DATA BROKERS, DATA PROVIDERS, PUBLIC RECORDS, AND REGULATION: FINDING THE RIGHT BALANCE

CSPRA
COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Executive Summary

Who We Are

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public records access. We represent data providers who follow the laws, enable useful transactions and societally beneficial activities, and who are responsible data stewards and corporate citizens. Data providers are part of the larger information industry on which much of America's prosperity, opportunity, and influence depend.

How Do Data Providers Provide Benefits to People?

A data provider gathers, curates, protects, and provides the data elements necessary to, and lawfully used for, **completing transactions, preventing fraud and harm, setting fair rates, meeting a legal requirement, enforcing the law or a contract, enabling communications with current and prospective customers, and making a variety of decisions.** The data they use to create these value-added services come from public records and private sources. Data provider services **include customer-initiated activities used in support of a customer service function or used to protect customers or the provider of a service from fraud, contract violations, misuse of resources, illegal activities, and other various harms.** Many of these services are part of licensed and/or regulated industries or government activities like insurance, credit, law enforcement, banking, employment, housing, transportation, consumer product safety recalls, federally required automotive recalls, civil legal processes, investing, child support recovery, and supply management to name a few.

Data Providers Level the Playing Field for Businesses and Governments by Providing Valuable and Cost-Effective Access to Data to the Benefit of All

A substantial amount of the data provider products and services are sold in a business-to-business or business-to-government (B2B/G) model. **Many of the more than 33 million small businesses in the US and thousands of government entities** cannot efficiently or affordably acquire or provide the data they need by themselves. Businesses and governments use the

Executive Summary Continued

economies of scale of data providers to save or gain billions of dollars in efficiencies, improved outcomes, and revenue and job growth. **If the government had to respond individually to all the public records needs of businesses, individuals, and other government entities, it would require many billions of dollars in new technology and staff.** If data provider services and resale were prevented by law or regulation, it would **paralyze the economy as many transactions and safety protections would be delayed or impossible to conduct.**

What Benefits Do Data Providers and the Larger Information Industry Provide for Customers, Consumers, Government, and Society?

Data providers produce value-added services, including protection of children and seniors, lending, oversight of government, child support enforcement, safety recalls, improved newsgathering, and economic forecasting. Data providers provide the capacity to enhance public safety, facilitate commerce, and reduce government and business costs and inefficiencies. In a single year, public records and data providers play a key role in the:

- Purchase of over **6 million residential homes**
- Sale of over **14 million new** vehicles and over **36 million used** vehicles
- Notification of tens of millions of **automobile recall notices** affecting an average of over **34 million Americans**
- Issuance of over **21 million passports and travel cards**
- Creation of **quality-of-care reports protecting over 7 million children** (under age 5} in day care and over **8 million adults** receiving long-term care
- **Detection of fraud and fair underwriting of 692 million insurance policies** (291 million life, 167 million health, and 234 million auto), and
- Checking the **performance, quality, and stability of 20,800 financial institutions** (6,800 banks, 13,000 credit unions, and 1,000 savings and loans).

These are the kinds of everyday activities made possible or far more efficient because of data providers and public records, which should be protected in any legislation:

- **Buying or selling a home**
- **Choosing a care provider**
- **Protecting vulnerable populations**
- **Fairer and faster insurance and loan transactions**
- **Buying a car**
- **Getting a job**
- **Starting and running a business**
- **Enabling commerce**
- **Traveling abroad**
- **Helping enforce the law**
- **Secure payments of obligations**
- **Keeping people safe**
- **Preventing fraud and identity theft**

FINDING THE RIGHT BALANCE

Overview

Much of the discussion about data these days is done in the context of proposals to increase regulation of what is broadly and inaccurately called the data broker industry. We will not use the term data brokers in this paper (except where it is used in law or common phrasing) as that phrase has been reduced to an epithet that paints all who have a business that uses data as villains. We represent and choose to discuss the work of data providers who follow the laws, enable useful transactions and societally beneficial activities, and who are responsible data stewards and corporate citizens. In doing so, we encourage policymakers and thinkers to consider such useful distinctions when discussing and proposing regulations. Data providers are part of the larger information industry on which much of American prosperity, opportunity, and influence depends. The paper begins with a look at that industry, places data providers in the information industry context, discusses a general regulatory approach, and spells out the benefits that may be affected by new regulations.

How Do Data Providers Provide Benefits to People?

