Carnegie Mellon

Consumer Privacy Costs and Personal Data Protection:

Economic and Legal Perspectives

Alessandro Acquisti
Sasha Romanosky

March 06, 2009
BCLT/BTLJ Symposium

Carnegie Mellon
Heinz College

Outline

1. We investigated the effect of data breach disclosure laws (aka SBNs) on identity theft rates

… this got us thinking about other legal mechanisms that try to reduce the privacy harm from firms' otherwise socially beneficial activities

2. Hence, we started investigating and contrasting the legal and economic doctrines on the costs of consumer data breaches and their remedies

Background

- Impact of data breach disclosure laws represents a familiar public policy issue of empirical estimation: the *treatment effect* of a law on a crime

- Also represents a very interesting research challenge
  - The outcome is not clear
  - Strong arguments to support both positions in favor of and against these types of laws

Why should SBNs work?

Sunlight as a disinfectant (Brandeis, 1933)

- Highlighting a firm's poor security practices will encourage firms to improve (reducing the externality)
- "Drive performance through transparency and public oversight" (Mulligan, 2007)

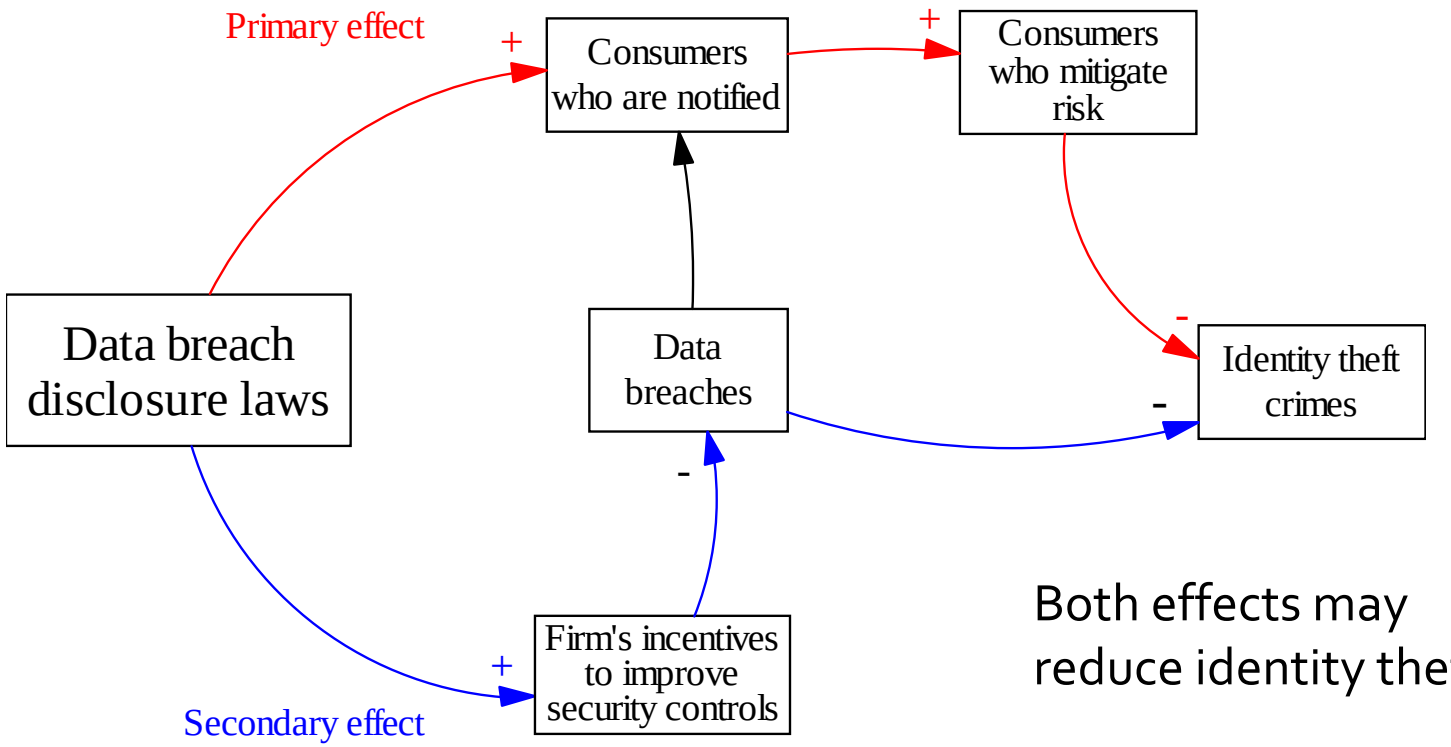
Right to know (Magat & Viscusi, 1992; Solove, 2004)

