CSPRA

COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Date: March 1, 2023
To: Members of the Vermont Legislature
Re: **Comments on H. 121 (the Bill)**

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 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. Members of CSPRA are just a few of the many entities that comprise a vital link in the flow of information for these purposes and provide services that are widely used by constituents in your state. Collectively, CSPRA members alone employ over 75,000 persons across the U.S. The economic and societal activity that relies on entities such as CSPRA members is valued in the trillions of dollars and employs millions of people. Our economy and society depend on value-added information and services that includes public record data for many important aspects of our daily lives and work, and we work to protect those sensible uses of public records.

Exemptions for Public Records, Fraud Detection and Prevention, and Data Already Covered Under Existing Privacy Laws are Needed

California, Connecticut, Utah, Virginia and the model Uniform Personal Data Protection Act (UPDPA) proposed by the Uniform Law Commission (ULC) all have clean public records *and* publicly available information exemptions. The UPDPA and state laws also exempt data already covered under federal privacy laws such as the Fair Credit Reporting Act (FCRA), Health Information Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA). In addition, these state and model acts exempt the Drivers Privacy Protection Act (DPPA) which is critical to the safety and efficiency of the automotive industry and for many important societal and governmental functions.

Federal privacy laws are national frameworks that all states and businesses are currently following. These laws strike a beneficial balance between consumer privacy and information use. We respectfully request that any Vermont privacy bill align completely with existing national privacy regimes and practices to allow companies to be able to comply in a standard and cost-effective way across the states.

We Recommend the Model Uniform Personal Data Protection Act Proposed by the Uniform Law Commission as a Clean Public Records Exemption.

The UPDPA language mimics the state statutory exemptions for public records by exempting the following from the act, and we support using this definition:

"(15) "Publicly available information" means information:

(A) lawfully made available from a federal, state, or local government record;

(B) available to the general public in widely distributed media, including:

(i) a publicly accessible website;

(ii) a website or other forum with restricted access if the information is available to a broad audience;

(iii) a telephone book or online directory;

(iv) a television, Internet, or radio program; and

(v) news media;

(C) observable from a publicly accessible location; or

(D) that a person reasonably believes is made available lawfully to the general public if:

(i) the information is of a type generally available to the public; and

(ii) the person has no reason to believe that a data subject with authority to remove the information from public availability has directed the information to be removed."

Public Records Exemption Must Be Consistent with Vermont Public Records Law

Not all public records are widely made available "to the general public." We recommend that this added "to the general public" language be removed from the exemption and that it read instead as noted in the ULC model act in section A above. It states: "Publicly available information means information: (A) lawfully made available from a federal, state, or local government record" Therefore, public records as a class and other publicly available information would not be personal information under any section of the act if it is properly placed in a definition section that covers the entire act.

Vermont's existing public records law regulates access to certain public records to certain persons and for certain purposes. Adding the unnecessary and problematic qualifier "to the general public" would weaken existing privacy protections under the Vermont public records law which restricts access to certain public records to certain persons and for certain purposes (also note our discussion below on vendors to government and their use of public records on government's behalf).

There Will Be Unintended Consequences from Including Opt-out and Secondary Use Restrictions Without Exemptions for Public Records, Fraud Detection, and Federal Privacy Laws

The interaction of the opt-out and secondary use clauses with the lack of an adequate and clear public records exemption that applies to all sections of the Bill would be fatal to many essential uses of public records for law enforcement, child support recovery, lien enforcement, debt collection, underwriting, tax enforcement, witness location, judicial and legal processes, loans, auto safety recalls, and numerous other uses. A clean public records exception and authorized government vendor exemption (see below) solves these problems.

The Bill does not include a general allowance for companies to retain and use personal information to prevent and detect fraud. While the biometric section of the Bill contains an exemption for retention to "protect against or prevent actual or potential fraud, criminal activity, claims, security threats, or liability" the rest of the Bill does not. All companies offering fraud prevention services acquire their data indirectly. Criminals should not be given the freedom to "opt-out" of such services. Without a strong fraud exemption, consumers who "opt-out" would be more vulnerable to fraud and would face real-world issues with having their identity authenticated. This allowance and exception are found in many other state and model statutes and need to be added to the Bill.

There Is a Need for A Clear Government and Government Vendor Exemption

Generally, government itself should not be governed by public access to public records laws, and rules as the specific role of government, the enabling statutes, the rights involved, and privacy rules vary widely from program to program. Therefore, any proposed general laws or rules on the privacy of data should not apply to and hence shackle the government itself. It is also important to make it clear that vendors, parties, and subcontractors who carry out activities for and at the behest of government are also exempt from any general statute such as the one proposed.

