Date of Hearing: March 26, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1202 (Chau) – As Introduced February 21, 2019

SUBJECT: Privacy: data brokers

SUMMARY: This bill would require data brokers to register with the Attorney General (AG), and would additionally require the AG to create a publicly available registry of data brokers on its website, and would grant enforcement authority for violations of these requirements to the AG. Specifically, **this bill would**:

1) Require, on or before January 31 following each year in which a business meets the definition of data broker, as provided, that the business register with the AG and provide to the AG the following:

    - A registration fee in an amount determined by the AG, not to exceed the reasonable costs of regulation.

    - The name of the data broker and its primary physical, email, and internet website addresses, and any additional information or explanation the data broker chooses to provide concerning its data collection practices.

2) Require a data broker to provide consumers the right to opt-out of the sale of their personal information (PI) and any other rights afforded by the California Consumer Privacy Act of 2018 (CCPA), consistent with that act.

3) Provide that a data broker that fails to register with the AG is subject to injunction and is liable for civil penalties, fees, and costs in an action brought in the name of the people of the State of California by the AG as follows:

    - A civil penalty of $100 for each day the data broker fails to register.

    - An amount equal to the fees that were due during the period it failed to register.

    - Expenses incurred by the AG in the investigation and prosecution of the action as the court deems appropriate.

4) Require any penalties, fees, and expenses recovered in an action prosecuted under this section shall be deposited in the Consumer Privacy Fund, with the intent that they be used to fully offset costs incurred by the state courts and the AG in connection with this bill.

5) Require the AG to create a page on its internet website where the information provided by data brokers shall be accessible to the public.

6) Provide that it is the intent of the Legislature that this act shall not be construed to supersede or interfere with the operation of the CCPA.

7) Define "business," "PI," "third party," and "sale" to have the same meanings as provided under the CCPA.

8) Define "data broker" to mean a business that knowingly collects and sells to third parties the PI of a consumer with whom the business does not have a direct relationship, but does not include the following:

   - A consumer reporting agency subject to the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

   - A financial institution subject to the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations.

   - An insurance company subject to the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 1791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code).

9) Make various findings and declarations related to consumer privacy and the practices of data brokers.

EXISTING LAW:

1) Establishes the CCPA and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

   - the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI;

   - the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;

   - the right to access the specific pieces of information a business has collected about the consumer;

   - the right to delete information that a business has collected from the consumer;

   - the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

2) Generally requires under the CCPA that a business subject to the CCPA do all of the following, among other things: comply with the above requirements, provide various notices to those ends, and execute various requests upon receipt of a verifiable consumer request, as specified; and provide certain mechanisms for consumers to make their lawful requests, including a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's internet homepage to enable consumers, or a person authorized by the consumer, to opt-out of the sale of the consumer's PI. (Civ. Code Sec. 1798.100 et seq.)

3) Prohibits a third party from selling PI about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out as specified. (Civ. Code Sec. 1798.110(d).)

4) Provides various exemptions under the CCPA, including for, among other things:

   - The sale of PI to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined under specified federal regulations, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).

   - PI collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), or the California Financial Information Privacy Act (Fin. Code Sec. 4050 et seq.) (Civ. Code Sec. 1798.145.)

5) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill, defines the following terms:

   - "Business" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' PI, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' PI, that does business in California, and that satisfies one or more of the following thresholds:

     - Has annual gross revenues in excess of $25,000,000, as adjusted as specified.

     - Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the PI of 50,000 or more consumers, households, or devices.

     - Derives 50% or more of its annual revenues from selling consumers' PI.

   - "Third party" means a person who is not any one of the following:

     - The business that collects the PI.

     - A person to whom the business discloses a consumer's PI for a business purpose, pursuant to a written contract that prohibits, among other things, the recipient from selling the PI, or retaining, using, or disclosing the PI outside the direct business relationship between the person and the business.

