HOGAN & HARTSON LLP

Privacy & Data Security Legislative Update

Presented to The Liberty Alliance

Mary Ellen Callahan, Esq.

PRIVILEGED AND CONFIDENTIAL/ ATTORNEY-CLIENT COMMUNICATION

Agenda

- Overview of the Current Legislative Environment
- Existing Privacy and Data Security Laws
- Federal Data Breach Legislation
- Federal Privacy Legislation
- Federal Spyware Legislation
- Overview of State Activity
- Overview of International Activity

Overview of the Current Legislative Environment

- Data breaches drove the agenda for much of 2005
- Omnibus privacy legislation is being touted by senior members of Congress.
- Activity on spyware legislation has slowed
- 2006 elections shorten the legislative year and other policy issues are taking center stage
  - Immigration reform
  - Lobbying reform
- States have focused on data breach notification laws
- International laws add complications

Current U.S. Regulations of Data Security

- Federal Trade Commission Act
- Gramm-Leach-Bliley -- for financial institutions and their service providers only
- State Laws

Federal Trade Commission Act

- Section 5 of the FTC Act prohibits "deceptive" and "unfair" practices.
  - ***Deceptive practices*** require a material representation, omission, or practice that is likely to mislead reasonable consumers
    - No intent to mislead is required for deception enforcement
  - ***Unfair practices*** do not require a misrepresentation and can include failures to provide basic safeguards
    - Harm to consumers must not be reasonably avoidable
    - Harm must be significant
    - Benefits to consumers must not outweigh the harm
    - The FTC has recently revived its use of this controversial doctrine

Gramm-Leach-Bliley

- Applies only to "financial institutions," but this term is defined broadly and includes, among other things, retailers that issue private label credit cards.
- Among other things, GLB requires developing a data security program that:
  - Designates at least one person to coordinate the program;
  - Includes employee training;
  - Identifies data security risks;
  - Implements safeguards to minimize those risks; and
  - Tests and monitors those safeguards.
- Companies must contractually require service providers to implement a similar data security program.
- The FTC has suggested it will try to expand the scope of GLB, particularly to apply to data processors.

State Laws -- California

- California enacted a security breach notification law that triggered recent breach disclosures and media coverage.
- Companies must notify consumers if there is/believed to be a breach of "unencrypted personal information" from computerized data.
- "Personal information" defined as first and last name plus
  - Social Security number;
  - Driver's license number or California Identification number; or
  - Account number, credit or debit card number, in combo with password or access code.
- If the personal information is encrypted, but the database has been breached, no consumer notification is required.
- Amendment proposed to extend to paper records (S. 852). Failed to pass through committee and is scheduled for reconsideration.

State Laws (cont'd)

- Multiple states followed suit in 2005 and early 2006, passing laws on security breach notifications.
  - AR CA, CT, DE, FL, GA (data brokers only), IL, IN, LA, ME, MN, MT, NV, NJ, NY, NC, ND (defines PII to include date of birth, maiden name, and employer ID #), OH, PA, RI, TN, TX, WA and WI
- Some states have also passed laws requiring reasonable security procedures.
  - AR, CA, NV, and TX
- Differing standards and requirements (even for those based on CA) have led to industry request for federal action.

Federal Data Security Legislative Update

- Five bills have passed out of House or Senate Committees
  - S.1326, the Notification of Risk to Personal Data Act (Senate Judiciary).
  - S. 1408, the Identity Theft Protection Act (Senate Commerce).
  - S.1789, the Personal Data and Privacy Security Act (Senate Judiciary).
  - H.R. 3997, the Financial Data Protection Act (House Financial Services).
  - H.R. 4127, the Data Accountability and Trust Act (House Commerce).

Federal Data Security Legislative Update (cont'd)

- All of the proposed bills have some similar provisions
  - Apply across industries, rather than the sector approach adopted by GLB and HIPAA.
  - Require companies to adopts a data security program roughly based on GLB with details left up to regulators and the private sector.
  - Require notification of breaches.
    - Use a risk-based trigger for notification
    - Standard for notification varies
  - Preemption of state laws.

Federal Data Security Legislative Update (cont'd)

- There are still some areas of disagreement in the proposals, which will lead to additional negotiations and amendments.
  - Standard for triggering notification:
    - Should a risk of harm other than identity theft trigger notification?
    - Reasonable risk vs. significant risk of identity theft or some other harm to consumers.
    - Does the loss or theft of only a small amount of data need to be publicly disclosed?
    - Is notification necessary when the data is properly encrypted?
    - Do Social Security numbers deserve special protection?

Federal Data Security Legislative Update (cont'd)

- State Law preemption:
  - Full preemption is likely, though Democrats continue to argue for a federal floor.
  - Whether attorneys general can enforce the federal standard is still open.
- Additional Open Issues:
  - Should companies already covered by other data security requirements, e.g., GLB, be exempt?
  - Should consumers be allowed to put a "freeze" on their credit?
  - Should paper records be covered by the proposed federal law?
  - Should data brokers be subject to stricter regulations than companies for whom data collection is ancillary to their business?

Federal Privacy Legislative Update

- H.R. 1263 – Consumer Privacy Protection Act (House Commerce)
  - Requires additional notice and choice to consumers regarding the use of their personally identifiable information (PII).
  - Requires companies to prepare and implement information security policies designed to prevent the unauthorized disclosure of PII.
  - Still awaiting subcommittee vote
- Chairman Barton has said he plans to move a comprehensive privacy bill in 2006
  - Barton has lost some momentum in 2006, and has been otherwise occupied with telecom reform.
  - Likelihood of privacy legislation this Congress slim, but could be bundled with telecom.

Federal Spyware Legislative Update

- Two bills have passed the House.
  - H.R. 29, the Spy Act requires notice consent before certain software can be downloaded .
  - H.R. 4661, the I-Spy Act would increase penalties for bad actors.
- Two Senate bills are under consideration.
  - S.687, the SPY BLOCK Act has cleared the Commerce Committee but won't reach the floor without some agreement from Sen. Allen.
  - S.1608, the Safe Web Act, which enhances the FTC's enforcement capabilities outside of the U.S., has been passed by the Senate.

State Overview

- States will continue to pass and enforce breach notification statutes pending possible preemption
- California breach notification has become the *de facto* national standard
- Key states have identified privacy and data security as areas of enforcement focus

International Overview

- Many foreign jurisdictions have their own statutes, including:
  - European Union Data Protection Directive 95/46/EC
  - Canada: Personal Information Protection and Electronics Documents Act
  - Japan: Personal Information Protection Law

Looking Ahead

- Privacy and data security will continue to be significant policy issues in 2006 and beyond
- Election shortens the legislative calendar, but a new data security law is still possible
- Spyware and general privacy legislation unlikely to be completed this year
- States will remain active unless preempted
- International law complicate compliance

Mary Ellen Callahan, Esq.
202-637-6406
mecallahan@hhlaw.com

PRIVILEGED AND CONFIDENTIAL/ ATTORNEY-CLIENT COMMUNICATION