A data provider gathers, curates, protects, and provides the data elements necessary to and lawfully used for completing transactions, preventing fraud and harm, rate determinations, meeting a legal requirement, making a judgment, enforcing the law or a contract, or making various decisions. Data provider services support customer-initiated activities and customer service. These services also protect customers or the provider of a service from fraud, contract violations, misuse of resources, illegal activities, and various harms. Many of these services are part of licensed and/or regulated industry or government activities like insurance, credit, law enforcement, banking, employment, housing, transportation, consumer product safety recalls, federally required automotive recalls, civil legal processes, investing, child support recovery, and supply management.

Existing Privacy Regimes Should Be Exemptions In Any New Laws or Regulations

Much of the data used in data provider services are public records and publicly available information. Such data either:

- Is already considered public data and, therefore, does not have privacy implications; or
- Is governed by the terms of public records law which determines what information is accessible, to whom, and for what purposes.

All states and the federal government have a comprehensive public records law that restricts access to some records and limits uses and users of others. They also have special-purpose public records acts that address such things as criminal background data or personal information contained in state motor vehicle records. The states and the national government regulate the use of data from public sources by law, rule, and contract terms. The contract terms require a variety of mechanisms to ensure the security and lawful use of public records by data providers. Given the legal and contractual protections and protections granted under the First Amendment, it has been broadly acknowledged that public records do not need a separate privacy regime. All adopted state omnibus privacy laws and the Uniform Law Commission Uniform Data Privacy Act specifically exempt lawfully acquired publicly available information which includes public records, widely available information, and self-publicized data.

Furthermore, these omnibus privacy laws recognize that we have adopted numerous context-specific national privacy laws and that those statutes should govern regulation and rights within those fields. These include **Gramm-Leach-Bliley Act (GLBA), Fair Credit Reporting Act FCRA), Drivers Privacy Protection Act (DPPA), Federal Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA),** and others. Any data provider laws and regulations should adopt the same approach and exempt these areas and any lawfully acquired publicly available information.

Data Providers Level the Playing Field for Businesses and Governments by Providing Valuable and Cost-Effective Access to Data to the Benefit of All

A substantial amount of the data provider products and services are sold in a business-to-business (B2B/G) model. Many of the more than 33 million small businesses in the US and thousands of units of government cannot efficiently or affordably get or provide the data they need by themselves. Businesses and governments use data providers to save or gain billions of dollars in efficiencies, improved outcomes, and revenue and job growth. Businesses, governments, their employees, their customers, our economy, and our society receive the benefits from the economies of scale the data providers can offer. Many free-to-use and advertising-supported services depend on data providers to provide the means of delivering value to the advertisers and users of the service. The value provided by the B2B/G part of the information industry is often invisible and simply taken for granted. It is not surprising that many people are not aware of how dependent we are on data providers for so many things we do in life. What is surprising is the lack of concern CSPRA sees for regulations and laws that damage the efficiency and availability of the data from data providers for these many essential purposes. Treating responsible and accountable data providers like unregulated black-market peddlers of private data does not address the harms that are occurring from the misuse of private data by bad actors.

Are All Brokers Villains?

We do not think so, but how can we make distinctions that preserve the socially beneficial work of data providers and the information industry and better address privacy concerns and the harms caused by bad actors?

Let us first explore what a broker is. We often have an overwhelming number of choices in goods, services, information, and any number of similar things we can generally call resources. A broker is a person or entity with access to a needed resource, the expertise to advise customers which ones are the best choice for them, acquire the resource, ensure its delivery, and manage it beyond the initial acquisition.

Brokers, in this broad view, are all around us—not all of which have “broker” in their name like stock, information, insurance, or real estate brokers do. Healthcare workers and entities, lawyers, concierges, airline seat aggregators, auto sellers, manufacturers, logistics companies, news organizations, data sources, many web-based apps and sites, governments, and so on act as brokers. However, we generally consider them as providers of goods and services and do not lump them all under some broker heading just to demean what they do. There is nothing inherently wrong with being a broker and we dismay at

the word being misused in this way. These providers listen to their markets, constituents, and customers, set up supply channels, and meet the constituent's and customer's needs. Having efficient and well-organized providers who can function as honest brokers serves our economic and societal interests as it encourages competition among suppliers, reduces friction in transactions, gives more informed choices, better serves needs, and creates a more efficient and functional society.

Providers vary in type, quality, importance, and value to users and society. Treating them all the same or demeaning them with overbroad terms and assumptions does not advance our common interests. In all the examples above, there are always bad actors who give that kind of provider, business, government, or brokerage a bad name. Assuming all who help to "broker" lawful activities are bad or that any entity in each category is the same as all the others is a logical fallacy that limits our ability to make useful distinctions, focus on harmful and illegal behavior, and respond appropriately.

The truth is that the phrase "data broker" has become a caricature or epithet that has clouded our understanding of what various information industry entities do and their value.