   - "PI" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. PI includes certain specific types of information, if that information identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. These include, for example:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- Characteristics of protected classifications under California or federal law.
- Commercial information, as specified.
- Professional or employment-related information.
- Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act.

PI does not include publicly available information, as specified. Among other things specifies that for these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, as specified. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

- "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to another business or a third party for monetary or other valuable consideration. For purposes of the CCPA, a business does not "sell" PI when, among other things:
  - A consumer uses or directs the business to intentionally disclose, as specified, PI or uses the business to intentionally interact with a third party, provided the third party does not also sell the PI, unless that disclosure would be consistent with this bill.
  - The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's PI for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's PI.
  - The business uses or shares with a service provider PI of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) the business has provided notice that information being used or shared in its terms and conditions, as otherwise specified under the bill; and (ii) the service provider does not further collect, sell, or use the PI of the consumer except as necessary to perform the business purpose. (Civ. Code Sec. 1798.140.)

6) Provides for specified enforcement of the CCPA. Provides a limited private right of action for any data breach, as specified, and otherwise provides the AG with enforcement authority for the above rights and obligations, as specified. Further provides that any civil penalty assessed, and the proceeds of any settlement of an action, shall be deposited in the Consumer Privacy Fund, created within the General Fund with the intent to fully offset any costs incurred by the state courts and the AG in connection with the act. (Civ. Code Sec. 1798.155.)

7) Establishes an address confidentiality (or Safe at Home) program within the Office of the Secretary of State in order to enable state and local agencies to both accept and respond to requests for public records without disclosing the name or address of a victim of domestic violence, sexual assault, stalking, elder or dependent adult abuse, or human trafficking, as well as well as reproductive health care workers (Gov. Code Sec. 6205 et seq.)

8) Prohibits a person or business from knowingly and intentionally publicly posting or publicly displaying on the internet the home address, home telephone number, or image of a program participant (or individuals residing at the same address) with the intent to threaten or incite a third person to cause imminent great bodily harm to the participant or co-resident. (Gov. Code Sec. 6208.1(a).)

9) Prohibits a person or business from knowingly and intentionally publicly posting or publicly displaying on the internet the home address, home telephone number, or image of a program participant if the participant has made a written demand of the person or business to not disclose the home address or telephone number, as specified. (Gov. Code Sec. 6208.1(b).)

10) Prohibits a state or local agency from posting home address or telephone number of any elected or appointed official on the internet without first obtaining the written permission of that individual. (Gov. Code Sec. 6254.21(a).)

11) Prohibits any person or business from knowingly post the home address or telephone number of any elected or appointed official, or of the official's residing spouse or child, on the internet, as specified, and intending to cause imminent great bodily harm or threatening to cause imminent great bodily harm to that individual. (Gov. Code Sec. 6254.21(b).)

12) Prohibits a person or business from publicly posting or displaying on the internet the home address or telephone number of any elected or appointed official if that official has made a written demand to not disclose his or her home address or telephone number, ,as specified. (Gov. Code Sec. 6254.21 (c).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to create a registry of data brokers so that California consumers may better know what businesses to contact in order to opt-out of the sale of their PI. This bill is author-sponsored.

2) **Author's statement**: According to the author, "the data industry is both pervasive and poorly understood by consumers. This bill would better allow privacy conscious consumers to exercise their rights granted under CCPA and develop a more thorough understanding of the data industry's scope and practices. It will also allow for a modicum of oversight over an industry that has so far been allowed to thrive with little to no obligations to the public or to the individuals whose personal information provides the foundation for their industry. In a world where an individual's real time location, arrest record, rental history, or court filings are available online, and conveniently aggregated for purchase, people deserve, at a minimum, to know who is collecting information about them, and to have the ability to opt-out of the sale of their personal information. AB 1202 would consolidate data brokers into one easily accessible list so that consumers may exercise their rights."

