The Good, the Bad, and the Really, Really Ugly

*in Federal Legislative Proposals and Government Initiatives*

Elizabeth Johnson
Partner
Poyner Spruill LLP
(919) 783-2971
ejohnson@poyners.com
Roadmap

- Themes in Federal Security Legislation
- Federal Agency Initiatives
- State Activity
Competing Bills

John Kerry (D-MA)
Commercial Privacy Bill of Rights Act of 2011

Patrick Leahy (D-VT)
Personal Data Privacy and Security Act

Al Franken (D-MN)
Personal Data Privacy and Security Act (co-sponsor)
Chairman, Judiciary Subcommittee on Privacy, Technology and the Law

Mary Bono Mack (R-CA)
Secure and Fortify Electronic Data Act (SAFE Data Act)

Cliff Stearns (R-FL)
Data Accountability and Trust Act (DATA) of 2011

Bobby Rush (D-IL)
Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act (BEST PRACTICES Act)

Richard Blumenthal (D-CT)
Personal Data Protection and Breach Accountability Act of 2011

“When a data breach occurs, it is essential that customers be immediately notified about whether and to what extent their personal and financial information has been compromised.”

John McCain (R-AZ)
Commercial Privacy Bill of Rights Act of 2011 (co-sponsor)

Richard Blumenthal (D-CT)
Personal Data Protection and Breach Accountability Act of 2011

“When a data breach occurs, it is essential that customers be immediately notified about whether and to what extent their personal and financial information has been compromised.”
Major Themes in Federal Legislation

Theme #1 – Security requirements
Theme #2 – FTC regulation and enforcement
Theme #3 – Breach notification
Theme #4 – Preemption/Exemption
Theme #5 – Additional enforcement
Theme #1: Security Requirements

- Good – Many codify “flexibility of approach”
  - Size and capabilities
  - Nature, scope and complexity of operations
  - Cost and benefit
  - Reminiscent of HIPAA, GLB and MA flexibility of approach
Theme #1: Security Requirements

• Bad – Fairly specific requirements
  – Required “security officer” (Bono Mack, Stearns)
  – Specific measures for secure disposal of “obsolete data” (Stearns) (similar but more general measures for Bono Mack)
  – Risk assessment (Rush)
    • prior to implementation (volume of data)
    • whether information “is and remains necessary for the purposes disclosed at the time of collection”
    • whether “ongoing collection practices are and remain necessary for a legitimate business purpose”
Theme #1: Security Requirements

• Really, really ugly – **VERY** specific requirements (Blumenthal, Leahy)
  
  “[P]rotect [PII] during use, transmission, storage, and disposal by encryption, redaction, or access controls that are widely accepted as an effective industry practice or industry standard, or other reasonable means”

  – Risk assessment and risk management
  – Access controls and logs (all views?)
  – System activity (log, monitor, detect)
  – “Proper” disposal of information and media
  – Training
  – Vendor due diligence and contracting
  – Vulnerability testing
  – Evaluation (changing technology, systems, threats, information, business (M&A, joint ventures, outsourcing, bankruptcy))
Theme #1: Security Requirements

• Really, really ugly – data minimization
  
  – “Minimize the amount of personal information maintained by the business entity, providing for the retention of such personal information only as reasonably needed for the business purposes of the business entity or as necessary to comply with any other provision of law.” — Blumenthal
  
  – “…establish a plan and procedures for minimizing the amount of personal information maintained…provide for the retention of such personal information only as reasonably needed for the business purposes…or as necessary to comply with any legal obligation.” — Bono Mack
  
  – See also Kerry/McCain, Leahy, Rush
  
  – Records management
Do We Need More Regulation?: The Existing Patchwork

• Sources of Requirements
  – Federal = industry sector (HIPAA, GLB, FCRA, etc.)
  – State = jurisdiction/topical (CA, NV, MA, NC, etc.)
  – Contracts (BAA, PCI DSS, data transfer, general, etc.)
  – Caselaw and government enforcement
  – Your own privacy notice