- Consumers have the right to know when a firm is using, or *abusing* their information.
- By notifying consumers of breaches, they can mitigate the risks (close accounts, warn banks/CC firms, freeze credit, idtheft insurance)

…but not everyone agrees

- Cause firms and consumers to incur unnecessary costs, esp. if the probability of idtheft from a breach is < 2% (idAnalytics, 2006; Ponemon, 2008)
- The externality is not nearly so grave: firms already bear ~90% of the cost of breaches (Javelin Research, 2003, 2005, 2006)
- Consumers could become desensitized to numerous breach notifications (Cate 2005)
- Stifles ecommerce and R&D by discouraging firms to innovate (Rubin and Lenard, 2005)

Conceptual model

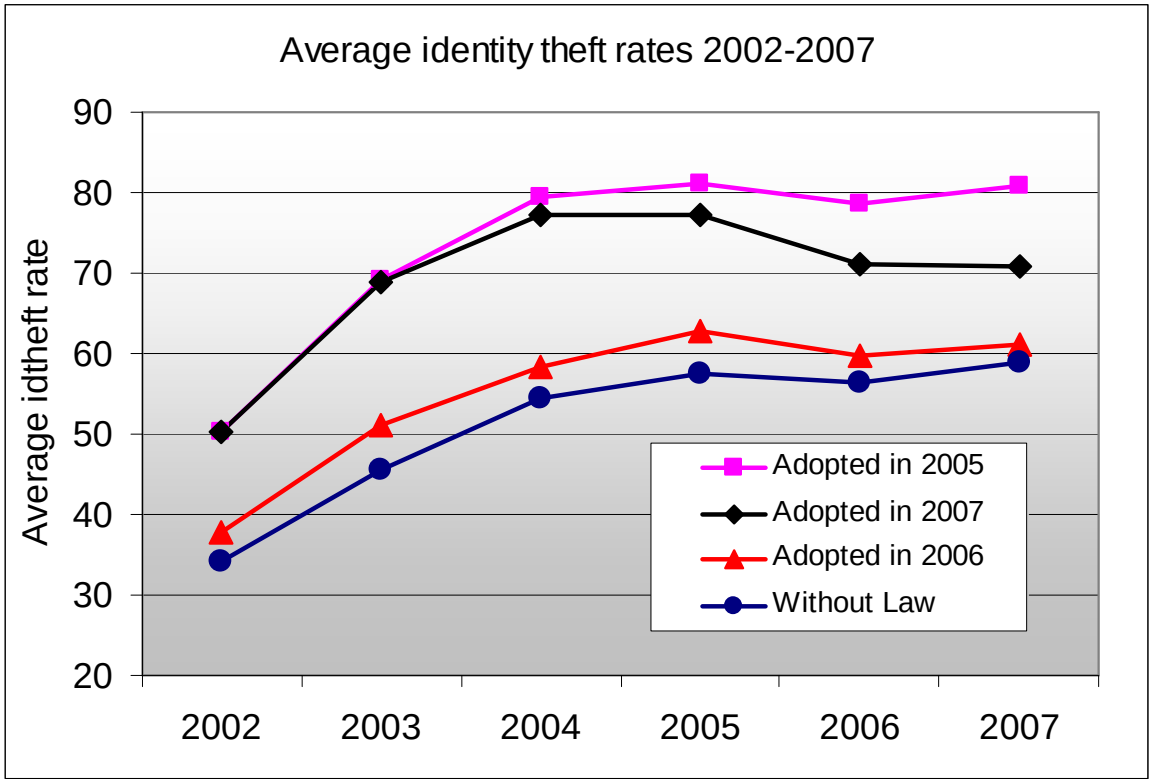


Both effects may reduce identity theft

Data collection

- We acquired monthly data, by state, for 2002-2007 from the FTC using Freedom Of Information Act
- Aggregated to semi-annual periods (smallest period over which we expect to see an effect of law)
- 12 periods * 50 states (+ D.C.) = 612 obs
- Reported data:
  - frequently used for research analysis (Blumstein et al, 1991)
  - represents the best panel we have on identity theft

ID theft rates for states with/without law



Idtheft for states *with* and *without* law appear to follow same trend.

