

Attorney General Remarks
House Bill 4017 – Data Broker Registry
House Business and Labor Committee
1 PM, February 2, 2022
As prepared for delivery

Good Afternoon, Chair Holvey, Vice-Chairs Bonham and Grayber, and members of the committee. My name is Ellen Rosenblum and I am the Attorney General for the State of Oregon. I had the chance to talk with you about this concept at an informational hearing in November, and I am pleased to appear before you again, this time in support of HB 4017.

Since I first took office as Attorney General in 2012, I am pleased we have partnered together to advance crucially important privacy and security protections for children, students and consumers. I am proud of all we have accomplished so far to keep Oregon abreast of ever-changing developments in the intersection of privacy and technology, from strengthening Oregon’s data breach law, to ensuring that smart devices we use every day are equipped with reasonable security features, to limiting the use of K-12 student personal information provided to Ed tech companies throughout the school day.

In recent years, consumers, advocates, and policymakers—that’s most of us— have become increasingly concerned about the vast amount of consumer data collected by companies and how this personal information is sold, shared and used. Most of us no longer feel we have control over our online privacy—and our feelings are borne out by reality.

In June of 2019, we formed the Attorney General’s Consumer Privacy Task Force to answer the growing call for comprehensive state consumer privacy legislation with the goal to give Oregon consumers more control over our personal information. This remarkable group of experts and advocates now includes over 100 participants from all over the country.

The task force efforts continue, and we plan to bring you a comprehensive consumer privacy bill in 2023. Our goal is for a law that will provide Oregonians with key protections, like the right to know how our personal information is being used, the right to correct errors in the data, more control over how and whether data is processed by a company, and special protections for children and minors.

In the meantime, HB 4017 is an important consumer protection and transparency bill that will shed some light on data brokers, a \$232 billion dollar industry that I hope you will agree has been operating under the radar for long enough. This is not a task force bill, but we have worked closely with that group of stakeholders to develop the legislation and ensure that it is both workable for businesses and useful to consumers.

The data broker registry we are proposing is a simple tool that will help shed some light on how this unchecked industry is operating and how we can protect our digital privacy in doing so.

Data brokers are companies you’ve likely never heard of that collect and sell information about YOU—who you are, what you buy, where you shop, what you click on, and what websites you visit. They

know an awful lot about you: your birth date, your children's birth dates, where you live, where you work, where your kids and grandkids go to school, your religion, your income, your education level and what size clothing you wear. They source all of these details about you, your life, and your habits – then they bundle it all up and sell it, mainly to advertising companies, but also to insurance companies and even to members of the public.

Most consumers would be shocked to know that companies like Spy Dialer, Swordfish AI, LoopMe Inc or True Influence LLC know more about them than most of their neighbors do. Now it's our turn to know more about who's out there, under the radar, monetizing our personal information!

It's one thing for a consumer to willingly turn over her personal information for a specific purpose. But the widespread sale of data, often done without consumer's knowledge, let alone our consent, gives data brokers broad latitude to do whatever they want with it. Consumers have no direct relationship with data brokers, yet this industry continues to thrive, largely unregulated.

As described in a recent Wired article,[\[1\]](#) data on hundreds of millions of Americans' races, genders, ethnicities, religions, sexual orientations, political beliefs, internet searches, drug prescriptions, and GPS location histories are for sale on the open market. and there are far too many advertisers, insurance firms, predatory loan companies, law enforcement agencies, scammers, and abusive domestic and foreign individuals willing to pay for it.

On December 7, 2021, the U.S. Senate Committee on Finance Subcommittee on Fiscal Responsibility and Economic Growth convened a hearing to bring to light a number of ongoing issues concerning data brokers. Committee members and witnesses outlined growing concerns with the indiscriminate sale of individuals' personal information and the potential consequences of that data falling into the wrong hands.

Witnesses explained how, even without stringing together full profiles, single pieces of various data can be equally effective to target an individual with the right amount of inference. Justin Sherman, a research fellow who studies the data brokerage industry at Duke University's Sanford School of Public Policy, explained some of the common data inference scenarios he's seen, including information belonging to U.S. military personnel, victims of intimate partner violence, and individuals with mental health conditions.

We should indeed be very concerned about what this practice means for the most vulnerable members of our community. Data brokers have sold lists of addresses for domestic violence shelters; police officer and sheriffs' home addresses; people with gambling or substance use disorders, and consumers who might take out payday loans, including targeted minority groups.

Irresponsible behavior by data brokers has included making available survivors' contact information to their offenders, using personal information to enable racial and ethnic discrimination, enabling doxing behavior and providing information on seniors who suffer from dementia.^[6]

Of course, the data broker industry includes some reputable companies that are crucial to the modern economy, but I hope we would all agree that when companies use our personal information for profit, it should be incumbent upon them to operate responsibly and with transparency. And that's what this bill is about. Certainly that is not too much to ask when so much is at stake.

The data broker registry we are proposing is simple. It is modeled after similar programs in California and Vermont, where almost 500 data brokers have already registered. Our proposal will require these companies to register with the Department of Consumer and Business Services and pay a fee in an amount that will support the program. The data broker must provide contact and other business information that will be posted on a public-facing website hosted by DCBS.

Consumers will be able to use the registry to contact data brokers directly and ask what information the broker has on them, and request that the broker no longer sell their personal information—called opting out. And, when Oregon adopts a comprehensive privacy law, this registry will be a valuable resource for consumers to assert their rights and for the Oregon Department of Justice to advocate for consumers.

Thank you for this opportunity to advocate for this relatively simple—but very important—bill that will help protect our privacy—yours, mine and all Oregonians. I am joined today by my Legislative Director Kimberly McCullough, who is going to share more detailed information about HB 4017 and answer any technical questions you may have.