TALKING POINTS IN OPPOSITION TO CALIFORNIA SB 362

Statement: We oppose SB 362 (the "bill") because it would severely harm the data economy in California, causing cascading harm to the nation's economy. SB 362 would directly reduce competition, increase costs to consumers, and undermine fraud prevention. SB 362 is unnecessary. It is duplicative of rights already afforded Californians. Furthermore, cost estimates for establishing and maintaining this new government program grossly underestimate the actual costs and will bloat the growing state deficit. The General Assembly should not pass SB 362.

Background: SB 362 would amend California's existing data broker registration statute to, in part, centralize registry management responsibilities and enforcement in the California Privacy Protection Agency ("CPPA"); add new registration disclosure requirements; create a recurring auditing requirement for registrants; and stand-up novel, centralized data deletion mechanism, effective against all registered data brokers, to be managed by the CPPA.

- **The bill's data deletion mechanism is an unreasonable, blunt instrument that consumers cannot use in a truly informed fashion.** Consumers who use the bill's data deletion mechanism would effectively delete data from hundreds of companies that provide very different products and services to the marketplace. It is inappropriate to treat all companies the same given that they have vastly different data practices and process different data types. Consumers cannot make an informed decision to execute a deletion right effective on hundreds or tens of thousands of downstream companies. A deletion request served on one data broker may have significantly different impacts on the consumer than it would have if served on another data broker. For instance, deleting data from one data broker may have serious implications for anti-fraud efforts, while others may impact marketing, loyalty programs, online identity and verification services, public interest research, discrimination prevention, risk management, insurance beneficiary location, and myriad other beneficial services that consumers desire.

- **The deletion mechanism is uniquely poised for competition abuse.** The bill permits companies to act as a consumer's authorized agent and send mass deletion requests against competing businesses. Companies not subject to the deletion mechanism, such as web browsers and other for-profit intermediaries, would have significant and undue power if SB 362 is enacted. Those intermediaries would be able to control the underlying workings of the deletion mechanism contemplated by SB 362, providing them with an unfair competitive advantage and an inappropriate position of power and control over competing entities in the marketplace. If companies are allowed to delete consumer data held by competitors, it would solely benefit their business and not consumers.

- **The bill would severely impact medium, small, and start-up businesses that rely heavily on marketing data to serve their consumers and reach new audiences**. For small and start-up businesses, third-party data sources are the lifeblood of their growth. Small and medium-sized businesses would not be able to access such data under the bill. Small, medium, and start-up entities depend almost entirely on data brokers and third-party data sets to grow their nascent businesses and reach customers interested in their products. SB 362's deletion mechanism would threaten small and start-up businesses' ability to enter and remain

in the market by virtually ensuring that their larger competitors will be better able to market and advertise to consumers. The General Assembly should not enact a law that would decimate California's small, medium, and start-up business community.

- **Business and government services would lack the ability to effectively manage the accuracy of consumer contact information**. Companies of all sizes and government services rely on third party marketing data to help maintain accuracy standards across complex data systems. Data hygiene services use marketing data to help organizations update missing or incorrect contact information. This allows the right consumer to be contacted and not receiving duplicative communications.

- **SB 362's existing fraud exemption is unreasonably limited.** The bill's limited fraud exemption would unreasonably restrain data brokers from providing data to power vital anti-fraud services. While data brokers could maintain data for the limited purpose of "security and integrity" following a deletion request, the bill would prohibit them from "selling" – transferring – data after a deletion request is received. Transfers of data that enable fraud control services offered by data brokers, as well as the ability of users of those services to detect fraud in their own systems, would be severely hampered by SB 362, thereby incapacitating critical anti-fraud services and aiding bad actors.

- **SB 362 is unnecessary, duplicative, and contradictory to existing law.** Data brokers are subject to the California Consumer Privacy Act ("CCPA"). There are no gaps in law. The full set of rights afforded to Californians under the CCPA are applicable to data brokers, including the transparency and deletion elements of SB 362. A bill applicable to data brokers alone is unnecessary.

- **The bill would conflict with the CCPA, as explicitly approved by California voters when the law was amended via ballot initiative.** Californians voted on and approved the CCPA in November 2020 through Proposition 24. The ballot initiative did not include or even contemplate a centralized deletion mechanism effective against data brokers. SB 362 could create a confusing and competing compliance environment for entities subject to both the CCPA and the bill. The California Legislature should not enact a new privacy law that overlaps or ignores key provisions of already-enacted legislation, especially when such legislation was expressly approved by the California electorate through a formal ballot initiative process.

- **The bill would severely decrease the free and low-cost availability of useful products, services, and online content and resources for consumers.** Third party data sources such as data brokers provide an indispensable and necessary service to consumers. Data provided by data brokers allows businesses to develop new products and services, keep prices for consumers down, and provide products and content for free or at a very low cost. SB 362's deletion mechanism would remove this vital data resource from the economy upon a single click of a button. The ultimate impact of this tool would be felt most acutely by consumers whose access to free online resources, critical content, and products and services would be diminished, and it would disproportionately impact Californians with less disposable income in comparison to consumers that can afford to pay more for online resources. The General Assembly should not make it harder for consumers to access free and low-cost online

resources at a time when many are already struggling to contend with inflated prices across the economy.

