April 20, 2020

Mr. William McGeveran
Reporter, ULC Collection and Use of Personally Identifiable Data Committee
Mondale Hall
229 19th Ave., South
Minneapolis, MN 55455
Via Email: mcgeveran@umn.edu

Dear Mr. McGeveran,

On behalf of LexisNexis Risk Solutions, part of RELX, a leading provider of technology solutions that support the government, insurance, financial services, and healthcare industries, thank you for the opportunity to provide comments on the proposed "COLLECTION AND USE OF PERSONALLY IDENTIFIABLE DATA ACT". We appreciate the work of the committee in seeking a workable privacy law model that can be used in the various states.

While there are many positive aspects to the proposed legislation, there are also some issues that need to be addressed in order for this legislation to be workable, as discussed further below.

Publicly Available Information

We support the inclusion of an exception for publicly available information both from a consistency standpoint with other state privacy laws including the California Consumer Privacy Act (CCPA) and 1st Amendment considerations around the availability and use of public records. However, unlike the CCPA which creates an exception for information "lawfully made available from federal, state, or local government records" (*see* CCPA § 1798.14 (o)(2)), the proposed draft adds a qualification that the publicly available exception is only applicable "provided the information is being used in a manner consistent with any conditions on its use imposed by law." This "any conditions" language is potentially problematic because it could open the door to unlawful restrictions on the use of public records. To the extent there is any qualification here, it should be in the form taken by the CCPA that the records must be "lawfully made available" in the first instance.

Exceptions for Federal Law

While we appreciate the inclusion of exceptions for certain federal laws including the Fair Credit Reporting Act (FCRA) and the Health Insurance Portability and Accountability Act (HIPAA) it is important both for compliance with federal law and for operational consistency amongst states that relevant federal privacy laws are explicitly exempted from any state privacy law.

In the latest draft, there is no exception included for the Driver's Privacy Protection Act (DPPA). The DPPA is a long-standing federal privacy statute which provides that information obtained from a State Department of Motor Vehicles can only be used for certain delineated uses such as underwriting and law enforcement. The California Consumer Privacy Act (CCPA) specifically includes a DPPA exception (*see* CCPA § 1798.145 (f)) as does most other state privacy legislation that has been introduced, including the Washington Privacy Act.

The exception from the CCPA is as follows: "This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.)."

Further, while we were glad to see the inclusion of an exception for the Gramm-Leach-Bliley Act (GLBA), that exception should not be limited only to financial institutions but to any entity that has data subject to GLBA. Non-financial institutions have data that is subject to the requirements of GLBA in that they receive the data from a financial institution pursuant to certain delineated uses such as fraud prevention. Accordingly, the exception should be for the data that is subject to the GLBA as opposed to a certain entity. The CCPA takes the approach that the GLBA exception is for the data instead of the entity (*see* CCPA § 1798.145 (e)) and this was also the approach taken in the Washington Privacy Act.

The exception from the CCPA is as follows: "This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations. . ."

Notice, Deletion, and Opt-Out Right are Sufficient for Sensitive Personal Data

The proposed language would provide that a data subject would need to "opt-in" to the collection of sensitive personal information. However, because the law already provides for notice, deletion, and opt-out rights, the inclusion of a specific opt-in, even for sensitive personal data, is not necessary and would create challenges both for consumers and for businesses regarding the legitimate use of sensitive personal data.

Thank you again for the opportunity to comment and please let us know if we can provide any information that would be helpful for the committee during its deliberations.

Sincerely,

Richard B. Gardner
Corporate Counsel
LexisNexis Risk Solutions