Idtheft rate: number of crimes per 100,000 people

Econometric model

- $idtheft_{st} = \beta_0 + \beta_1 hasLaw_{st} + \beta_2 breaches_{st} + \sum \rho_i Related_{st} + \sum \delta_j Economic_{st} + \sum \alpha_k Crime_{st} + \theta_s + \lambda_t + \varepsilon_{st}$

- A familiar approach to analyzing such policy issues
- Identification comes from variation across *state and time*

- We controlled for:
  - Breach in one state causing reported idtheft in another state
  - Increase in reporting due to disclosure laws (awareness bias)
  - Also: socio-economic variables, population, unemployment, other crimes.

Results

- Adoption of the laws reduce identity theft rate by 1.3
- For 2005, this represents about a 2% reduction in ID theft due to data breaches; $1 billion reduction in total loss

- Compare impact against similar analyses:

Research	Treatment	Outcome measure (Result)
Hamilton (1995)	Disclosure of toxic release (TRI)	Stock price: -0.3%
Acquisti, Telang, Friedman (2006)	Disclosure of security breach	Stock price: -0.6%
Epple and Visscher (1984)	Coast guard monitoring (measuring deterrent effect)	Oil spill frequency: +2.1% Oil spill volume: - 3.1%
Cohen (1987)	Coast guard monitoring	Oil spill frequency: -2% Oil spill volume: -1.7%

Conclusions (first paper)

- Overall, while some evidence shows that data breach notification laws have an effect…
  - on companies: new access controls, auditing measures, and encryption (Samuelson Clinic 2007; Mulligan & Simitian 2009)
  - increasing cost of data breaches for companies (Ponemon 2009)
  - lowering consumers losses (time, money) (Javelin 2008, 2009)
- **… we found only limited evidence of impact on identity theft**
- A lack of stronger influence may be due to the following:
  - Our regression analysis may be too blunt an instrument with which to measure an effect
  - The reported data may be a poor source
- **Or, it may signal a more "structural" challenge for the legislative approach**

From SBNs to the economics of liability, regulation, and disclosure

- Our findings got us thinking about other legal mechanisms that try to reduce the privacy harm from firms' otherwise socially beneficial activities
- Hence, we started investigating and contrasting the legal and economic doctrines on the costs of consumer data breaches and their remedies
  - I.e., not just ID theft, and not just SBNs

Alternative approaches to consumer (data) protection

Pre-event (harm has not yet occurred)	Potential for harm exists	Post event (harm has occurred)
		
Prevention mechanism that reduces the probability of a harmful event from occurring	Corrective mechanism. Disclosure of potential harm. A light-handed incentive device.	Recovery mechanism. Meant to compensate injured parties for their loss.

… corresponding to a patchwork of legislative initiatives

- *Ex ante* regulation
  - SOX, HIPAA
  - New state laws requiring encryption of portable devices (MA, NV, …)
  - New state laws mandating protection of SSNs (CT, RI, TX)
  - …
- *Ex post* liability
  - Plastic Card Security Act (MN)
  - State laws that hold breached firms liable to acquiring banks for cost of sending new credit cards (CT)
  - Some state disclosure laws allow private right of action
  - …
- Disclosure
  - SBNs: Data breach disclosure laws (at least 44 states)

What is their impact?

- Lack of systematic evidence
  - Most laws are recent
  - Difficult to gather good data
  - Appropriate metrics not always clear, because of complex interactions between firms, consumers, policy makers
    - E.g.: Focus on ID theft number or magnitude? Consider secondary effects (such as impact of credit availability) or not?
- Also, loaded question
  - Are legislator's intentions clear?
    - Is the intention to "protect" privacy or rather balance information needs of various parties?
  - Must consider costs and benefits for various parties
  - And to calculate overall welfare effects, we must often resort to (subjective) weights

A mixed picture

- Qualitative evidence
  - Damage per ID theft is down, and disclosure may be improving firms' practices, but…
  - Breaches keep increasing
  - ID theft incidents keep increasing
  - Yet, fines are few and (relatively) minor
    - Single SEC fine (LPL financial, $275,000), a couple dozen FTC fines/sanctions, limited PCI fines ($11.5M in 2007) (contractual), …
  - Few or no successful private actions (i.e. suing breached companies)
- Quantitative evidence
  - Limited impact of breaches on stock market valuation of breached firms
  - Limited impact on ID theft incidence

➢ *Notwithstanding significant legislative efforts, a mixed picture*

What may explain a limited impact of the laws?

- A problem of focus?
- A problem of mechanisms?