- **Data from data brokers creates opportunities for new, small, and growing businesses to access and thrive in the market. Loss of these services is particularly acute for minority-owned businesses.** Data from data brokers fosters a competitive marketplace where small and mid-size businesses, as well as self-employed individuals, of which many are minority owned, can compete with the economy's largest players.[1] Companies of all sizes use data-driven advertising, but smaller firms and new market entrants depend on it for a significantly greater portion of their revenue. Losing access to the products provided by data brokers would disproportionately harm the ability of these small businesses to find and retain customers and compete against larger firms in the market.[2]

- **Nonprofits and mission-driven organizations would struggle to reach new donors and prospects if SB 362 is enacted**. Nonprofits and mission-driven entities rely on data brokers to provide data that enables them to reach new donors and volunteers with their important messages. SB 362's deletion mechanism will remove data from the marketplace and detract from the ability of nonprofits and for-cause entities to further their missions. Charities, nonprofits, and other organizations that facilitate donations to and support for causes such as climate change, affordable housing, domestic violence prevention, immigration services, and others will be unable to locate new donors or volunteers outside their existing network for their missions because the data necessary to reach those prospects would be removed from the online ecosystem at the click of a single button.

- **SB 362 would undermine fraud protection and myriad other consumer benefits that result from data brokers' ability to maintain data.** Data brokers provide information that businesses use to consumers' significant benefit beyond the marketing and advertising of products and services. Fraud prevention efforts, for example, rely heavily on data provided by data brokers to verify consumers interactions and request and ensure that consumers are who they say they are when they communicate or transact with various kinds of businesses. If SB 362 is enacted, fraud prevention services that depend on data brokers will be severely impacted, along with several other products that benefit consumers and increase their safety in the online ecosystem.

- **The bill duplicates existing deletion obligations that already fall on data brokers under the CCPA.** Under the CCPA, "businesses," which can include data brokers, must effectuate deletion requests from consumers. The CCPA also requires businesses *to flow deletion requests down to service providers, contractors, and third parties to whom personal information was sold to or shared with*. Deletion requests served on individual businesses under the CCPA will consequently reach data brokers, making SB 362's requirements

[1] Nora Esposito, *Small Business Facts, Spotlight on Minority-Owned Employer Businesses*, U.S. SMALL BUSINESS ADMINISTRATION (May 2019), https://advocacy.sba.gov/wp-content/uploads/2019/05/Small-Business-Facts-Spotlight-on-Minority-Owned-Employer-Businesses.pdf.
[2] J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, 21 (2022), https://www.privacyforamerica.com/wp-content/uploads/2022/11/Study-221115-Beales-and-Stivers-Information-Economy-Without-Data-Nov22-final.pdf.

duplicative existing California law. SB 362 is unnecessary and would waste meaningful resources the CPPA could otherwise dedicate to its enforcement efforts.

- **The bill would impose premature auditing requirements on data brokers that could contradict regulations the CPPA is currently working to draft.** The CPPA has initiated a pre-rulemaking process to issue regulations governing cybersecurity audits and risk assessments. Those draft regulations have not yet been publicized, making SB 362's auditing requirements premature and potentially contradictory to the rules the CPPA is presently drafting. SB 362's auditing terms could conflict with or frustrate requirements the CPPA is currently working to draft in its regulations under the CCPA. The California Legislature should not take steps to preempt the CPPA's ongoing rulemaking process related to auditing by enacting SB 362.

- **SB 362 is severely out of step with every data broker registration statute enacted to date.** No other data broker registration includes a centralized deletion mechanism, recurring auditing requirements, and no exemptions necessary for the functioning of a modern economy. Data broker registration statutes in Vermont, Oregon, and Texas require data brokers to provide information to certain government agencies and to pay an annual fee. SB 362's terms extend far beyond mere "data broker registration" to impose substantive privacy requirements on entities that are already fully regulated under the CCPA and other applicable California privacy laws.

- **The bill's definition of "data broker" could encompass virtually every company in the marketplace—including entities that engage in minimal data processing solely on behalf of business customers.** The bill's definition of "data broker" is extraordinarily broad and could subject many companies to its requirements. The definition includes any entity that collects and "sells,"—*i.e.*, transfers, personal information of a consumer they do not directly interact with. As a result, any entity that performs data gathering services on behalf of a business customer and transfers data to that customer could be considered a data broker, even if the data transfer is one-time, de minimis, and the data is not retained in the entity's systems or databases for future use. The breadth of the data broker definition could impact routine transactional relationships between entities, where an entity obtains information only after receiving a specific request from a customer, and only keeps copies of such information for the purposes of record-keeping, not to build a database for future use.

* * *