Summary & Overview of Personal Data Protection and Information Security Act
("Alternative Uniform Act")

1. Integrate Protection of Information Privacy into Existing Consumer Protection Law

The Alternative Uniform Act integrates the protection of information privacy into existing consumer protection law. This eliminates the need to create new institutional frameworks to monitor business compliance. Existing consumer protection law is supported by a mature, well-established institutional framework that is familiar to both businesses and consumers.

2. Achieve Regulatory Coherence between New and Existing Information Privacy Laws

The Alternative Uniform Act provides a framework within which regulatory coherence between its provisions and the provisions of other U.S. and foreign information privacy laws can be achieved and maintained.

The Alternative Uniform Act promotes regulatory coherence in the following ways:

A. U.S. consumer protection law is already integrated into existing sectoral information privacy protection laws at the federal and state level.

B. The Alternative Uniform Act explicitly provides that it does not displace existing U.S. federal and state information privacy laws that target different economic sectors in order to avoid over- or under-inclusive regulation. The Act fills in the gaps in these existing "sectoral" information privacy laws. It does not purport to mandate uniformity across sectors through "command and control" techniques.

C. Under the Alternative Uniform Act, businesses that are in compliance with information privacy laws of another country or region that address similar issues in a similar manner are deemed to be in compliance with the Act.

D. The Act authorizes state and federal consumer protection regulators to grant qualified recognition to voluntary, consensus standards that harmonize compliance obligations for businesses subject to multiple regulatory frameworks.

3. Safeguard Constitutional Liberties

The First Amendment safeguards the free flow of information in American society by restricting the power of government to determine what information individuals may exchange.

A. Foreign information privacy laws such as the GDPR that regulate information directly were enacted in jurisdictions that lack this fundamental safeguard of individual liberty. Transposing such foreign information privacy legislation into United States legislation risks violating the free speech rights of U.S. citizens.

B. Publicly available information is among the categories of information that receive the strongest form of First Amendment protection. See, e.g., Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975). The Alternative Uniform Act carefully defines publicly available information then subjects it to the Act's system level protections and exempts it from the individualized protections (discussed in Section 5 below) in order to pass constitutional muster.

C. Because the Alternative Uniform Act regulates information incident to a consumer transaction in order to support trust relationships between businesses and consumers, it does not infringe the kind of freedom of expression protected by the First Amendment. See, e.g., Sorrell v. IMS Health Inc., 564 U.S. 552 (2011) ("the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech").

4. Minimize the Risk of Statutory Obsolescence

The rapid pace of change of technologies and processes for collecting, using and storing personal information increases the risk of statutory obsolescence. The Alternative Uniform Act makes use of three "future proofing" strategies to mitigate this risk:

A. Under information privacy laws such as the GDPR, it is not lawful for businesses to collect personal information in the absence of an explicit grant of authority to do so. The Alternative Uniform Act does not attempt to control how the original collection, use or storage of personal information must take place provided that the business and consumer are engaged in a lawful relationship. In the event of a dispute, courts may determine what is "lawful" collection of personal information on a case-by-case basis.

B. After the initial collection, the Alternative Uniform Act uses the notion of "compatible" uses to create a framework within which permissible from impermissible uses of personal information can be distinguished. The definition of "compatibility" in the Act is taken from Section 552a(a)(7) of the Privacy Act of 1974, which has been clarified by the courts over nearly half a century.

C. The Alternative Uniform Act, consumer protection regulators may grant safe harbor status to sector specific standards distinguishing compatible from incompatible uses developed through transparent, accountable, and inclusive standard setting processes (discussed in Section 7 below). Once safe harbor status has been granted, then business compliance with such standards will be deemed to be compliance with the law.

5. Distinguish between System Level Protections and Individualized Protections

The Alternative Uniform Act defines two different categories of personal information and applies a different level of protection to each:

A. "Personally identifiable information" is defined as any information that is linked or could be linked to an individual in an information system. The law establishes mandatory minimum levels of privacy and information security risk management practices that apply at the level of the information system.

B. "Personal data" is defined as personal information that is structured so that it can be used to make decisions that have an impact on individuals. Businesses must follow recognized fair information privacy practices with regard to this type of personal information.

6. Align Business and Consumer Interests within a Two-Tiered, Risk-Based Framework

The two-tiered, risk-based framework in the Alternative Uniform Act removes barriers to business compliance by aligning the interests of businesses and consumers, thus delivering improved information privacy protections to consumers in reality, not just in theory.

A. Businesses already have strong economic incentives to safeguard the integrity of their information systems, as well as to preserve the trust of their customers in the quality of the decisions they make that have a direct impact on their customers.

B. The first tier of protection provided by the Act maps onto current best practices for business information system risk management.

C. The second tier of protection provided by the Act maps onto the current best practices for computer-supported decision making by businesses making choices that have a direct impact on their individual customers.

7. Reward Responsible Public-Private Collaboration with Safe Harbors

Since the 1970s, the U.S. Office of Management and Budget Circular A-119 has authorized a unique form of public-private collaboration designed to improve compliance with federal regulations. OMB Circular A-119 provides a framework through which private sector standards can be linked to public laws which in turn clarifies for regulated entities how those laws will be applied to them by regulators. The OMB defines "voluntary, consensus standards" as those emerging from processes that embody strong due process guarantees of transparency, accountability and inclusion. Only those private sector standard setting organizations that meet the OMB's requirements for producing "voluntary, consensus standards" are eligible for inclusion in this process.

A. The Alternative Uniform Act transfers the OMB Circular A-119 framework from the broad, general context of federal administrative law to state consumer protection law and the regulation of business use of consumers' personal information.

B. The process of developing voluntary, consensus standards is very similar to the Uniform Law Commission process for developing uniform laws. Both rely heavily on the willingness of

stakeholders with relevant interests and subject matter expertise to volunteer their time and talent to contribute to large, complex, slow processes with no guarantee of success.

C. In order to provide businesses with incentives to contribute the time and talent required for success, the Act permits consumer protection regulators to confer compliance safe harbor status on appropriate private sector voluntary, consensus standards.

D. The Act's safe-harbors for voluntary consensus standards simultaneously increases the effectiveness of regulators' enforcement efforts and business compliance efforts.

8. Permit Effective Stakeholder Engagement in the Design of Compliance Frameworks

The law increases democratic accountability in the administration of information privacy law by recognizing the right of individuals, civil society organizations, businesses and regulators to help define what constitutes compliance with the law.

A. The definition of "voluntary, consensus standards" set out in OMB Circular A-119 is very similar to other well-known due process criteria applied to standard setting processes. These include the American National Standards Institute "Essential Requirements" and the Code of Good Standardization Practice in Annex 3 of the World Trade Organization Technical Barriers to Trade Agreement.

B. By using transparent, accountable and inclusive standard setting processes to mediate among different stakeholder groups, the Alternative Uniform Act levels the playing field between regulators and businesses at the same time it promotes more informed, constructive dialogue among all stakeholder groups.