3) **Background**: As of 2016, there are over 286,942,747 internet users in the United States, and that number is increasing by approximately one user per second. Every internet user creates a "digital footprint," or a record of every action the user takes on the web. These footprints contain public activity, such as posts and comments made on social media websites, as well as more sensitive activities, such as cookies that follow a user from website to website, or archived lists of all the terms entered into a browser's search bar.

Data brokers (generally businesses operating without any direct relationship with individual consumers), collect and sell this information without the knowledge of the individuals to whom the information relates. As an industry, data brokers have existed in the shadows and have largely been able to operate outside of any meaningful regulation, and until recently, public scrutiny.

That being said, the industry has arguably also provided a number of services that support integral functions in modern society, as indicated in the findings and declarations of this bill. Specifically, "[d]ata brokers may provide information that can be beneficial to services that are offered in the modern economy, including credit reporting, background checks, government services, risk mitigation and fraud detection, banking, insurance, and ancestry research, as well as helping to make determinations about whether to provide these services."

However, while data brokers may offer benefits, there are also risks associated with the widespread aggregation and sale of data about consumers. California has long protected the information of certain individuals, including survivors of domestic violence and elected officials, from public disclosure. (*See, e.g.*, Gov. Code Secs. 6205 et seq. and 6254.21.) However, without the ability of these individuals to contact data brokers and request that their PI not be sold, these protections can be rendered meaningless. The Federal Trade Commission (FTC) has long been concerned regarding the business practices of data brokers. In fact, as early as 2012, the FTC proposed "targeted legislation" to regulate the industry in a report on consumer privacy. The report notes:

> To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation […] that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain. (FTC, *Protecting Consumer Privacy in an Era of Rapid Change: recommendations for businesses and policymakers* (Mar. 2012).)

The FTC reiterated this proposal in a 2014 report focused specifically on data brokers. (FTC, *Data Brokers: a call for transparency and accountability* (May 2014).) However, at the federal level, no specific data broker legislation has been enacted. At the state level there has been more movement and last year Vermont enacted a first-of-its kind data broker regulation which imposes several specific requirements on data brokers, including:

- Registration: Data brokers, defined as a business that collects and sells/licenses information to third parties about consumers with whom the business does not have a direct relationship, have to register annually with the Vermont Secretary of State.

- Disclosures: The annual registration calls for a variety of mandatory annual disclosures, including, among others:

    - If the data broker permits a consumer to opt-out of the data broker's databases or data collection, how to do so, and whether such opt-outs are limited.

    - Whether the data broker requires purchasers of its information to be credentialed.

    - How many security breaches the data broker experienced in the last year, and how many consumers were affected.

    - If the data broker knows it possesses information about minors, a separate statement detailing data collection practices, sales activities, and opt-out procedure applicable to that information.

- Mandatory information security: Data brokers have to develop, maintain, and implement a "comprehensive information security program" to protect PI with administrative, technical, and physical safeguards appropriate to the size and scope of the business. Data brokers must also, among other things, designate employees to maintain the program, make risk assessments and implement subsequent mitigation processes, adopt security policies, and regularly monitor and update the security program. (H.764 (Act 171).)

Late last year, the Electronic Frontier Foundation (EFF) applauded the State of Vermont on its new privacy protective law, but warned Vermont's legislators to not rest on their laurels. EFF additionally noted that Vermont's new law "demonstrates the many opportunities for state legislators to take the lead in protecting data privacy. It also shows why Congress must not enact a weak data privacy law that preempts stronger state data privacy laws." (Schwartz, *Vermont's New Data Privacy Law*, EFF (Sept. 2018).)

