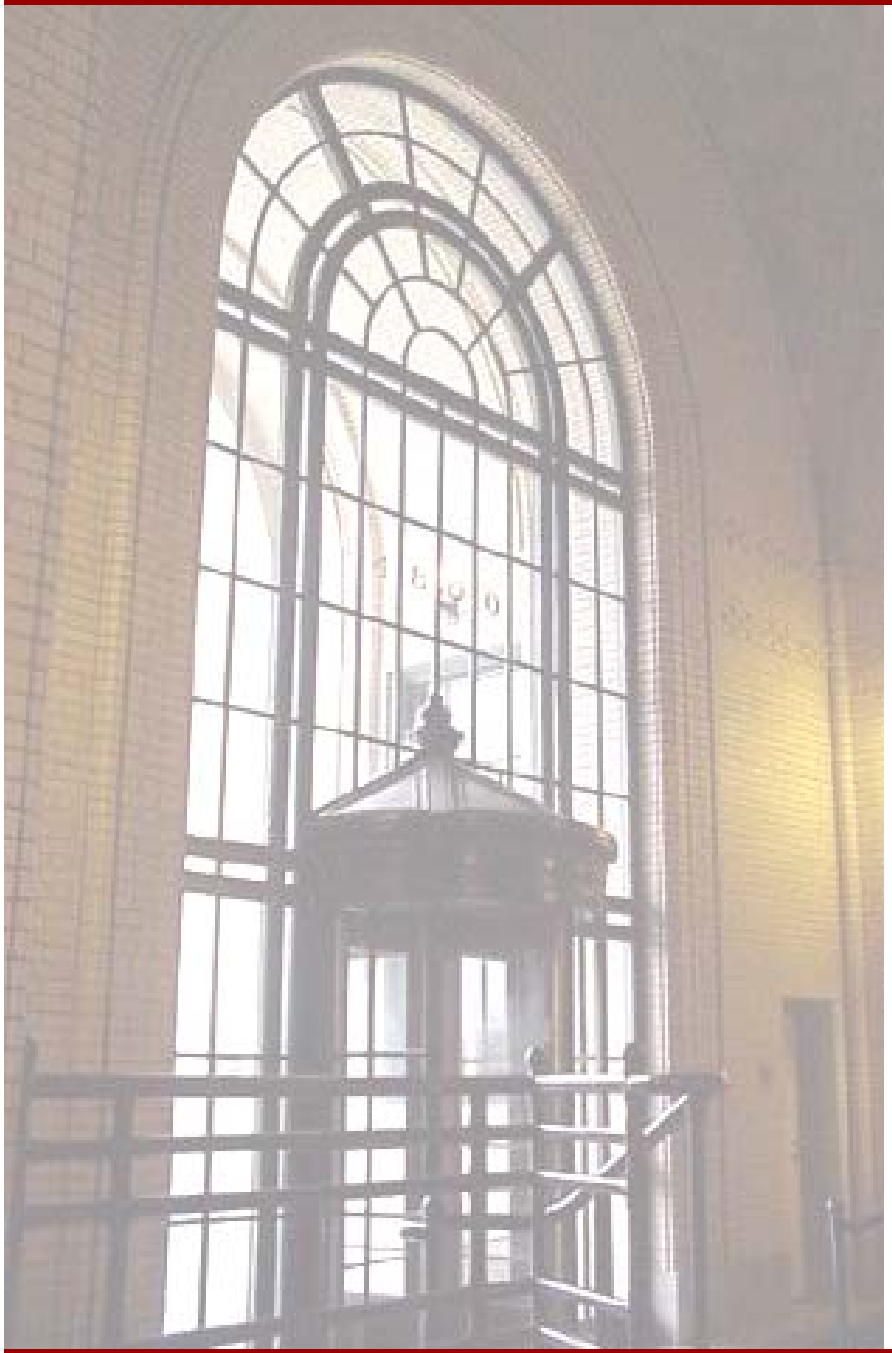
Carnegie Mellon



Data Breach Notification Laws:

An Economic Perspective on the US Experience

Alessandro Acquisti
Sasha Romanosky
Carnegie Mellon University

Responding to Data Breaches
European Parliament, 23 October 2009

Carnegie Mellon
HeinzCollege

SB 1386: The first data breach disclosure law

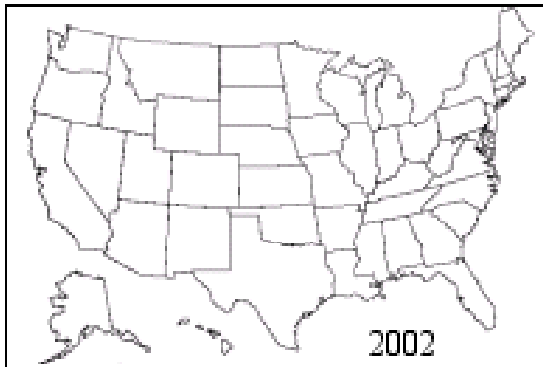
- In 2003, California was the first state to adopt a data breach disclosure (or "notification") law
  - Significant precedents of disclosure laws in the US: EPCRA, FDA, Hazardous Substances Act, Nutrition labeling, Fuel Octane levels, …

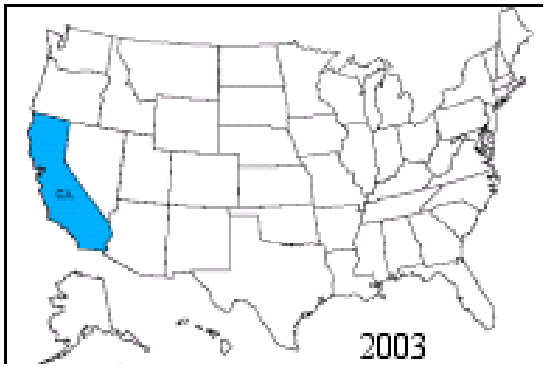
- SB 1386 has been the model by which most other states crafted their laws

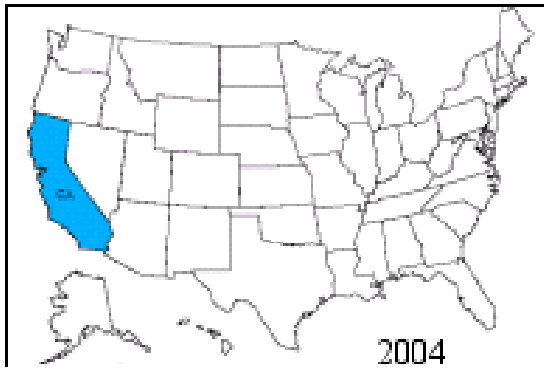
Data breach disclosure laws

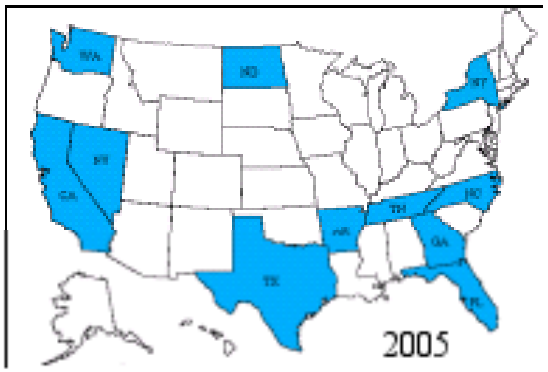
- Disclosure laws require firms to notify individuals (i.e., consumers) when their personal information has been lost or stolen
  - However, features of the laws greatly differ across States
- Objectives: inform consumers, incentivize investments in security, **reduce ID theft**
  - Five US Congressional hearings
  - Many laws were titled, "identity theft prevention" (MN, NJ, NC, and so forth)

