

Are "Better" Security Breach Notification Laws Even Possible?

Jane K. Winn

Charles I. Stone Professor

University of Washington School of Law

Assessing Security Breach Notification Laws

- Legislative intent
 - Control identity theft or something else?
- What is “better” regulation?
 - What is “adversarial legalism”?
- Assessing strengths & weaknesses of SBNL
- Alternative approaches
- Obstacles to alternative approaches

Legislative Intent of SBNL

- Don't get mad, get even
 - California state payroll database hacked into but victims not notified for weeks
 - Unfunded delegation of regulatory function to private sector
 - Anti-money laundering laws and banks versus customers
 - Security breach notification laws and data custodians versus self
- Narrow issue with high probability of enactment
 - Presumed causal link between security breaches and identity theft
- Is it economic regulation or social regulation?
 - Disclosure regulation as substitute for substantive regulation
 - What specific response to notice was expected?
 - After enough security breach notifications will public consensus shift?
 - Correct market failure with competition?
 - Credit monitoring services
 - Easy credit as a fundamental right v. privacy as a fundamental right

Environmental Protection Analogy

- Goal: mandate internalization of externalities; sustainable development
- Prelude: **National Environmental Policy Act 1970 to collect and disclose information to inform policy**
- 1st generation command and control regulations
 - Technology-based control measures
 - Air/water quality standards
- 2nd generation
 - Economic incentives: taxes; cap-and-trade toxic byproducts
 - New liability rules: Superfund/CERCLA
 - Public/Private cooperation: negotiated regulation/regulatory “contracts”
 - EMS/ISO 14000
 - **Mandatory information disclosure of emissions**

What is “Better Regulation”?

- 1997 UK Better Regulation Task Force Principles:
 - Proportionality
 - Accountability
 - Consistency
 - Transparency
 - Targeting
- But isn't UK doing even *worse* than US?
 - Failure to remember significance of “systemic risk”
 - Ideological commitment to deregulation
 - Not all bad ideas: Child Trust Fund £250 born after 2002
 - <http://www.childtrustfund.gov.uk/>
- Responsive Regulation & Enforcement Pyramid
 - Most effective strategy for regulators is “tit-for-tat”

SBNL as Regulation

- Information regulation
 - Correct market failure due to information asymmetry
- De facto strict liability rule
 - Breach notwithstanding best practices burden unchanged
 - Distortion of investment to avoid litigation rather than improve security
- Unsupervised delegation creates impaired self-regulatory regime
 - Wholesale ignorance/noncompliance by putative enforcement personnel

Enforcement Pyramid



Are SBNLs “Better” Regulation? (1)

- Not Proportional
 - Good data custodian follows “best practices” but suffers breach, pays millions to mail letters
 - Bad data custodian is unaware of breach, sends no notices
- No accountability
 - Data custodians make notice determinations in private without review
 - No public audits required, limited public enforcement
 - No entitlement to remedy after receiving notification

Are SBNLs “Better” Regulation? (2)

- Consistency (laws must be “joined up” and fairly enforced)
 - No general duty of information security, general right of privacy
 - Limited recourse after notice received
 - No public funding for enforcement, no monitoring of self-regulation
 - Public companies over-disclose, over-invest
 - SMEs simply clueless
 - Bad actors conceal information with impunity
- Transparency (“user-friendly” regulations)
 - Are notices designed to avoid liability or inform?
- Targeting
 - Focus on fact of breach and formal notice, not on actual risk of identity theft
 - Compare: FTC Red Flag Rule applies to creditors who open new accounts
 - Lack of focus on choices facing system operators, end users
 - Compare: FFIEC failure to mandate 2 factor identification for old accounts

Are SNBLs “Responsive Regulation”?

- Advise and persuade
 - Australia, Canada, New Zealand, United Kingdom Security Breach Guidance
 - US vendors selling products and services
- Inspect and examine (ex ante)
 - Nothing?
- Notices and warning letters (ex ante to data custodians)
 - Nothing?
- Civil penalties
 - Cost of sending notices?
- License revocation, suspension of business
 - PCI DSS block access to credit card networks?

Alternative Approaches

- Clarify objectives
 - Reduce identity theft?
 - Strengthen information privacy rights?
 - **Improve information security?**
- Improve enterprise level information security
 - Enforced self-regulation based on integrated risk management
 - Public subsidies for basic research and standards

Obstacles to alternative approaches

- Ambivalence about adversarial legalism
 - Craft limited remedy based on limited facts, then adapt
 - Class action anxiety among data custodians
 - Ex post search for “total justice” versus ex ante cost-benefit analysis
- Ambivalence about privacy and commerce
 - Commodification of identity compatible with US consumerism
- What if the real problem is systemic risk?
 - What if open networks are the Afghanistan of administrative systems?