Hughes Hubbard & Reed

Bipartisan Privacy Bill of Rights Act Introduced in Senate

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Last Tuesday, U.S. Senators John Kerry (D-Mass.) and John McCain (R-Ariz.) introduced the Commercial Privacy Bill of Rights Act of 2011 which is intended to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission." According to the bill, current laws at the state and federal level provide inadequate privacy protection for individuals and the Federal Government has "eschewed general commercial privacy laws in favor of industry self-regulation" which has largely been unenforceable and has provided insufficient privacy protections. If enacted, the law would direct the FTC, within specified timeframes, to make rules requiring "covered entities" - those that collect, use, transfer or store "covered information" of more than 5,000 individuals over any consecutive 12-month period - to comply with a host of new requirements protecting the security of the information as well as the privacy of the individuals to whom information pertains. Specific requirements are imposed directly on entities covered under the act. "Covered information" that is protected under the proposed bill includes personally identifiable information ("PII"), unique identifier information and basically and any information that may be used to identify an individual. Some provisions require different standard with regard "sensitive personally identifiable information", which is defined as information relating to medical records or religious affiliations and PII which, if lost, compromised, or disclosed without authorization could "result in harm to an individual." A high level summary of a draft form of the bill was discussed in our recent webinar, "App-Endectomy: Removing the Mystery from the App Ecosystem." Here we'll present the key highlights of the proposed bill.

Right to Security and Accountability

The bill requires the FTC to initiate a rulemaking proceeding to require covered entities to carry out security measures to protect the covered information it collects and maintains. These security measures should be proportional to the size, type and nature of the covered information and should be consistent with recognized industry standards and the current guidance provided by the FTC in its privacy framework. Each covered entity shall have "managerial accountability", a process to respond to on-frivolous inquiries from individuals. The bill requires that covered entities implement a "privacy by design" approach that builds privacy protections into their everyday business practices.

Right to Notice and Individual Participation

The bill also requires that the FTC to initiate a rulemaking proceeding to require covered entities to: (i) provide clear, concise and timely notice regarding its information practices and any material changes to such practices; (ii) offer individuals a clear and conspicuous opt-out mechanism for (a) unauthorized uses of their information or (b) use by third parties of their covered information for behavioral advertising or marketing. The higher opt-in consent is required whenever an entity is dealing with sensitive PII, materially changes its stated practices or when the uses or transfer of information to a third party creates a risk of economic or physical harm to an individual. Entities should also provide individuals with access to their PII and mechanisms to correct inaccurate PII. In the event an entity enters bankruptcy or an individual terminates its relationship with an entity, the individual must also have the option to request that is covered information be rendered not personally identifiable if possible.

Rights Relating to Data Minimization, Constraints on Distribution, and Data Integrity

The bill's requirements on data constraints and integrity are fairly standard. Covered entities should only collect what's needed. They must have procedures to ensure the accuracy of the information and they should only retain the info as long as necessary to provide the service. Whenever a covered entity transfers information a third party, the covered entity and third party must enter into a contract that says the third party won't combine information to identify individuals without such individual's opt-in consent.

Enforcement and Penalties

The bill grants the FTC enforcement authority over "knowing or repetitive" violations which shall be treated as unfair or deceptive acts or practices. State attorneys general are given civil action authority to enforce the Act. Notably, the Act does not provide for a private right of action, which is likely to raise opposition from privacy advocates. Monetary penalties for violating the Act are stiff – a covered entity that knowingly or repeatedly violates the Act is liable for a civil penalty of $16,500 multiplied by the number of days of noncompliance. If a covered entity violates the Act and fails to obtain proper consent when required, the penalty is $16,500 multiplied by the number of days of noncompliance or the number of individuals whose consent was not obtained, whichever is greater. Liability is capped at $3 million. The act would preempt state laws, except those laws dealing with health or financial information or data breach notification.

Safe Harbor

There would be safe harbor programs which the FTC would create and supervise that would exempt participating entities from certain requirements of the Act. However, these programs would have to have, in the FTC's opinion, similar or more protective requirements than the Act itself. While Senators McCain and Kerry tout the proposed legislation as a step towards greater and more consistent privacy protection, privacy advocates have argued the Commercial Privacy Bill of Rights Act of 2011 does not go far enough. Unlike the FTC's 2010 privacy framework which recommends a "Do Not Track" mechanism, the bipartisan bill doesn't provide for a "universal opt-out" in which consumers can end all tracking but using a national registry. Consumer advocates also claim that the bill would prohibit states from implementing stricter measures. We will continue to track the ongoing developments in privacy legislation and its potential impact on our clients.

Related Areas of Focus