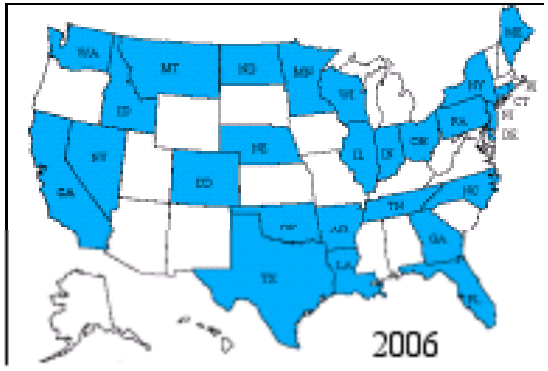
Adoption of state laws, 2002 - 2007

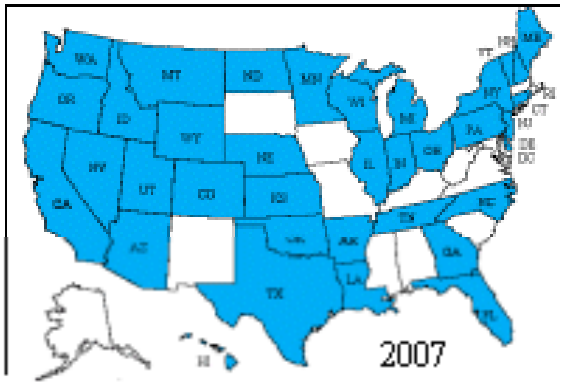












Why should breach notification laws work?

Sunlight as a disinfectant (Brandeis, 1933)

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

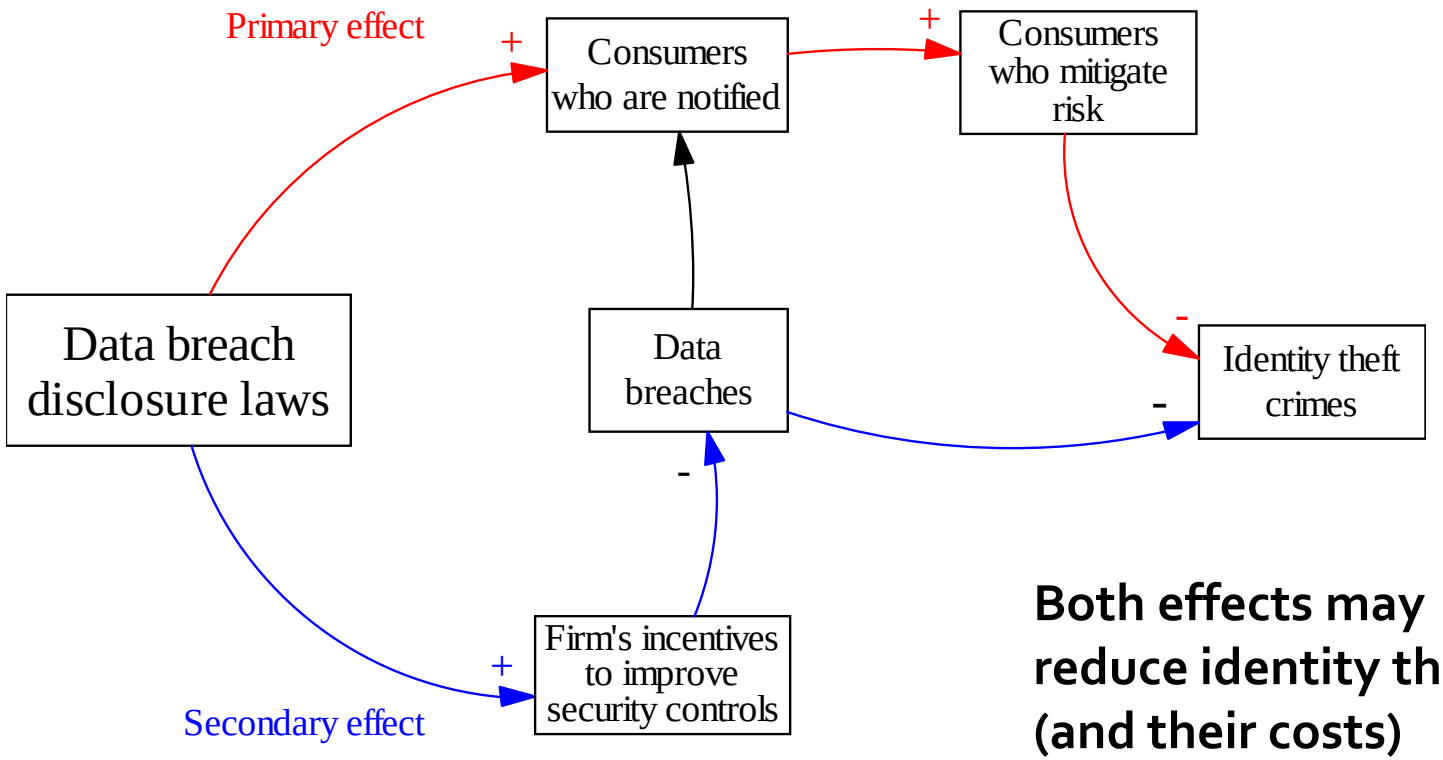
Right to know (Magat & Viscusi, 1992; Solove, 2004)

