose all of these negative side effects without substantially serving any significant government interest. By definition, the inferences could be made and disseminated by other, non-covered parties. Even under intermediate scrutiny, the government cannot defend a restriction "by merely asserting a broad interest in privacy." *U.S. West*, 182 F.3d at 1235. Rather, the government "must specify the particular notion of privacy and the interest served. ... [T]he 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." *Id.* at 1234-1235; *compare Individual Reference Servs. Grp., Inc. v. FTC*, 145 F. Supp. 2d 6, 42 (D.D.C. 2001) (concluding "Congress and the defendant agencies" had specified sufficiently particularized privacy interest "by articulating that the purpose of the

Act as ensuring 'that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal account information.'" (citation omitted)), *aff'd sub nom. Trans Union LLC v. FTC*, 295 F.3d 42 (D.C. Cir. 2002).

Individuals have no genuine expectation of privacy in—and the government has no substantial interests in protecting—information that, although falling within HB 8152's definition of "sensitive covered data," can nonetheless be inferred from publicly available information. But the bill's sweeping definition of "sensitive covered data" means that it would restrict the collection and dissemination of considerable data that could be inferred from publicly available information. Section 2(27)(B)(ii)(II) would therefore fail both strict and intermediate scrutiny.

2. Restricting the collection and dissemination of publicly available information that at some point has been combined with covered data does not advance any significant privacy interest

Section 2(27)(B)(ii)'s exclusion of "[p]ublicly available information that has been combined with covered data" from the definition of "publicly available information" could be interpreted to mean that once publicly available information has been combined with covered data, that publicly available data remains covered data even in its original, pre-combination form and even if all otherwise covered data is excised and withheld. If that were the case, the provision would violate the First Amendment by restricting the collection and dissemination of publicly available information. No significant privacy interests are served by requiring businesses to delete the publicly available information component of a set of data that is a combination of publicly available information and non-public covered data. Nor are any privacy interests served by barring a business from disclosing or transmitting publicly available information (or inferences drawn from that information) simply because the business has, in other contexts, combined that same publicly available information with covered data.

For example, imagine that a company has the following information: (1) a publicly available deed showing that John Harold Doe lived at a certain address as of June 2009; (2) non-publicly-available, covered data showing that "John Doe" lived there as of July 2009; and (3) non-publicly-available, covered data showing that "J. Harold Doe" lived there as of September 2012. Combining that data, the company concludes that a single person, John Harold Doe, AKA John Doe, AKA J. Harold Doe, likely lived at that address from July 2009 to September 2012. It may be permissible under the First Amendment for a law to grant a person who is the subject of this set of information a right to demand that the company delete from its database (and not in the future disclose) the combined inference that a single person, John Harold Doe, AKA John Doe, AKA J. Harold Doe, likely lived at that address from July 2009 to September 2012. But it would not be permissible to extend that same result to the information that the company acquired

through the publicly available deed: the fact that John Harold Doe lived at the address in question as of June 2009.

The current version of the ADPPA's inclusion of publicly available information that has been combined with covered data in the definition of covered data could be construed as requiring the company to delete (and refrain from disclosing in the future) such publicly available information on request. That requirement could not withstand First Amendment scrutiny. As discussed, restricting the retention or dissemination of publicly available information does not advance any substantial or compelling interest. Thus, deletion of that publicly available information simply because it had previously been combined with covered data would be an "excessive restriction[]." *Central Hudson*, 447 U.S. at 564; *R.A.V. v. City of St. Paul.*, 505 U.S. 377, 395-396 (1992).

3. The presumptive inclusion of aural observations of an individual in a public space in the definition of "covered data" does not advance any significant privacy interest

HB 8152 includes "*visual* observation[s] of the public presence of an individual … in a public space" in the definition of "publicly available information." Section 2(27)(A)(v) (emphasis added). It does not include *aural* observations of the public utterances of individuals in a public space. It follows that such aural observations would be considered "covered data" under the bill and therefore be subject to its various restrictions on collection and dissemination.

As discussed above, a person has no reasonable expectation of privacy in what he "knowingly exposes to the public, even in his own home or office." *Katz v. United States*, 389 U.S. 347, 351 (1967). The bill itself recognizes this by including "visual observation[s]" in the definition of publicly available information. Individuals have just as little privacy interest in aural observations of them made in public. *See id.* at 361 (the "expectation of privacy" in "conversations in the open, [which] would not be protected against being overheard" "would be unreasonable"). The bill therefore should be amended to include public aural observations in its definition of publicly available information.

D. The bill's conclusory declaration that it shall not be interpreted to limit or diminish First Amendment rights does not cure its constitutional failings

Section 101(e) of HB 8152, entitled "Journalism," states that "[n]othing in this Act shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution." Whatever comfort—if any—this provision might provide to persons or entities engaged in "journalism," it would in no way resolve the First Amendment problems identified above. Persons and companies engaged in activities other than journalism possess First Amendment rights, too, and they are the targets of the bill. *See, e.g.*, *Branzburg v. Hayes,* 408 U.S. 665, 684 (1972) ("[T]he First Amendment does not guarantee the press a constitutional right of special

access to information not available to the public generally."). And even without the journalism-specific title, the provision could not preempt or cure the constitutional problems posed by the bill's text, which is not narrowly tailored to advance a compelling interest. *See Committee in Solidarity with People of El Salvador v. FBI*, 770 F.2d 468, 474 (5th Cir. 1985) (holding that statutory provision stating "nothing contained in this section shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution of the United States" cannot "substantively operate to save an otherwise invalid statute, since it is a mere restatement of well-settled constitutional restrictions on the construction of statutory enactments").