Focus: Economic vs. legal costs

- Consider DPPA (1994)
  - Enacted to explicitly "[prohibit] release and use of certain personal information from State motor vehicle records"
  - Specifically, established that the offended individual may bring a civil action in a US district court against violators, and the court may award "***actual damages***, *but not less than liquidated damages in the amount of $2,500*"
    - …making it really difficult for any damages to be actually liquidated

Focus: Economic vs. legal costs

- Legal and economic theories consider costs differently
  - Usually, rightly so
- The law thinks (mostly) in terms of realized damages
  - *"threat of future harm, not yet realized, will not satisfy the [actual] damage requirement" … "plaintiffs failed to demonstrate that any damages were actual or imminent" … "unless you have an actual showing of harm as a victim of identity theft, potential harm will not suffice"*
- Economics thinks in terms of *expected costs*
  - The value associated with distribution of events, times the probability of those events
  - I.e. , current and future, tangible and intangible, actual costs as well as opportunity (e.g., loss in value) (See also Solove 2008)

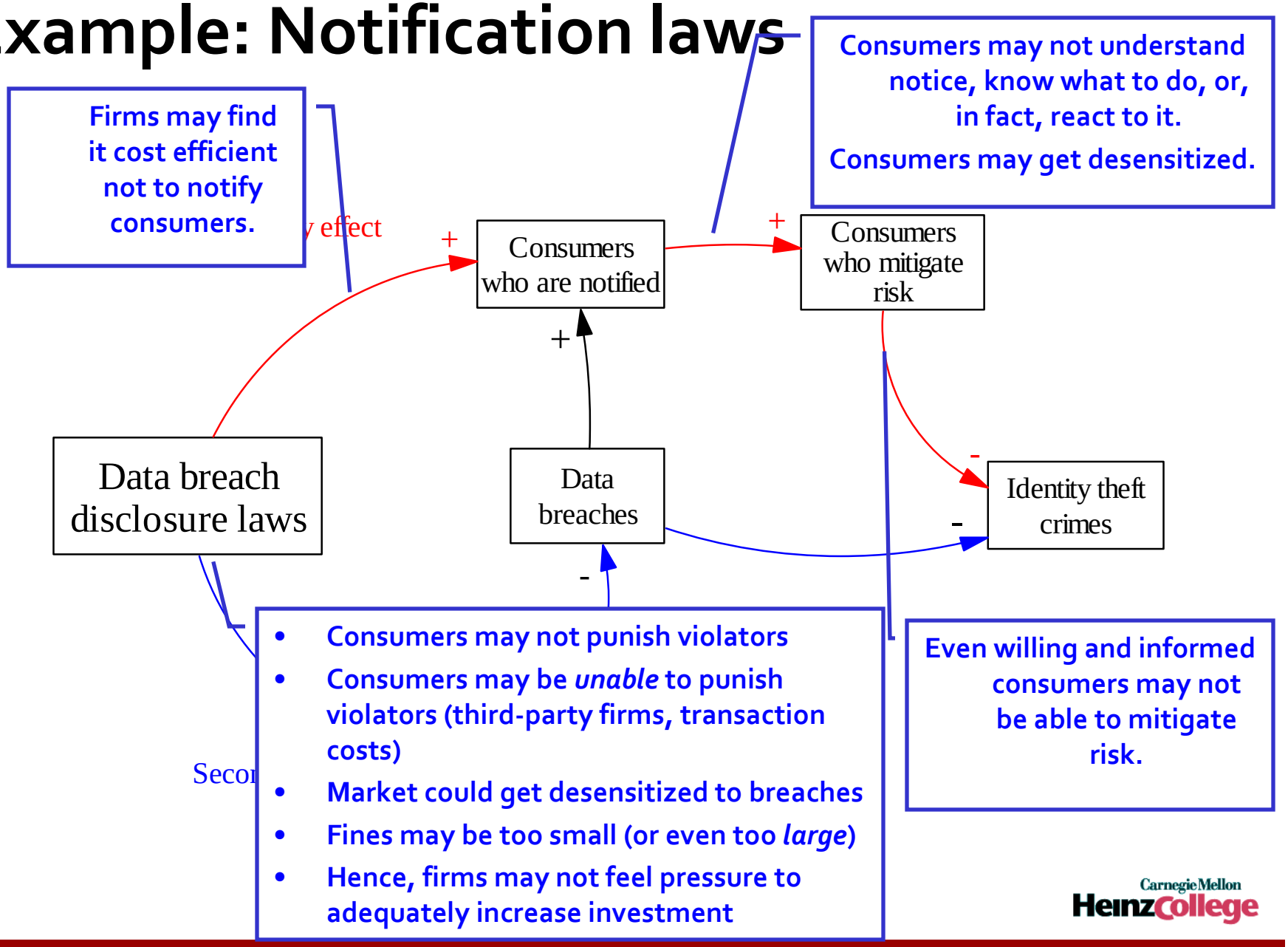
Focus: Economic and legal costs

- The issue: consumer costs from data breaches may in fact arise:
  - Long past the breach event (IdAnalytics 2005)
  - Difficult to attribute to one specific event or firm
  - Furthermore, there exists an inherent uncertainty in the process through which privacy losses impact consumers - many privacy costs are in fact *ex post*, intangible, or opportunity costs
  - See Varian's *blank check* analogy

