Crafting a National Standard for Consumer Data Security and Breach Notification

The Insights Association, a nonprofit trade association representing the marketing research and analytics industry, supports the enactment of a federal data security law requiring data security and breach notification.

Placing reasonable limits on what constitutes a breach of concern to consumers (and thus being worthy of notification in an era of over-saturation of breach notices) and on the power of the Federal Trade Commission (FTC) to write regulations (and expand definitions) are of key importance to our industry. The data our members collect and analyze, in order to understand the opinions, attitudes and behaviors of groups of consumers, would not be susceptible to criminal abuse if breached, which is why such limitations matter to us.

Our policy concerns include:

- **State preemption**: A national standard that pre-empts all the conflicting patchwork of 48 state laws.
- **Equal application to both for-profit and non -profit companies/organizations**.
- **No private rights of action**. Avoid another litigation cottage industry.
- **Exemption for encryption/deidentification**: Exempt data that is rendered unreadable or unusable.
- **Exclude public data**: Exclude data that is publicly-available or part of a public record.
- **Significant risk of harm**: If an entity suffering a breach runs an appropriate risk assessment and finds no significant risk of harm, notification should not be necessary.
- **Limit the data requiring notification**: The definition of personal data covered by legislation should be circumscribed to only that which could most open to criminal abuse, like personally identifiable information (first name and last name with contact or location information) combined with social security numbers, or financial account or credit information, that could allow for identity theft, fraud or other kinds of tangible consumer harm. Anything further becomes a slippery slope down which almost any piece of data could ultimately be included.
- **Data security and privacy should be separate**. Data that could raise privacy-specific concerns should not be covered for purposes of breach notification.
- **Don't empower the FTC to radically expand covered data**: Many data security bills seek to give the Federal Trade Commission (FTC) APA rulemaking authority (section 553 of title 5, U.S. Code) -- authority specifically denied to the regulatory agency in current statute because of abuses in the 1970's -- to alter the definition of covered data, instead of the agency's regular Magnuson-Moss rulemaking procedures. FTC staff and commissioners have stated for years that they consider most types of data to be ultimately personally identifiable and that they should be included in such a definition.[1] The definition should rightfully be set by Congress, not an unelected regulatory body, and set in a limited fashion.
- **Don't set an arbitrarily brief timetable for data breach notification**: Several recent bills would require breach notification within 30 days of discovery -- too short a time frame for some high-tech data security breach investigations. State laws usually require a "reasonable" amount of time. (For comparison, even HIPAA has a 60 day limit.)

[1] For example, at an Energy & Commerce CMT Subcommittee hearing on July 15, 2011: "I think that the touchstone here is information that can be uniquely tied to an individual... broader than the definition that is currently used in the draft bill."

Insights Association
1156 15th St, NW, Suite 302, Washington, DC 20005 • Ph: (202) 800-2545
Website: http://www.insightsassociation.org • Email: howard.fienberg@insightsassociation.org