Following in Vermont's footsteps, this bill seeks to enhance consumer privacy protections for California consumers by creating a data broker registry to which consumers may refer when seeking to exercise related rights afforded to them by California law. Such right, discussed further below include, for example, how data brokers collect and use consumer data. In support, the Media Alliance and Oakland Privacy write:

> [AB] 1202 is primarily a transparency bill that allows consumers to exercise their privacy rights as they desire without being blocked or impeded by the inability to locate or identify a third party broker who has acquired their data. The [California] Legislature acted in 2018 to give consumers a nationally unrivaled ability to seek and receive information about how their personally identifiable information has been sold, and if they desire, to take action to prevent further dissemination of their information without their consent. But that right, in order to be fully vested, requires consumers to be able to locate and contact recipients of their data to express their preference. This is an action that can be difficult in the shady world of third party data brokers. [AB] 1202 would provide a simple solution without greatly increasing administrative burden by employing a straightforward licensure process.

4) **California consumers now have the right to opt-out of the sale of their PI**: Last year, the Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their PI, including: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt out of the sale of their PI, or opt-in in the case of minors under16 years of age. While the CCPA gives consumers more opportunities to control the use and sale of their PI, consumers have little practical ability to enforce their rights against businesses that they do not know exist. As noted by Apple CEO, Tim Cook, earlier this year:

> [O]ne of the biggest challenges in protecting privacy is that many of the violations are invisible. For example, you might have bought a product from an online retailer – something most of us have done.
>
> But what the retailer doesn't tell you is that it then turned around and sold or transferred information about your purchase to a 'data broker' – a company that exists purely to collect your information, package it and sell it to yet another buyer.
>
> The trail disappears before you even know there is a trail. Right now, all of these secondary markets for your information exist in a shadow economy that's largely unchecked – out of sight of consumers, regulators and lawmakers. (Cook, *You Deserve Privacy Online. Here's How You Could Actually Get It*, Time (Jan. 2019).)

On this subject, California took large strides toward better protecting consumer data last year with the enactment of the CCPA. Of particular relevance to this bill, the CCPA governs data brokers that meet the thresholds in the CCPA definition of business, but consumers need to know how to locate data brokers before they can take steps to exercise the particular rights granted under the CCPA. To that end, the CCPA requires third parties who are sold PI from other businesses to provide consumers with explicit notice and the opportunity to opt-out of the sale of their PI. In the case of data brokers, explicit notice may become difficult when there is no direct relationship with the consumer and the data broker does not have the consumer's current contact information. Accordingly, this bill would require data brokers, defined generally as businesses that are buying and/or selling the PI of consumers with whom they have no direct relationship, to register with the AG. The AG would then be required to create a registry on its website. Under the CCPA, businesses (including data brokers) are required to provide consumers with contact information so that consumers may inquire as to what types of information are collected and sold about them, and businesses are also required to provide consumers with a simple method of opting out of the sale of their information. By providing tools so that consumers may discover what businesses collect and sell PI about them, the registry required by this bill would help consumers better enforce their rights under the CCPA.

To a large extent, data brokers collect and sell information that is found online and in public records, or in other words, publicly available. The definition of PI relied on by this bill provides that "publicly available" information is not PI, but with an important caveat. Specifically, the definition provides that "[i]nformation is not 'publicly available' if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained." (Civ. Code Sec. 1798.140(o)(2).) Accordingly, this bill would cover data brokers who sell

publicly available information if the information is not being used for its intended purpose. For example, information from property record (which is generally intended to prove chain of title), would be covered if the data broker was selling it for advertising purposes, allowing a consumer to opt-out of the sale of that information.

In opposition, a coalition of advertising and marketing trade associations (coalition) urge the Committee to take additional time to consider the unintended consequences of the bill. The coalition specifically argues the following:

- The bill's registration requirement does not provide consumers with new or helpful information.

- The bill would create enormous new responsibilities for the Attorney General at a time when that Office is burdened with responsibilities pertaining to the CCPA.

- The bill's transparency and opt-out provisions are duplicative of the CCPA, may conflict with the CCPA, [thereby] hurting consumers and undermining the goals of the CCPA.

