Data Broker Transparency FAQ – HB 2052

Simplified description of what this bill does:

This bill applies to business entities that do not have a direct relationship with residents of Oregon and that collect and sell or license our personal information.

Those entities must register with DCBS and provide the public with information about who they are and whether we can opt out of the collection and sale or licensing of our personal information. If we can opt out, they have to tell us how.

What data is covered by this bill?

We've defined the scope of data we are talking about as "brokered personal data." We used this term to be very clear that this definition only applies to this law.

That's important, because defining what is included in personal data is actually quite complex. These definitions need to be different, depending on what is being regulated.

In this particular bill, "brokered personal data" is data that identifies or can be reasonably associated with us. That does not include deidentified data or aggregated data. So again, it is only data that can point back to us.

Who has to register?

This bill applies to business entities who collect and sell or license "brokered personal data."

The bill does not apply to state and local government.

This bill does not apply to business activities that are already regulated by the federal Fair Credit Reporting Act (FCRA) or the federal Gramm-Leach-Bliley Act (GLBA).

> The FCRA protects information collected by consumer reporting agencies such as credit bureaus, medical information companies and tenant screening services.
>
> The GLBA requires companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
>
> Because these federal laws already require transparency by the activities they regulate, we are not creating redundant regulations here at the state level.

For example, insurance companies are already subject to both of these federal laws and additional state laws that strictly regulate their use of personal information. So, activities insurance companies engage in that are regulated by these federal law are exempt under this bill.

The bill does not apply to entities that have a past or present direct relationship with the individual whose information is being sold. Examples of that direct relationship include, for example:

A business and its customers.

A business and individuals it has a contractual relationship with.

Employers and employees.

DCBS has rulemaking authority to expand this list. Although we have over 135 people (with diverse perspectives) on our task force distribution list and have vetted the bill with this group, something might come up during implementation, and this will allow us to be nimble and make adjustments if needed.

We have also included exemptions for a number of activities that aren't what we consider data brokering, including:

Providing business or professional directories, health and safety alerts, information that is available from government records, and directory assistance.

Activities that involve the distribution of media, such as newspapers, periodicals and more.

We've also made it clear that a one-time or occasional sale of the assets of business that is not part of the ordinary conduct of a business is exempted.

Does an entity that collects and stores brokered personal data in its business databases for internal use only, with no intention of disseminating outside the business have to register?

No, internal use does not involve a sale. Internal use only does not trigger the registration requirement.

Does the sale of publicly available health care professional information or provider directories require registration?

No, this is covered by exemption for "[p]roviding publicly available information that is related to a resident individual's business or profession."

Illustration of an entity that does not have to register because they only sell deidentified data:

A business serves a data function for hospitals and government entities. It collects identifiable data under contract with the state. It then uses data to count individuals seeking care across the state. Data is provided for research, public health or healthcare operations. Data that is provided to customers is not identifiable. For example, data may show how many patients in a particular zip code have a specific medical condition or have been to the hospital for a mental health issue.

Identifiable data can also be stripped of certain personal identifiers to create de-identified data sets. These data sets can then be analyzed to understand a particular population and are commonly used for research. The goal of deidentification is to transform data in a way that protects privacy while allowing individuals to make inferences drawn on that data. Federal technical standards exist for deidentification, including under the HIPAA privacy rule, at 45 CFR § 164.514, and publications from the US Department of Commerce's National Institute of Standards and Technology.

The key reason this entity does not fall under the registration requirement of the data broker bill is that the data it provides to its customers cannot "reasonably be associated with a resident individual." Although the entity collects identifiable data, it is not identifiable at the time that it is provided to its customers. Our bill requires registration only when identifiable data is collected and sold or licensed. Collection of identifiable data alone is not sufficient to require registration. Identifiable data must also be sold (in an identifiable state) to trigger registration.

Illustration of an entity that does not have to register because they are acting as an agent of an entity with a direct relationship with a resident individual (in the context of HIPAA-covered entities):

HIPAA-covered entities may sell personal health information in very limited circumstances: for research. This can only be done with patient consent. When this occurs, the entity has a direct relationship with the patient, which falls outside the definition of a data broker. Some HIPAA-covered entities may contract with "business associates" as those entities are defined under HIPAA. Those entities may assist the covered entity by acting as an agent of the covered entity in a transaction that involves compensation paid for the transfer of data for research purposes.

Here, the business associate is acting merely as an agent of the covered entity, and the covered entity has a direct relationship with the patient. Thus, the business associate falls outside the definition of data broker under our bill.

How will DCBS implement this?

DCBS will likely be using the Nationwide Multistate Licensing System & Registry (NMLS) as the service where data brokers will register and their information will be provided for the public.

This is a service that DCBS already uses for other purposes. This service and administration by DCBS will be paid for with funds collected as a registration fee.

DCBS will also have authority to impose civil penalties for failure to register.

What is a sale?

"Sale" is intended to be consistent with the common definition of this term.

This bill uses the term "another person", while other state laws use the term "third party." Are these the same?

Yes, Oregon drafting conventions are to use the words "another person" to describe what other state laws describe as a "third party."

This FAQ was prepared by the Oregon Department of Justice and updated on January 17, 2023.

Contact:
Kate Denison, Deputy Legislative Director, 971-599-9851, kate.e.denison@doj.state.or.us
Kimberly McCullough, Legislative Director, 503-931-0418, kimberly.mccullough@doj.state.or.us