• Challenges
  – Piecemeal application (industry sector, residency of individuals, topic-specific, multiple jurisdictions, etc.)
  – Disparate contractual obligations
  – Intricacy of the requirements…
Statutory/Regulatory Security Requirements – Selected Examples

• Implementation of “administrative, physical and technical safeguards”

• Employee assigned with responsibility for program

• Physical and technical access management
  – Authorization
  – Establishment
  – Modification
  – Termination
Security Requirements – Selected Examples (2)

- Person or entity authentication
- Security awareness and training
- Security incident (breach) response procedures
- Contingency and disaster recovery planning
- Emergency mode operation plan
- Data back-up
- Device and media controls
- System logging and monitoring
Security Requirements – Selected Examples (3)

- Data integrity controls
- Encryption of data in storage
- Encryption of data in transmission
- Facility access plan
- Workstation security
- Employee sanctions
- Periodic risk analysis and management
- Periodic compliance evaluations
Security Requirements – Selected Examples (4)

- Vendor management
  - Diligence and ongoing oversight may be required
  - Written security contract legally required
  - Mandatory contract provisions
  - Service provider must downstream all requirements to subcontractors

- Secure disposal

- Program must be fully documented
Security – Additional Contractual Obligations

- Breach reporting
- Breach mitigation
- Audit rights
- Encryption (mandatory)
- Security certification
- Control of subcontractors
- Cost shifting
Theme #2 – FTC Regulation and Enforcement

• Good? – at least the following bills provide for FTC regulation:
  – SAFE Data Act
  – Commercial Privacy Bill of Rights Act of 2011
  – Personal Data Privacy and Security Act
  – Personal Data Protection and Breach Accountability Act of 2011
  – Data Accountability and Trust Act (DATA) of 2011
  – BEST PRACTICES Act

• Bad? – regulations likely to evolve

• Really, really ugly – steep penalties
  – Violations of FTC rules generally charged at $16K per violation, no cap; equitable relief generally includes biennial audits for 20 years
Does the FTC Need Greater Authority?: Current Enforcement

- Current authority does not include monetary penalties (unless order or rule is violated)

- Typical consent order:
  - Requires risk assessment
  - Requires implementation of a comprehensive, written information security program with administrative, physical, and technical safeguards (see below)
  - Third party audit required with FTC oversight
  - Biennial for duration of order (10 or 20 years)
  - Audit report and all underlying policies, procedures, training, etc. provided to FTC for review
FTC Enforcement – Specific Security Allegations

- **DSW**
  - Stored information in multiple files when it no longer had a business need to keep the information
  - Stored the information in unencrypted files that could be accessed easily by using a commonly known user ID and password

- **TJX**
  - Stored and transmitted personal information in clear text
  - Did not require network administrators and other users to use strong passwords or to use different passwords to access different programs, computers, and networks
FTC Enforcement – Specific Security Allegations (2)

• Reed Elsevier Inc. and Seisint, Inc.
  – Failed to establish or enforce rules sufficient to make user credentials hard to guess; allowed customers to use the same word, including common dictionary words, as both the password and user ID, or a close variant of the user ID as the password
  – Failed to require periodic changes of user credentials, such as every 90 days, for customers with access to sensitive nonpublic information
  – Failed to suspend user credentials after a certain number of unsuccessful log-in attempts
  – Allowed customers to store their user credentials in a vulnerable format in cookies on their computers
FTC Enforcement – Specific Security Allegations (3)

• Twitter
  – Failure to use strong passwords
  – Failure to maintain separate site for administrator log on
  – Employees storing passwords in email accounts

• Dave & Buster’s
  – Failure to employ sufficient measures to detect and prevent unauthorized access, such as an intrusion detection system and monitoring system logs
  – Failure to monitor and filter outbound traffic from networks to identify and block export of information without authorization
Theme #3 – Breach Notification

