Technology Industry Principles for Federal Legislation on Data Security and Breach Notification

Criminal and state sponsored hackers pose a significant threat to all entities large and small, public and private. There are many ramifications of these dynamic and evolving cyber threats, including but not limited to the risk posed to consumers who may be at significant risk of identity theft or other financial harm. Year after year, identity theft is the number one category of fraud reported to the Federal Trade Commission (FTC).

The current scope of legal obligations in the United States following a data breach is complex. Each of the 52 state and territory breach notification laws varies by some degree, and some are in direct conflict with one another. Without a uniform national standard for data security and breach notification, the current patchwork is likely to grow even more complex and confusing for consumers, enhancing the compliance challenges for businesses, while failing to advance consumer notification or data protection.

Our associations, collectively representing a broad range of the technology industry, support creation of a uniform national standard for data security and breach notification that is effective, simple and protects consumers. To achieve this, legislation should reflect the following principles.

Responsible, Flexible Notice Requirements—Timely consumer notification is critical in the event of a breach that poses significant risk of financial harm or identity theft. However, this is only one element of combating the pernicious effects of data breaches. The first response to any suspected breach is to assess and restore the integrity of the impacted information system. Any public notification prior to this will simply invite hackers and phishers to engage in additional nefarious activity targeting both consumers and the entity impacted by the breach. Therefore, federal legislation must provide realistic and flexible time requirements, allowing for organizations to address the vulnerability and conduct thorough investigations before notifying consumers or government agencies. Notice requirements must also be flexible, allowing breached entities to gather actionable information for consumers and utilize a notification measure that is most timely and practical for consumers, including providing for a public notice in certain cases where individual notices cannot be achieved in a timely manner.

Effective Harm-based Trigger—It is critical to identify the delicate balance between over—and under—notification, recognizing that not all data breaches create a risk of harm to consumers. Notification is critical to put consumers in a position to take necessary action to protect themselves from financial harm or identity theft when there is an elevated risk of such harm. Providing notice in all instances of breach will create "notice fatigue," rendering consumer notification much less effective. Therefore, consumer notification should be required only after a breached organization determines the unauthorized acquisition of sensitive personal data poses a significant risk of identity theft or financial harm. Identifying the risk of harm must also take into consideration whether the data is unusable due to encryption, obfuscation, anonymization or the absence of critical pieces.

Practical, Consumer-centric Third-Party Requirement—Many businesses contract with third parties to maintain or process data containing their customers' personal information. In the event of a breach of confidential personal information handled by a third party, the third party should be required to notify the consumer-facing company of the breach if the third party knows the data contained confidential personal information. A requirement for third parties to provide notice directly to consumers is less effective and creates confusion for consumers who would not recognize the entity as one with which they have a relationship. Additionally, such a requirement is impractical because third parties often do not have access to their customers' data to determine whether confidential personal information was breached or to perform the requisite risk analysis, and they often lack the relationship and necessary contact information to directly notify impacted consumers. Federal legislation should enable consumer notification to be provided by the consumer-facing entities, or to continue to be determined by contract. This approach is consistent with the current law under the range of state and territory regimes.

Establishment of Reasonable Security Safeguards—The FTC holds companies accountable for employing data security measures it deems reasonable in light of the sensitivity and volume of consumer information they hold, the size and complexity of their data operations, and the cost of available tools to improve security and reduce vulnerabilities. However, there is currently a lack of clarity regarding what constitutes reasonable security, particularly in light of rapidly evolving threats and technological security standards, and the growing number of disparate state and federal requirements. Federal legislation should provide flexible, risk-based security requirements for companies to protect the confidentiality and security of confidential personal information from unauthorized acquisition. Creating such a framework would afford much-needed predictability for companies at a time when the contours of reasonableness are increasingly confusing. However, legislation should avoid the creation of a stagnant, prescriptive set of requirements that will prove incapable of adapting to ever-changing cyber threats.

No Criminal Penalties or Private Right of Action—Companies have substantial market incentives to secure their systems and protect valuable data, as breaches of confidential personal information have repeatedly resulted in substantial economic loss to the companies and the displacement of senior management. Most data breaches are also the result of criminal acts. Therefore, federal legislation should not create criminal sanctions or penalties for these entities that are victims of a crime. An effective breach notification requirement and an efficient enforcement framework provides the best protection for consumers and will avoid unnecessary and frivolous litigation.

Federal Preemption—Given the often-conflicting patchwork of state laws, federal legislation must establish effective federal preemption that will eliminate confusion and conflicts around breach notification and data security requirements. Preemption will result in businesses being able to notify consumers more quickly, while also maximizing the effectiveness of a security framework. Without preemption, any federal law would simply add a 53rd standard to the existing patchwork.