IV. The Provisions of HB 8152 Discussed in This Paper, As Currently Drafted, Threaten Important Public Interests and Pose Serious Practical Concerns

The bill's inclusion in its definition of covered data of (1) inferences drawn from publicly available information, (2) publicly available information that at some point has been combined with covered data, and (3) aural observations of individuals in public places threatens to hamstring a variety of beneficial collection and communication of information such as:

1. Dissemination of non-fiction books reflecting certain types of research that draws inferences from publicly available information.
2. Private sector services used in fraud investigations or other criminal or regulatory inquiries in which a claimant for public benefits in a particular state is shown by inferences from a combination of public real estate records, social media posts, and other public sources to be ineligible for those benefits.
3. Private sector services used in investigations of large-scale, complex, and sometimes international criminal schemes that use shell companies to avoid detection. Such private sector tools organize and analyze amassed publicly available data, identifying patterns and allowing for the efficient sorting of relevant and irrelevant information. They have been used to investigate, for example, mass pandemic payment fraud, human trafficking of sex workers, and fentanyl distribution networks.
4. Inferences drawn from multiple sources of publicly available information including social media feeds, which can provide guidance on the mental state of a mass shooter.
5. Private sector services that analyze combined public government records data and non-public data (such as drivers' license data or automobile ownership data) to quickly identify potential wrongdoers in rapidly evolving and life-threatening situations. For example, such data and analytics combinations have recently allowed law enforcement to quickly associate an out-of-state license plate with a local resident, facilitating both the identification of a kidnapper and the suspect in a murder case. Such data combinations were critical, for example, in identifying the "D.C. Sniper" and advancing the investigation of the Boston Marathon bombers.

6. Identity authentication and fraud-prevention services which rely on combining publicly available information with data regulated by the Gramm-Leach-Bliley Act ("GLBA"), a common and accepted practice used by countless fraud investigators and law enforcement agencies. Combinations of such data may, for example, raise fraud red flags if the physical delivery address for a major new online purchase does not appear to be associated with the identity being used to make the purchase.
7. Use of inferences drawn from publicly available data such as an individual's health status to provide services to healthcare institutions like hospitals to identify people who might need additional services and offer support services, as is done to address requirements from insurance carriers.
8. The collection and combination of information—both public and non-public—when conducting due diligence about officers and directors of a particular business when another company seeks to buy or enter into a relationship with that business.
9. The use by financial institutions and other businesses of services that use both non-public and publicly available data sources to help them meet "know your customer" or anti-money laundering, antiterrorism and anti-human trafficking obligations, as well as other financial laws, regulations, and industry practices. For example, banks have specific obligations when opening accounts for Politically Exposed Persons ("PEP") who are close relatives of senior government officials. PEP lists are compiled from publicly available media combined with nonpublic data. These services allow for the implementation of best practices in line with international objectives for corporate governance and efforts to combat bribery and corruption around the world and compliance with standards set in the UN Global Compact.
10. Corporate actions to rid supply chains of modern-day slavery and human rights abuses, aided by analysis of and inferences drawn from publicly available data.
11. Industry analysts' and ratings services' acquisition and handling of information critical to their analyses.

V. HB 8152 Should Be Modified To Cure These Constitutional Shortcomings

To prevent violations of citizens' and businesses' First Amendment rights, as well as to avoid expensive and protracted litigation about the constitutionality of the problematic provisions discussed above, HB 8152 should be modified such that:

1. The bill's exclusion from "covered data" of inferences made from exclusively publicly available information should be absolute; it should not include a carveout for such inferences that reflect "sensitive covered data," because the fact that such inferences are drawn from publicly available information means that those inferences do not implicate a significant interest in privacy.

2. The bill's treatment of combinations of covered data and publicly available data should be clarified by adding language stating that (1) in no circumstance may a person demand that a covered entity delete any component of information that reflects or is based upon only publicly available information or one or more inferences drawn solely from publicly available information and (2) in no circumstance does the law bar a covered entity from disclosing or transmitting publicly available information (or inferences drawn from publicly available information), even if the covered entity or some other person or entity has in another context combined that same publicly available information with covered data.
3. Section 2(27)(A)(v) should be revised to include aural observations of individuals in public places.
4. Section 2(27)(A)(i) should be clarified to (1) require compliance with only constitutionally valid restrictions or terms of use placed on governmental records by the relevant government entity and (2) apply to only covered entities that directly agreed to comply with those restrictions or terms of use.

We respectfully submit that none of these modest amendments would impair the Bill's protection of genuine privacy interests.