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

…but not everyone agrees

- May cause firms and consumers to incur unnecessary costs, esp. if the probability of idtheft from a breach is < 2% (Rubin and Lenard, 2005)
- The externality may not be 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)
- May stifle ecommerce and innovation by discouraging firms' investments in R&D (Rubin and Lenard, 2005)

Conceptual model: Impact on identity theft



Both effects may reduce identity theft (and their costs)

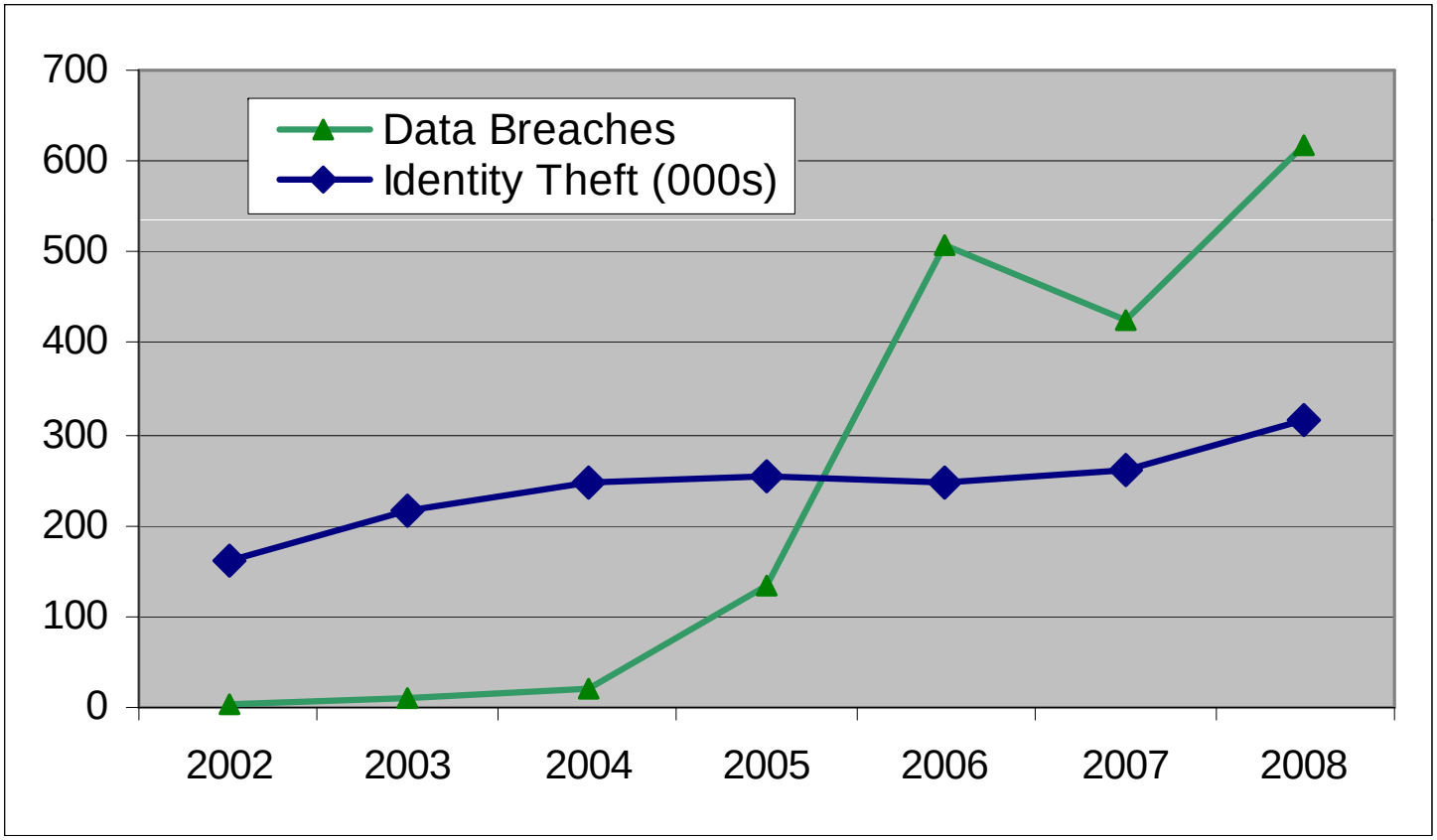
Data collection

- We acquired state-level, monthly data about *reported* identity theft incidents, for the 2002 through 2007 period
  - From the FTC, using a Freedom Of Information Act request

