Uniform Law Commission

June, 30 2020

The undersigned organizations appreciate the opportunity to offer feedback on the Uniform Law Commission's ("ULC") most recent draft data privacy law, the "Collection and Use of Personally Identifiable Data Act ("Draft Act"). We strongly believe in the need for a national data privacy and security framework and support the ULC's efforts to promote uniformity in this area of the law. In submitting this letter, we hope to build consensus on a strong, workable data privacy legislation template to help states that have struggled to reach agreement on this issue.

We applaud the work of the ULC and recognize that significant progress has been made in the development of a model bill. While there is broad support for many aspects of the current draft, several key issues are still of concern and will make passage of the bill in state legislatures very difficult. The aspects in question are the Gramm-Leach-Bliley Act Exemption, Fair Credit Reporting Act Exemption, Enforcement and the Private Right of Action, and Publicly Available Data.

Data privacy and security legislation are critical in an increasingly digital world and, while we recognize the necessity of such legislation, a balance must be struck between consumer protections and workability of the provisions in such bills by business. It is in the interest of all consumers that laws in this arena are written with a clear understanding of the issues, are forward-thinking with respect to advancing technologies, and are not designed to be punitive for businesses that act in good faith.

Gramm-Leach-Bliley Act Exemption

A Gramm-Leach-Bliley Act (GLBA) exemption has been included in almost every piece of U.S. data privacy legislation since the passage of the California Consumer Privacy Act ("CCPA")'s follow-up bill in 2019. GLBA, passed in 1999, requires financial institutions to describe how they share and protect the private information of their customers and is divided into three parts: the Financial Privacy Rule, which regulates collection/disclosure of private financial information; the Safeguards Rule, which stipulates financial institutions must implement security programs to protect such information; and the Pretexting provisions, which prohibit accessing private information under false pretenses. GLBA also requires financial institutions to give customers written privacy notices regarding a financial institution's information-sharing practices. Central to the GLBA are the same principles found in this and other model bills across the country: safeguarding privacy, disclosures regarding collected private information, and protections on access and use of that information. Since financial institutions have already been doing this for two decades, duplicating the requirements for financial institutions in a privacy bill draft adds unnecessary complications for businesses. An unambiguous exemption for those entities already complying with GLBA ensures businesses can process data for customers and know that the potential for confusion has been completely nullified.

Moreover, it is unlikely that an exemption for financial institutions covered by the GLBA would do much to limit the scope of the proposal. As currently drafted, the Draft Act targets business who earn more than 50 percent of their gross revenues directly from "activities as a data controller or data processor[.]" Few, if any, financial institutions will satisfy these criteria, as their revenues are not primarily derived from such activities. Thus, rather than limit the Draft Act's scope, an exemption for financial institutions subject to the GLBA would simply clarify the scope currently reflected.

Finally, with regard to data security standards, financial institutions are already subject to the GLBA's Safeguards Rule which is implemented by the appropriate federal regulator. The current language in the Draft Act regarding data security appears to parallel implementing regulations for the Safeguards Rule. This GLBA requirement is already applicable at the institution level, and there is no benefit to establishing a separate parallel requirement. This is especially true as, by necessity, the determination as to what constitutes reasonable security practices is a risk-based determination that would differ from one financial institution to the next. It is more appropriate to have that determination made by federal regulators with ongoing oversight over the financial institution than by state Attorneys General or state courts, which would likely lead to divergent interpretations and conflicting standards as to what is "reasonable."

Fair Credit Reporting Act Exemption

In addition to the GLBA exemption, the Draft Act should include an exemption for data covered by the Fair Credit Reporting Act (FCRA). Generally speaking, the protections of the FCRA apply to any written, oral or other communication of any information by a consumer reporting agency bearing on a wide range of information about the consumer including his or her credit worthiness, character and reputation, and personal characteristics. The FCRA draws specific limitations on when this information can be obtained, how it can be used, and it requires detailed disclosures to consumers regarding the creation, reporting, use and correction of this data. It also includes a right to opt out if information will be shared with affiliates for marketing purposes. Information subject to the FCRA would also be subject to the GLBA, and the laws have complimentary provisions intended to function in tandem.

These rules are technical and specific, and part of a larger regulatory ecosystem that includes contractual obligations between financial institutions and consumer reporting agencies and private standards and frameworks established by the Consumer Data Industry Association (CDIA) and other entities which establish the systems used by financial institutions in the reporting of consumer data and resolution of disputes.

Enforcement/Private Right of Action

The current draft provides for two separate means of enforcement: public enforcement through the State Attorneys General offices, and private enforcement through private rights of action. In this way, the draft Act diverges from most state privacy bills which provide for exclusive AG enforcement for violations of statute and limit any private enforcement to data breaches.

One of many issues with drafting omnibus-style legislation in this arena is how duplicative and unnecessarily divergent the efforts can often be. By way of example, all 50 states, as well as the District, have addressed the issue of data breaches in separate legislation that include notification requirements as well as penalties. The penalties, typically an unfair trade practice violation, are most often enforced by the Attorney General. To add additional requirements for private enforcement solves a problem that does not exist, as states have already determined they want enforcement powers to vest in the Office of the Attorney General.

That states have declined to incorporate private enforcement mechanisms is completely understandable given that, from a public policy standpoint, permitting private enforcement is a bad idea. For financial institutions and other risk averse businesses, a private right of action – or 50 – creates unknown risk. This has the effect of deterring innovation, thereby depriving businesses and consumers of the benefits of that innovation. To avoid these unintended consequences, enforcement policy must be implemented in a way that accounts for society's interests in privacy and innovation. As most states have found, such balancing can best be accomplished through a public enforcement mechanism.

Public enforcement is particularly appropriate as establishing a specific, material harm to a consumer and tying causation of that harm to a specific privacy violation through admissible evidence is an incredibly difficult task. Further, calculating proper restitution has been next to impossible to do. Bypassing this complexity using statutory damages creates significant policy problems. Those who profit most under these frameworks are typically plaintiff's attorneys. An example would be the current legal regime, including the PRA provision, around the Telephone Consumer Protection Act (TCPA) which has resulted in a surge of litigation that far outweighs any underlying consumer harm. From 2010 to 2016, the number of TCPA lawsuits has increased by 1,272 percent, with plaintiffs' attorneys receiving millions of dollars in compensation against legitimate businesses for technical violations. Plaintiff attorneys benefit from multi-million-dollar attorneys' fees, while individual consumers in these class action lawsuits often receive only a nominal award and businesses are forced to adopt cumbersome validation procedures or limit communications that would be beneficial for consumers.

Publicly Available Data

Currently there is discussion regarding whether the exemption for publicly available data should extend beyond data culled from government records to widely circulated media (the draft now exempts both).

We agree that if information is already in the public domain, it does not make any practical or policy sense to say that information, once obtained by a third party, should then revert to private information.

We appreciate the time and thoughtfulness that has gone into the Draft Act thus far. The discussions around principles have been robust and we look forward to helping craft a finished product that all parties can be proud of.

Sincerely,

American Financial Services Association

American Land Title Association

Consumer Bankers Association

Marketplace Lending Association

Mortgage Bankers Association

National Association of Federally-Insured Credit Unions