Mechanisms: Economic and legal views

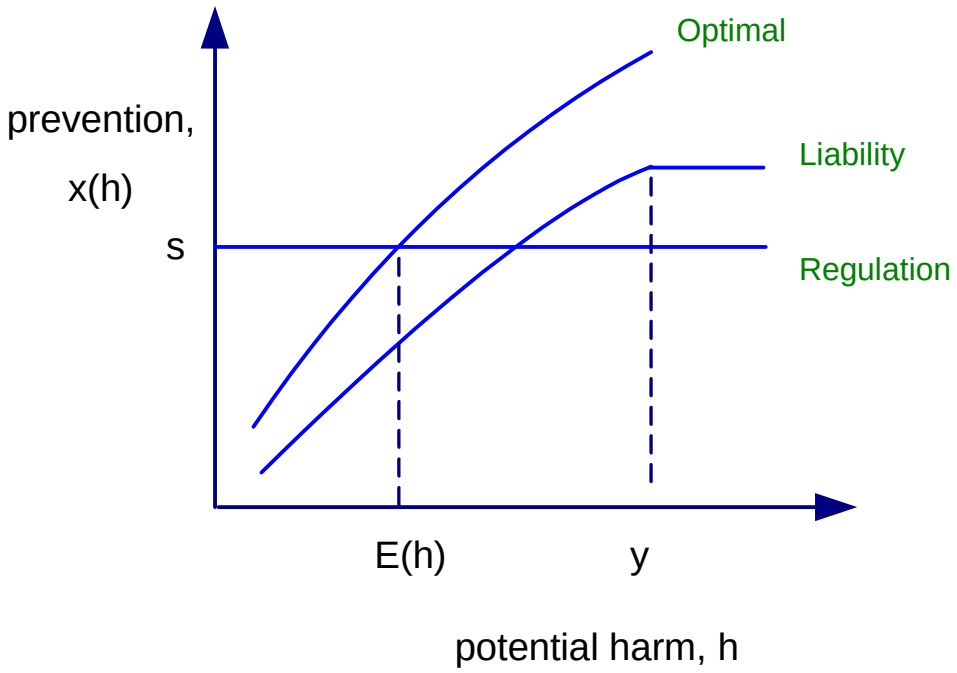
- *Ex post*, *ex ante*, and disclosure approaches sometimes rely on implicit assumptions about
  - Market players' incentives
  - Complete information
  - Limited transaction costs
  - Rational consumer behavior
  - …
- While in fact market players may not react to the incentives, consumers may not be willing (or able) to punish the violators, and firms may find it cost effective to do nothing
  - Lessons from behavioral economics and transaction costs economics

Example: Notification laws



Is there an "optimal" mechanism?

- Economic theories of regulation and liability
  - E.g., Shavell (1984); Kolstad, Ulen and Johnson (1990); …



Findings from this literature – and how they apply to breach costs

- *Ex ante*: appropriate when…
  - When harm is distributed across many victims
  - When knowledge of harm is unclear, even by victims
  - Long delay between event and resulting loss
  - When harm can be demonstrated statistically but not individually
- *Ex post*: appropriate when…
  - When firms are clear about the legal standard of care
  - When courts can observe a firm's level of care
  - When damages owed don't exceed a firm's assets (bankruptcy)
  - When probability of harm is low (admin costs occur only with lawsuit)
- Disclosures: appropriate when…
  - When consumers heed warning and actually take action to mitigate harm
  - When consumers penalize firms for bad behavior

Conclusions (so far)

- So far, mixed impact of data protection laws
  - More data needed for better analysis
- Possibly, a challenge both in terms of *focus* and *mechanisms*
- Economic theory suggests that *ex ante* and *ex post* approaches, alone, are inefficient - can't resolve all the issues
- Information disclosure bolsters these mechanisms with a different approach (command-and-control vs light-handed paternalism)

➢ *Even under these cooperative approaches, lessons from transaction costs and behavioral economics should be considered*