The data broker label has been indiscriminately slapped on large swaths of the information industry. The information industry is one of the largest in the world, with many distinct and overlapping players. We understand the instinct to try and simplify things with a single label. But it distorts the reality of the industry to see all the parts and parties as the same. This distortion is advanced most frequently by those whose main concern is selling security products or advocating for a specific privacy philosophy. They describe all as personal information collectors and dossier builders acting outside of any controls who are destroying privacy, democracy, fairness, and equality, as well as perpetrating a litany of claimed harms. CSPRA does not approach this problem as a battle between good and evil but rather as an ongoing set of challenges where the only sustainable strategy for policymaking is continuously balancing the interests, rights, responsibilities, harms, and benefits as the information industry and society co-evolve.

What Exemptions Should Be Considered in Regulation?

Data providers support activities by individuals, businesses, and government that are essential to our daily lives, economy, and safety. Often, the data and/or activities are either public or already the subject of substantial regulation or privacy and consumer protective statutes. For this and the many reasons stated above, the data used or regulated under existing statutes, including general and special purpose public records laws, have commonly been exempted from state privacy laws. The Uniform Law Commission's Uniform Data Privacy Protection Act also includes these exemptions. We recommend that any new federal or state laws or regulations follow this example and include strong public records and publicly available information exemptions and exempt uses already regulated by federal law. We recommend that any new federal and state laws and regulations specifically address any behaviors that create real harm and not regulate the data provided or single out a subclass of the entities providing it.

Cutting through these recommendations is the idea of looking more carefully at what is being done with the data and whether that is part of a consumer-initiated transaction, an activity regulated by other laws or

Data providers support activities by individuals, businesses, and government that are essential to our daily lives, economy, and safety.

privacy regimes, or designed to prevent harms like fraud, identity theft, theft of services and property, terrorism, threatening behavior, bodily harm, and so on. These activities need exemptions or leeway to function with a lighter touch of regulation. Two examples of these kinds of exemptions and the rationale for them are given below. We also think that activities that enable ads to support news, media, and entertainment need protection, as do any press activities and other First Amendment speech. We must preserve our rights to know, learn, investigate, discover, infer, think, and speak in our information and data-rich society. Advertising support is crucial to many things we enjoy every day, and we need to find the proper balance between marketing and privacy and not simply ban marketing uses of data.

Public Safety & Security Exemptions

Reputable businesses in the information services sector play an important role in the work law enforcement and government agencies perform daily. Investigators and government workers rely on fast and accurate information, particularly when it comes to stopping crime, investigating suspects, and finding missing children. Their access to data that is continuously maintained and updated by an information service provider is an essential tool critical to their success.

While it is possible that the data provided by information services providers could be obtained by a government entity directly, this would be an enormous undertaking. Law enforcement or government agencies would have to enter into separate licensing agreements with each data source, develop a mechanism to continuously collect, store, and make available the information through an aggregation vehicle, and put into place safeguards to both comply with existing laws and regulations and prevent a breach. The risk of building a system in-house is far too high and cost prohibitive. Practically speaking, exempting businesses that currently have the infrastructure in place to continuously remain compliant and preserve the data is a cost-effective solution.

Fraud Prevention & Remediation Exemptions

In an era characterized by rapid technological advancements, it's paramount that businesses collaborate with law enforcement agencies, furnishing them with the requisite tools and resources to safeguard society. The recent surge in fraudulent activities, especially within state and federal assistance programs during the pandemic, underscores the importance of this partnership. By bridging the technological divide, we can bolster our collective security mechanisms, ensuring that fraudulent actors are swiftly identified and held accountable.

While we emphasize strengthening our defenses, we must concurrently prioritize the prevention of fraud, particularly in programs crucial to our nation's well-being. The Government Accountability Office's findings on the vulnerabilities in the Unemployment Insurance System are a stark reminder of the costs associated with neglecting fraud prevention. Companies, in tandem with governmental agencies, must develop shields against wrongdoing while adopting innovative strategies to do so. Through this balanced approach, we can protect society at large while preserving the integrity of our state and national programs.

What Benefits Do Data Providers and the Larger Information Industry Provide for Customers, Consumers, and Society?

Why must we balance the approach to regulating parts of the information industry? Because business customers, consumers, and government benefit from the combination of public and private records systems, those benefits can be destroyed or limited by imbalanced regulation. What is at risk? These information systems produce value-added services, including protection of children and seniors, lending, oversight of government, child support enforcement, safety recalls, improved newsgathering, and economic forecasting.

Public and private records systems working individually and alone, without the value additions of the information industry, do not provide an equivalent capacity to enhance public safety, facilitate commerce, and reduce government and business costs and inefficiencies.

