Discussion Points for Testimony Regarding VT HB 121 Amendment Draft
Coalition for Sensible Public Records Access (CSPRA)
Richard Varn, Executive Director

We support this exemption for state government and their vendors:

"…but does not include the State, a State agency, any political subdivision of the State, or a vendor acting solely on behalf of, and at the direction of, the State."

We do not support the current definition of publicly available information.

The language copied below is non-standard compared to other state privacy laws and the ULC model and is inadequate.

> (17) "Publicly available information" means information that:
> (A) is lawfully made available through federal, state, or municipal government records or widely-distributed media; and
> (B) a data collector or a data broker has a reasonable basis to believe a consumer has lawfully made available to the general public.

First, this should be an "or" conjunction not an "and". Second, the ULC model and other states have clean exemptions for lawfully acquired public records because public records acts have their own privacy rules and limits that are under constant review and have laundry lists of well-debated exceptions. They also provide the public with a ground source of truth about matters that are public or a fact that according to law or judgement applies to the subject of a record. Third, this definition does not work because not all public records that are accessible are available to the public. There are records that may be available only to certain persons and for certain purposes and are not something that any member of the public can see or were not provided to government for sharing with the "general public". Also, this definition does not include a complete definition of what publicly available information is beyond just what the broker's reasonable inference is. To better address this, see VA or UT as examples or the ULC model act for a broader and more complete definition of publicly available that protects beneficial uses, First Amendment rights, and what can be observed by persons in public.

Here are those three definitions and all use "or" instead of "and" in the publicly available section (highlighting added for emphasis).

Virginia:

> "'Publicly available information' means information that is lawfully made available through federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience."

ULC Uniform Data Protection Act:

(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.

Utah:

(29) "Publicly available information" means information that a person:

(a) lawfully obtains from a record of a governmental entity;

(b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or

(c) if the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

There are three different definitions of publicly available information throughout the bill and there are conflicting exemptions applied to each one. Therefore, it is not clear that a clean public records/publicly available information exemption applies across the statute, and it should.

Lawfully obtained publicly available information needs to be exempted across the act. On page 2, lines 15-17 seems to say that publicly available information that is not related to a profession or business is not exempted. The sentence should stop at the word "information." But it goes on to undermine both the First Amendment rights of those who wish to use publicly available information for other kinds of speech and undermines the purpose of public records in a free society.

"(B) Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.

The data broker beach section would place unnecessary burdens on data brokers for the same information held at any business. The definition of data broker has a very narrow exemption for publicly available information. An expansion from an annual registration to direct consumer notice is much broader than the state's breach law. The legislature should not conflate a data

breach subject to disclosure on an annual registration and a data breach that places a consumer at the risk of harm.

Finally, we think the statute would work best if there were one definition of publicly available information in the definitions section and it applies across the entirety of the act.

The definition of personal information is very broad, can be triggered by just one item of information plus a name.

The challenge we have consistently seen with privacy acts is the interaction between broad definitions and the prescribed acts and limits of the law. A broad definition of personal information can lead to unintended consequences stemming from the complexity of the interactions and the pervasive need for information for our society and commerce to function. Mapping each effect and interaction within the statute with such broad definitions takes time and can lead to confusion, higher compliance costs, and unintentional regulation. We suggest working with data users to simplify and streamline the definition and ensure that data items like name and address alone do not trigger unintended regulation and consequences. For example, the National Change of Address System works as well as it does because, to my knowledge, this information is not kept secret or part of an opt-out scheme.

We support the list of exemptions that include those entities and data that are already covered by federal law.

Data broker registration is overly broad and does not exempt publicly available information.

The bill requires a registered data broker to provide opt-out of data. The definition of data broker is very broad. It reaches beyond credit reporting agencies, and includes healthcare companies that resell marketing information, fraud service companies, commercial credit services, and software-as-a-service companies. There are no exemptions, except for a limited one related to consumer reporting agencies. The provision would subject opt-out to protected healthcare data, fraud, business information, marketing services data, and publicly available information. Publicly available information is a ground source for societal truths. One cannot have persons opt-out of the use publicly available information without destroying the purposes of that information and the right to use it for lawful purposes.

Consumers need more defined choices about the types of data brokers they wish to provide deletion/opt-out. For example, a consumer may wish to only opt-out of a people search services, but not from other types of marketing offers or fraud protection. A blanket approach is not good for competition or consumers. Data brokers would still be subject to consumer privacy rights and consumer can exercise those right through the contact information contained in the registration or through a third-party service.

Finally, we support the list of non-covered activities such as fraud prevention and identity theft, however, the act should not allow persons to opt-out of uses of data that facilitate these preventative and investigative needs.

Persons should not be able to opt-out of a use that is protected by the act. A simple example of the problem this creates is that a person engaged in criminal activity can opt-out of use of their information for the purposes of detecting that very criminal activity.