• Good
  – Preemption of state requirements (more later)
  – Harm thresholds for notification (e.g., Blumenthal, Leahy – “significant risk of harm or fraud,” but with required risk assessment and review by Secret Service or FBI)
  – Presumption of no risk if encrypted (Bono Mack and Stearns provide possibility of other technical options to qualify for presumption)
Theme #3 – Breach Notification

• Bad
  – Covering data in addition to the “norm” (SSN, driver’s license, financial account info, info permitting access to financial resources)
    • Blumenthal and Leahy include (1) biometric data, (2) passport number, (3) alien registration number, (4) combo of any two of maiden name, DOB, phone number, and home address, and (4) any data that would permit access to foregoing
    • Bono Mack would allow FTC to expand definition
  – Tight timeframe for notification (Bono Mack – 48 hours)
  – No harm threshold (Bono Mack – law enforcement)
  – Mandatory 2 years of credit monitoring (Blumenthal, Bono Mack, Stearns, etc.)
Theme #4 – Preemption/Exemption

• Good – clear preemption/exemption standards
  – Clear preemption of state data security and all state and federal breach notification requirements (Leahy, Stearns)
  – HIPAA and GLB covered entities exempted to the extent laws apply (Bono Mack)

• Bad – confusing or ambiguous preemption/exemption
  – Unclear extent of exception for HIPAA and GLB covered entities; no express recognition of limited scope
    • Blumenthal, Leahy, Kerry/McCain, Stearns (silent)
  – Types of data covered
    • Kerry/McCain – (1) preempts state laws regarding collection and use of information covered by bill; (2) expressly preserves state laws regarding health and financial information; (3) everything else?
    • Hard copy
Theme #4 – Preemption/Exemption

• Really, really ugly – no express preemption
  – No express preemption of state data security requirements – Blumenthal
  – Expressly preserves state breach notification laws – Kerry/McCain, Rush
Theme #5 – Additional Enforcement

- Good (sort of) – FTC or U.S. Attorney General only
- Bad – state attorney general enforcement (in addition)
  - Blumenthal – equitable relief, penalties of $500 per day per individual with maximum cap of $20M per violation, unless conduct was willful (then no cap); violations presumed willful
  - Bono Mack – $11K per violation to $5M max (per section of bill)
  - Leahy
    - Regarding data security requirements – equitable relief, penalties of $500 per day per individual with maximum cap of $500K
    - Regarding security breach requirements – equitable relief, penalties of $1K per day per individual with maximum cap of $1M unless conduct was willful (then no cap)
Theme #5 – Additional Enforcement

- Bad – state attorney general enforcement (cont’d)
  - Stearns – $11K per day with maximum cap of $5M total
  - Rush – $11K per day with maximum cap of $5M for “related series of violations”
  - Kerry – knowing or repeated security violations $16.5K per day or per person (whichever greater) with maximum cap of $3M for “related series of violations”
Theme #5 – Additional Enforcement

• Really, really ugly – private rights of action and criminal penalties
  – Blumenthal – “harmed” individuals may sue for $500 per day violation persists to maximum of $20M per violation, punitive damages and equitable relief
  – Blumenthal – violations of certain provisions constitutes per se negligence (supports tort claim)
  – Rush – greater of any actual damages of not less than $100 and not more than $1,000, punitive damages, and attorney’s fees
  – Leahy – Criminal sanctions for concealing a security breach
Federal Agency Initiatives
Evolution FTC Enforcement

• Becoming increasingly granular in allegations
• “Unfair” trade practice and “reasonable” security are subjective standards that evolve with:
  – Technology
  – Types of attacks and risks
  – Best practices
• Security flaws typically do not otherwise constitute a legal violation (no underlying HIPAA or state law violation alleged by FTC)
  – Meeting your statutory/regulatory obligations may not be enough
FTC Initiatives

- “Privacy by Design”
- Google Buzz
  - Unfair and deceptive trade practice
  - Safe Harbor violation
- Consent Order
  - Bars further misrepresentations
  - Requires consent before sharing information contrary to privacy promises/notice
  - Requires comprehensive privacy program “reasonably designed to address privacy risks related to the development and management of new and existing products and services for consumers”
  - Biennial audits by independent third party the next 20 years
  - Anti-competitive behavior?
U.S. Department of Health and Human Services