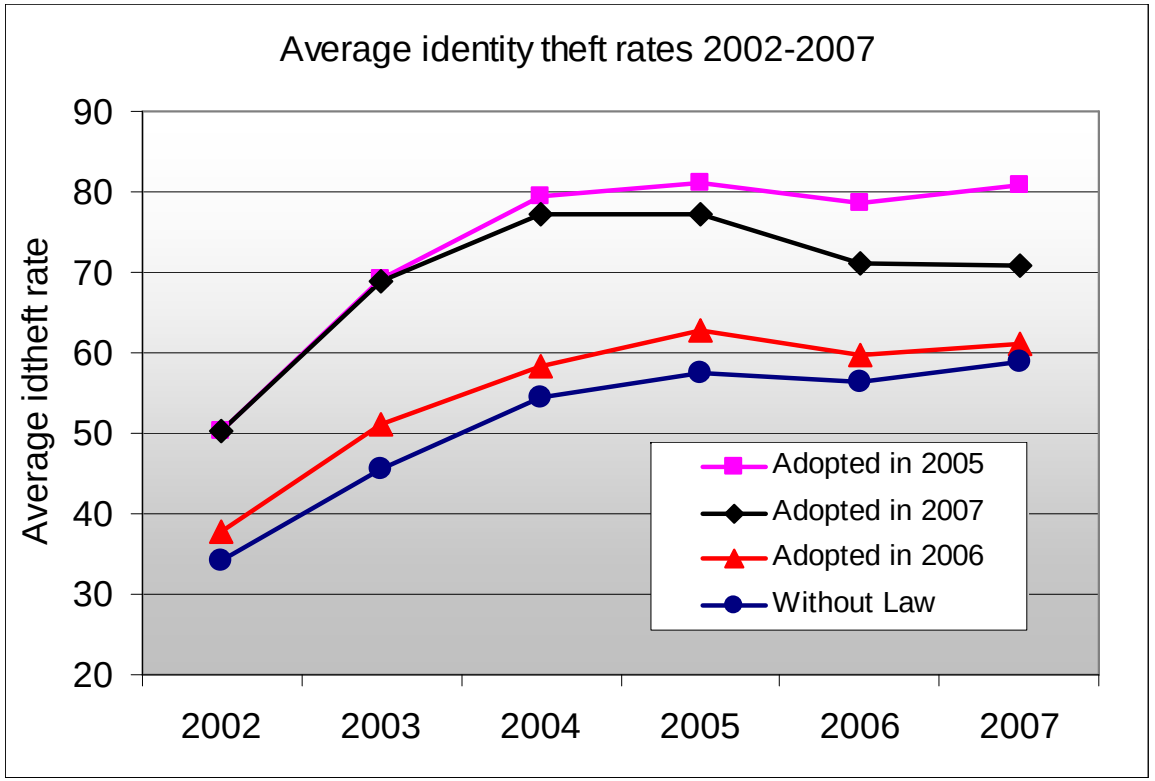
- We aggregated data to semi-annual periods (smallest period over which we expect to see an effect of law). We then compared state-level ID theft data (as well as breach data) to timing of adoption of disclosure law in each state

- 12 periods * 50 states (+ D.C.) = 612 obs
- Romanosky, Telang, and Acquisti (2008)

Both breaches and identity theft crimes are increasing



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: Panel data, Random Effects regressions

- $idtheft_{st} = \beta_0 + \beta_1 hasLaw_{st} + \beta_2 breaches_{st} + \sum \delta_j Economic_{st} + \sum \alpha_k Crime_{st}$

- 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.