There are several ways that private entities use public and private data to support government administration, investigation, and enforcement of several laws. For example, vendors help with finding missing and exploited children and trafficked persons, child support collection, tax lien collection, witness location, criminal investigations, and finding potential claimants or injured parties as part of a civil enforcement action by government. The Bill needs to clearly exempt government and its selected vendors from the law for the lawful purposes for which the government uses those vendors.

The Single Opt-Out Service Proposal is Unworkable and Should be Removed

The Bill allows the Secretary of State to set up a one-stop opt-out service. Currently, there are 431 data brokers registered with the Secretary of State. This includes a broad range of companies, such as credit reporting agencies, fraud prevention companies, and background screening services. A broad based opt-out requirement would have a significant impact on society's use of these services and may conflict with federal law. Additionally, consumers should have flexibility on the type of companies they seek to opt-out from, rather than a requirement that only applies to a small segment of commercial services.

The Bill lacks adequate identity proofing and data sharing requirements for data brokers to ensure that only the subject of a record exercises this new right and that adequate information is provided to the brokers to ensure that the right person is opted out of the data's use. Identity proofing and security have long been a weak spot in government administration and programs for reasons too involved to discuss here. But absent a rigorous identity proofing process, the State of Vermont will not be sure that the right is being exercised by and benefitting the correct person. Identity proofing is also not free nor cheap although as a shared service across government it can have a substantial return on investment in reduced fraud, expense, paperwork,

and time to process transactions securely. Many democracies around the world make great use of such services but the U.S. and certain states have lagged causing the need for point solutions to the problem or not having a solution and suffering the consequences of false and mistaken identity.

Vermont Law Already Strikes a Balance Between Access and Privacy in Public Records and No Special Study Is Needed

There is a clear need to adequately protect public records and strike a proper balance between privacy and trust. Vermont's public records law already protects selected records from disclosure. The existing laws limit access to certain parties in other cases and they ensure that disclosable public records are available to all. These protections ensure that people can see public records without interference from government or anyone who fears public scrutiny.

There is no reason to have a separate study to explore the effects of a public records exemption on privacy as proposed in the Bill. This issue is debated and studied regularly as a part of the public records act and its administration. Information in public records from local, state, and federal government sources are **owned by the People of Vermont**, not the person who is the subject of the record. Public records already do not include selected personally identifiable information and do include limits on its availability to selected parties for selected purposes. Best practice is to directly address any questionable behaviors in the use of public and private data that should be banned, regulated, or criminalized. Degrading the value and use of public records harms beneficial uses, undermines trust, is unlikely to stop the bad behavior, and will lead to a lot of pointless and wasteful litigation without any corresponding benefit.

Public Records Help Provide Essential and Valuable Services to State Residents, Businesses, and Government

Many persons and entities access and add value to the records they receive from public sources. They use these public records for a variety of personal, socially desirable, and essential civic and governmental purposes. We have attached an infographic that summarizes the benefits and uses of public information in the everyday lives of state residents and businesses. You will see that the information in the public record is foundational to many important life events and transactions of your state's residents.

Value-added services such as risk management, property title protection, news, protection of vulnerable populations, the administration of justice, law enforcement, monitoring government spending and corruption, enforcement of court orders and child support collection, and economic forecasting are just a few of the uses of public data. Consumers depend on the services that access, combine, and add value to public and private data almost every day and in ways that benefit all residents in every state whether they are aware of it or not.

Many institutions like the free press as well as businesses and service providers greatly rely on combinations of public and private records to function, and we all benefit in ways including, but not limited to, the following.

- Public and private data is used to monitor government for waste, fraud, and corruption.
- Data is used to find parents delinquent on child support.
- Combined public and private mapping data are used for locations, safety, consumer protection, and ratings of restaurants and retail stores.
- Real estate facts like square footage derived from public databases are key to buying and selling houses and provide consumers with accurate information.
- Vehicle registration data is used for safety recalls and helping forecast car sales data on which stock markets and manufacturing suppliers rely.
- Public information is used to find missing persons, witnesses, and suspects.

Protect Legal and Beneficial Uses of Public Records

Information is so intricately embedded in so many aspects of life and commerce that it is difficult to predict all the ways a change in information policy will affect various people, products, services, uses, and government functions. CSPRA has tracked such policies over the last three decades and we often see many unintended consequences of limits on access and use of public records. This often results in a long list of frequently revised exceptions. The root cause of such unintended consequences is the attempt to limit access to public records and public information rather than focusing on bad actors and acts that the society wants to regulate.

Thank you for your consideration of our input. We strongly request that proposed privacy legislation include a clean public records exemption such as the UPDPA model, a strong fraud exemption, and the suite of federal privacy exemptions for the FCRA, GLBA, HIPPA and the DPPA.

Richard J. Varn
Executive Director
Coalition for Sensible Public Records Access
San Antonio, TX
Email: rvarn@cspra.org
rjmvarn@msn.com
Cell : (515) 229-8984
(210) 236-1282
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, commercial, and societal benefit.