

Security Breach Notifications: Politics and Approaches

Priscilla M. Regan

George Mason University

March 6, 2009

BCLT Security Breach Notification

Symposium

Congressional Activity

- 109th Congress
 - More than 20 bills
 - 3 hearings
 - Senate & House committees reported 3 bills
 - VA data breach law
- 110th Congress
 - Similar number of bills
 - Senate committee reported 3 bills
 - House passed bill w/new req'ments on federal agencies and req'ing OMB to notify about security breaches
- 111th Congress

Typical Case of Information Privacy?

■ Differences

- Defined in terms of security not privacy
- Affirmative requirement on organizations –focus not on rights to individuals
- Notice to affected data subjects as group
- All organizations treated similarly – not sectoral approach

■ Similarities

- Notice in tradition of FIPs
- Incident or crisis driven

Congressional Politics: Procedural Factors

- Multiple congressional committees w/jurisdiction
- Variety of congressional approaches
- Partisan politics
- Executive and FTC activity as well

Congressional Politics: Substantive Issues (1)

- Federal Preemption
 - 44 states with laws modeled largely on CA's
 - Likely to weaken state laws
 - Industry advocating national policy

Congressional Politics: Substantive Issues (2)

- Policy Problem and Goal
 - Increased risk of identity theft, then goal is to reduce likelihood of identity theft
 - Lax or ineffective organizational data security, then the goal is to improve data security practices
 - Lack of public awareness about the ways in which personally identifiable information is collected, exchanged, retained, then policy goal is to provide public with necessary information

Congressional Politics: Substantive Issues (3)

- Effectiveness of Notices
 - Critics
 - Individuals will ignore, unnecessary costs on consumers
 - Supporters
 - Incentive to organizations
 - Value in meeting policy goals
 - Reducing identity theft
 - Increasing effectiveness of security practices
 - Increasing public awareness

Effectiveness of Notices – Targeted Transparency*

- Effective policies:
 - provide facts in ways that people want in times, places and ways that enable them to act – user-centered;
 - embed new information in users’ and disclosers’ existing decision-making routines;
 - increase knowledge that informs choice;
 - impose sanctions for non-reporting and misreporting;
 - require watchdogs, oversight, enforcement system; leverage existing systems.

*Fung, Graham and Weil, *Full Disclosure: The Perils and Promise of Transparency* (Cambridge University Press, 2007)

Targeted Transparency

- Sanguine about the political reality
 - politics always affect transparency policies;
 - there is never full disclosure;
 - initial policies are often somewhat incremental with improvements over time;
 - there is a need to incorporate analysis and feedback

Congressional Politics: Substantive Issues (4)

- Scope of policy
 - Seriousness of the breach (“reasonably likely” or “reasonably possible” that the information could be “misused” or “significant risk of identity theft” or “material risk of harm”)
 - Whether the breach has to affect a certain number of individuals (in one proposed bill notice requirements would apply only to entities holding information on more than 10,000 persons)
 - Whether data that is encrypted should be exempted (depending upon the encryption standard used)
 - Whether uniform for all organizations

Congressional Politics: Substantive Issues (5)

- Larger Framework – Ancillary Protections
 - Restrictions on use of SSN
 - Credit Freezes on consumer reports
 - Oversight body

Likelihood of Congressional Action

■ Unfavorable Factors

- Original “policy window” closed
- Conflicting agendas
- Classic regulatory – costs on small group, benefits widely distributed

■ Favorable Factors

- Current political climate
 - emphasis on transparency and accountability
 - disparagement for those who are causing “moral hazards”
- Public attention still high