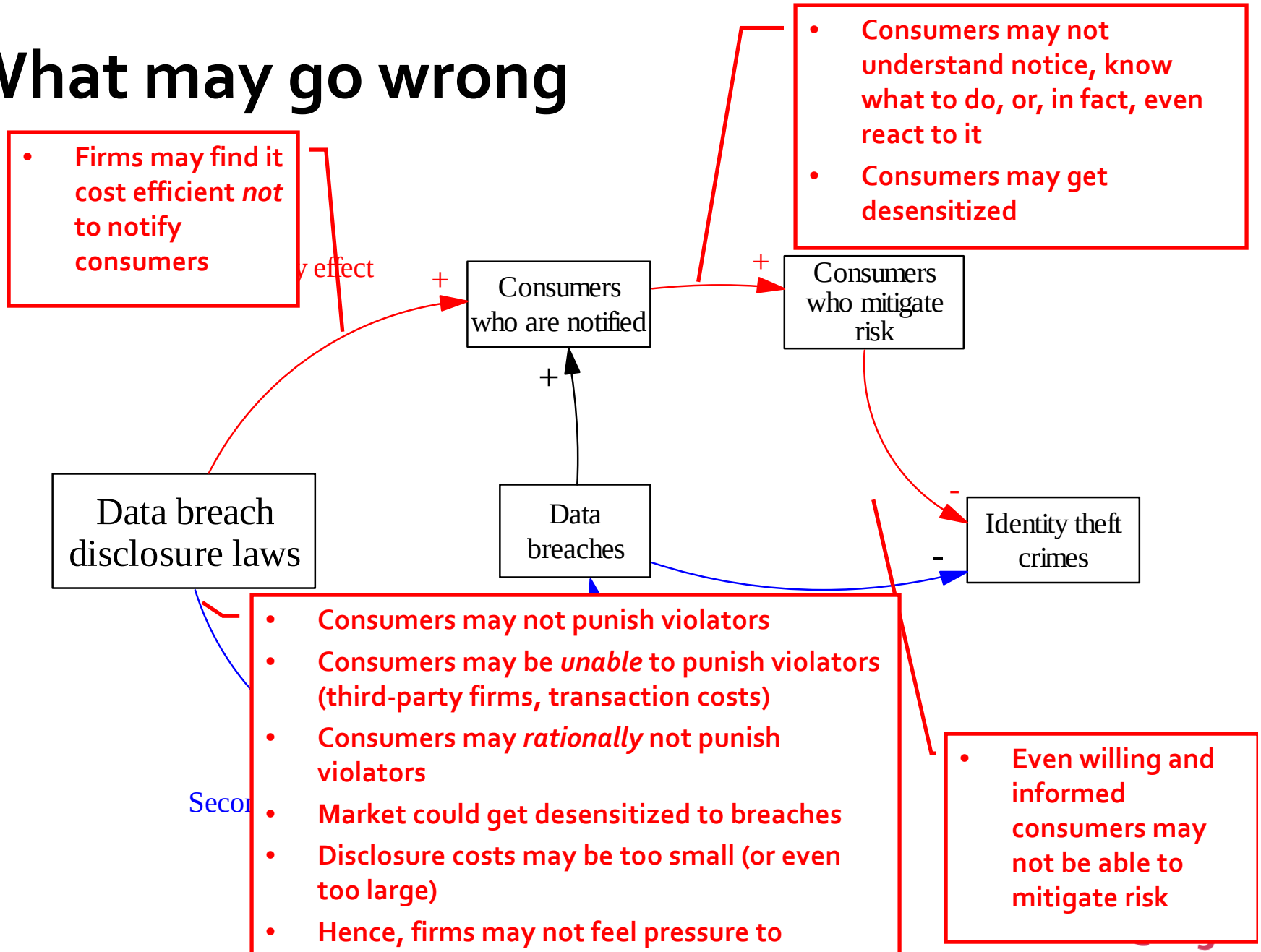
Results

- Statistically significant, but economically marginal effect:

  Adoption of the laws reduce identity theft rate *due to breaches* by about 1.8%

- However, consider other metrics: breach notification laws may have an effect…
  - fostering 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)
- Why not a stronger effect on ID theft?
  - Our regression analysis may be too blunt an instrument
  - The reported data may be a poor source
  - Or…

What may go wrong



Can mandatory data breach disclosure reduce social costs?