• HITECH Act
  – Shifted security enforcement to OCR
  – Breach notification
  – Fining authority
  – Mandatory Audits
  – State AG training

• New rules due imminently
  – Business Associates must fully comply with Security Rule
  – BAAs must be updated
  – Direct liability for Business Associates and BAA no longer a shield from liability for Covered Entities
  – New privacy requirements (including Access Report?)
U.S. Department of Health and Human Services

• Enforcement
  – CVS Caremark ($2.25M) (joint FTC)
  – Rite Aid ($1M) (joint FTC)
  – Cignet Health ($4.3M)
  – Mass General ($1M)
  – UCLA (~$900K)

• Remedies
  – Corrective action plan / comprehensive info security program
  – Assessments and compliance reports (HHS – annually for 3 years, FTC – biennially for 20 years)
More NLRB Rulings Illustrate Broad Scope Of "Concerted Activity" Protection

03.28.2011
Louis B. Meyer III
David L. Woodard

In a recent alert, we reported on two recent cases before the National Labor Relations Board (NLRB) involving a provision of the National Labor Relations Act (the Act) that protects employees’ rights to engage in “concerted activity.” Under this provision of the Act, “concerted activity” includes, among other things, two or more employees discussing wages, hours, or working conditions. The Act prohibits employers from disciplining or discriminating against employees who engage in such discussions. This “concerted activity” protection extends to employees whether or not they are unionized.

In one of the cases discussed in our earlier alert, the employer allegedly fired an employee for her disparaging Facebook posts about a supervisor, to which several of her Facebook “friends” who were also co-workers added their comments. The employer fired the employee for violating a policy in its company handbook prohibiting employees from making disparaging or defamatory comments when discussing the company or their superiors. The NLRB filed a complaint against the employer asserting that its policies and disciplinary actions were an unlawful infringement on the Act’s “concerted activity” protection because the Facebook communications between the fired employee and her co-workers were discussions about
National Labor Relations Board

• About a dozen cases involving social media
  – No adverse action required!

• A few cases ended badly for employers:
  – Employee asked coworkers on her Facebook page for their reaction to another employee’s complaints about work quality and staffing levels
  – Employee complained on her Facebook page about supervisor’s refusal to permit union rep to assist her in developing a response to a customer complaint filed against her
  – Employees’ Facebook posts reveal employer’s failure to withhold state income taxes; state tax authorities issued payment demand
National Labor Relations Board

• More likely to be protected activity
  – Subject matter related to terms and conditions of employment, exercise of union rights, or other matters traditionally considered “protected activity”
  – Other employees were participating in the conversation (“concerted activity”)
  – Content that is part of a continuing dispute with employer or ongoing conversation with other employees

• Less likely to be protected activity
  – Negative impact on productivity
  – Complaints amounted to “name calling”
  – Content inappropriate (keep it clean!)
State Initiatives
State Initiatives – Enforcement

• Little FTC Acts (unfair and deceptive)
  – Beware of multi-state actions

• State breach notification laws (timing)
  – Indiana AG sues Wellpoint for $300,000 for delayed breach notification (settles for $100,000 – delay was almost 3 months)

• State disposal laws (dumpster diving)
  – Special focus in TX; some activity in other states (including NC!)

• HIPAA
  – Several actions in CT, one 6-figure settlement
  – OCR training for AGs
  – “Elected Official Effect”
State Initiatives – Added Complexity

• HIEs
  – Legislative changes (opt in v. opt out)
  – Highly contractual
  – Triggering additional requirements? (Texas)

• Smart Grid
  – State utility commissions – regulatory changes
  – Example – CA PUC
    • Reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.
    • Breach notification (to PUC)
Questions?

Elizabeth Johnson  
Partner  
Poyner Spruill LLP  
(919) 783-2971  
ejohnson@poyners.com