The lack of transparency regarding the data broker industry and consumers' lack of awareness as to the industries practices has been well documented. As discussed in Comment 3, above, the industry has long been a focus of the FTC specifically because of the industry's business practices. To the extent that consumers who visit the registry will be able to see a list of businesses that they otherwise would not know exist, the information provided by this bill would indeed be new and helpful. Additionally, if the transparency and opt-out provisions are duplicative of the CCPA, then the bill would arguably not require any additional action from industry.

Further, staff notes that the bill's definition of "data broker" is intentionally narrow and excludes industries and information that are governed under different statutory themes, as to not overly regulate or burden industries that are complying with industry-specific privacy laws. Specifically, this bill would exempt financial institutions subject to the Gramm-Leach-Bliley Act, consumer reporting agencies subject to the federal Fair Credit Reporting Act, and insurance companies subject to the Insurance Information Privacy Protection Act, from the requirements of the bill. Each of these industries have statutory schemes narrowly tailored to the type of service they provide, and give consumers other resources they can access to exercise their rights.

5) **Administration and enforcement of registry**: This bill would require data brokers, as defined, to register with the AG, and would allow the AG to determine a registration fee, not to exceed the reasonable costs of regulation. The bill would subject each data broker who fails to register to a civil penalty of $100 per day, plus the fees that were due during the period that it failed to register, and any expenses incurred by the AG in the investigation and prosecution of the action. Any penalties, fees, and expenses recovered would be deposited in the Consumer Privacy Fund, a fund created by the enactment of the CCPA with the intent to fully offset any costs incurred by the state courts and the AG in connection with the CCPA.

As noted in Comment 3, above, this bill is modeled to a certain degree after the new Vermont law regulating data brokers. In Vermont, data brokers must register with the Secretary of State and enforcement for violations of the law is provided by Vermont's Attorney General.

This bill, by comparison, would assign the AG with both the creation and maintenance of the registry and the enforcement for violations of obligations created under the bill. Tasking with AG with the development and maintenance of the registry is arguably appropriate in California, where the AG is not only the exclusive public enforcement authority of the CCPA, but the AG also provides a robust library of privacy information and resources for Californians on the Department of Justice's (DOJ) public website. The "Privacy Enforcement and Protection" page of that website notes that "[i]n the 21st century, we share and store our most sensitive personal information on phones, computers and even in 'the cloud.' Today more than ever, a strong privacy program, which includes data security, is essential to the safety and welfare of the people of California and to our economy." The page also connects viewers with links to resources and further describes the role of the Department of Justice's Privacy Enforcement and Protection Unit to "enforce state and federal privacy laws," and "empower Californians with information on their rights and strategies for protecting their privacy." (DOJ, *Privacy Enforcement and Protection,* <https://oag.ca.gov/privacy> [as of Mar. 17, 2019].)

6) **Prior legislation**: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment 4.

SB 1121 (Dodd, Ch. 735, Stats. 2018) ensured that a private right of action under the CCPA applies only to the CCPA's data breach section on and not to any other section of the CCPA, as specified, corrected numerous drafting errors, made non-controversial clarifying amendments, and addressed several policy suggestions made by the AG in a preliminary clean-up bill to AB 375.

SB 1348 (DeSaulnier, 2014**)** would have required a data broker, as defined, to permit an individual to review the personal information that the data broker holds about them and to request that the data broker cease selling, or otherwise sharing, that personal information to third parties, except as specifically allowed. This bill was never heard in the Assembly Committee on Arts, Entertainment, Sports, Tourism & Internet Media.

REGISTERED SUPPORT / OPPOSITION:

Support

Media Alliance
Oakland Privacy

Opposition

American Advertising Federation
American Association of Advertising Agencies
Association of National Advertisers
Interactive Advertising Bureau
Network Advertising Initiative

Analysis Prepared by: Nichole Rapier / P. & C.P. / (916) 319-2200