As a result, data providers and other information industry parties are a critical part of the nation's information infrastructure and public records play a critical part in delivering benefits from that infrastructure. In a single year public records and data providers play a key role in the:

- Purchase of over 6 million residential homes,
- Sale of over 14 million new vehicles and over 36 million used vehicles,
- Notification of tens of millions automobile recall notices affecting an average of over 34 million Americans,
- Issuance of over 21 million passports and travel cards,
- Creation of quality-of-care reports protecting over 7 million children (under age 5) in day care and over 8 million adults receiving long-term care,
- Detection of fraud and fair underwriting for 291 million life, 167 million health, and 234 million car insurance policies,
- Checking the performance, quality, and stability of 6,800 banks, 13,000 credit unions, and 1,000 saving and loan institutions.

The following list shows some of the kinds of everyday activities made possible or far more efficient because of a combination of public and non-public records and the information industry companies who use them as part of their services.

Buying or Selling a Home:
- Evaluate the mortgage applicant and validate the funds,
- Verify the payment of property taxes,
- Conduct a lien search,
- Produce a clear title,
- Discover any pending litigation against the seller,
- Discover environmental hazards,
- Verify easements or encroachments, and
- Find neighborhood ratings (criminal activity, school performance, walkability).

Choosing a Care Provider:
- Verify provider's credentials, including background check,
- Obtain public health and safety reports,
- Determine available public assistance programs, and,
- Obtain a care provider report card.

Buying a Car:
- Conduct credit check for a loan,
- Identify recalled vehicles,
- Confirm proper titling,
- Find safety and fuel consumption ratings,
- Reveal crash and repair history, and
- Align insurance rates to driver behavior.

Getting a Job:
- Perform background check,
- Verify licenses and credentials, and
- Confirm work eligibility under the law.

Enabling Commerce:
- Open a bank account,
- Apply for credit,
- Reduce identity theft crime,
- Help consumers know where their purchases come from,
- Improve supply chain efficiency for businesses,
- Identify optimal business locations,
- Identify and prevent money laundering, and
- Allow investors to better value stocks and bonds.

Traveling Abroad:
- Obtain a passport or travel visa,
- Prove residency,
- Identify country immunization and public health restrictions, and
- Access terrorism and safety alerts.

Keeping People Safe:
- Arrest criminals,
- Reduce consumer fraud,
- Improve access to the justice system,
- Identify known offenders, and
- Protect vulnerable people.

Beyond the important every day uses, and value provided by the information industry, there are also important systemic benefits that inure to businesses, people, and our society. Some of those benefits are listed below for each of these categories:

Businesses:

- Growth and development,
- Efficiency,
- Compliance with laws and contractual requirements,
- A more level playing field for new market entrants and new products and ideas,
- Aligning resources and market trends, and
- Protecting business from fraud, harm, misuse, and other proscribed behavior.

People:

- Faster and more efficient transactions,
- Identity theft protection and identity security,
- Accurate association of data with the consumer to prevent false positive and false negative effects,
- Protection of vulnerable populations,
- Workplace and renter safety,
- Access to and use of free and freemium services,
- Fairer rate setting for individuals and groups, and
- Protection from fraud, harm, misuse, and other proscribed behavior.

Society:

- Functioning and robust markets,
- Public safety,
- Economic growth and jobs,
- Resource efficiency,
- Democratization of opportunity and information access,
- Leveling the playing field for small and medium sized businesses,
- Support for free speech and advocacy, and
- Governmental and societal transparency and accountability.

CONCLUSION

There is a lot of cognitive dissonance and inconsistency in what are broadly held American values, and the new regulations and laws being proposed. For example, Americans want to live in a free society with functioning markets. Americans want good deals, fair rates for what they get, and at least a few choices. Americans generally support businesses, especially small to medium ones, that struggle to find and keep customers, provide jobs, and remain profitable. America supports entrepreneurs who create new products and services that challenge entrenched players to better serve the consumer. The American Constitution supports free speech about matters of public or commercial interest. Americans widely patronize advertising-supported businesses from broadcast and published media to most of the Internet and App ecosystems. But how does one square these common beliefs, values, and actions with regulations and laws effectively saying we do not think anyone should know anything about anybody? CSPRA rejects the absolutism that says all information providing or brokering is either bad or good and that all data is either private or public. Since the inception of our organization, we have always maintained these as false choices between absolutes that do not serve us well. We believe in balance: between privacy and openness, cost and benefit, regulation and market forces, and the duty to the greater good and individual choices and responsibility. A more balanced, distinguishing, and logically applied approach to regulating the information industry is clearly in all our best interests, and singling out, demonizing, and over-regulating that entire industry is not.

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, governmental, commercial, and societal benefit. For more information, visit us on the web at www.cspra.org.