- Romanosky and Acquisti 2009 (based on economic theories of regulation and liability - e.g., Shavell 1984; Kolstad, Ulen and Johnson 1990; …)

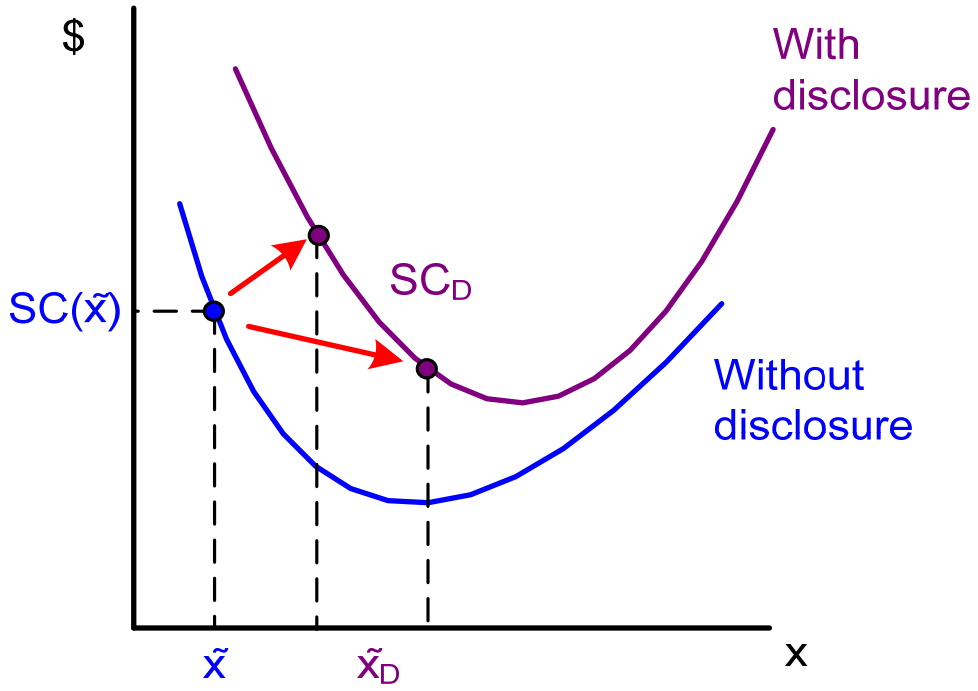
- A firm invests in some level of care (security), x:
  - but this care comes at a cost, c(x),
  - data breach occurs with some probability, p(x), inversely related to x

- Absent disclosure laws:
  - firm incurs cost of investigation
  - while consumer bears all loss

- Under disclosure laws:
  - consumer takes action, reducing their loss
  - **Direct costs**: firm incurs cost of disclosure
  - **Indirect costs**: firm internalizes some consumer loss

Net Social Costs

- Social costs will always be lower when the benefit from lower consumer harm is lower than the direct cost of notification
- When notification costs are higher, total firm costs will be higher, which induces firms to invest more in security -- yet social costs may still be lower



Conclusions

- So far, mixed impact of breach disclosure laws
  - Positive, but limited. More data needed for better analysis
- Possible reasons: Notifications are good, but, alone, may not be enough

➢ *Lessons from transaction costs economics and behavioral economics should be considered*

The behavioral economics of privacy

- Hurdles which hamper (privacy) decision making
  1. Incomplete information
  2. Bounded rationality
  3. Cognitive/behavioral biases

- Behavioral experimental economics has uncovered evidence for several systematic biases in consumers' preferences and behaviors
  - Many of those biases have applications to the privacy arena (as well as information security)

➢ *Hence, the need arises for the application of behavioral economics to the understanding of consumer privacy (and policy making in this area)*

For more info

- Google: economics privacy
- Visit: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm
- Email: acquisti@andrew.cmu.edu