Data Breaches and Identity Theft:

When is Mandatory Disclosure Optimal?

WEIS
06.07.2010

Sasha Romanosky (Heinz)
Richard Sharp (Math. Sci.)
Alessandro Acquisti (Heinz)

Carnegie Mellon
Heinz College

Overview

- Data breaches occur when PII is lost by, or stolen from, retail stores, financial institutions, schools, hospitals or govts.

- In response to growing concerns, 46 US states have adopted data breach disclosure (SBN) laws:
  - notification should empower consumers to reduce expected loss
  - but they can also impose substantial costs on firms

- We analytically examine the conditions under which data breach disclosure laws reduce social cost

Thanks to SBNs, Consumers Can Take Action and Reduce Expected Losses

- Examples of loss includes:
  - financial, medical, tax, social security fraud
  - denial of credit, loans
  - time/effort to correct errors and repair financial credit
  - erroneous criminal investigations

- Examples of consumer care: closing financial accounts, purchasing identity theft insurance, credit monitoring, etc.

SBNs Impose Two Types of Firm Costs

Disclosure Tax: costs the firm would otherwise not incur but-for the disclosure laws ($100k – Millions),

- Retaining legal counsel, litigation holds
- Customer notification, support, PR
- Regulatory fines, fees (FTC, PCI)

Consumer Redress: compensation paid by the firm to the consumer in the event of a breach ($100k – Millions),

- Voluntary idtheft insurance, credit monitoring
- Compensation through court settlements

SBNs Empower Consumers, Impose Costs on Firms

Without SBN Laws	With SBN Laws
1) Consumer bears all loss from data breach	2) Consumer empowered to reduce expected loss
3) Firm only incurs cost of investigating breach	4) Firm incurs additional costs from “disclosure tax” and consumer redress

However: ***Net*** Change of ***Social*** Costs is Unclear

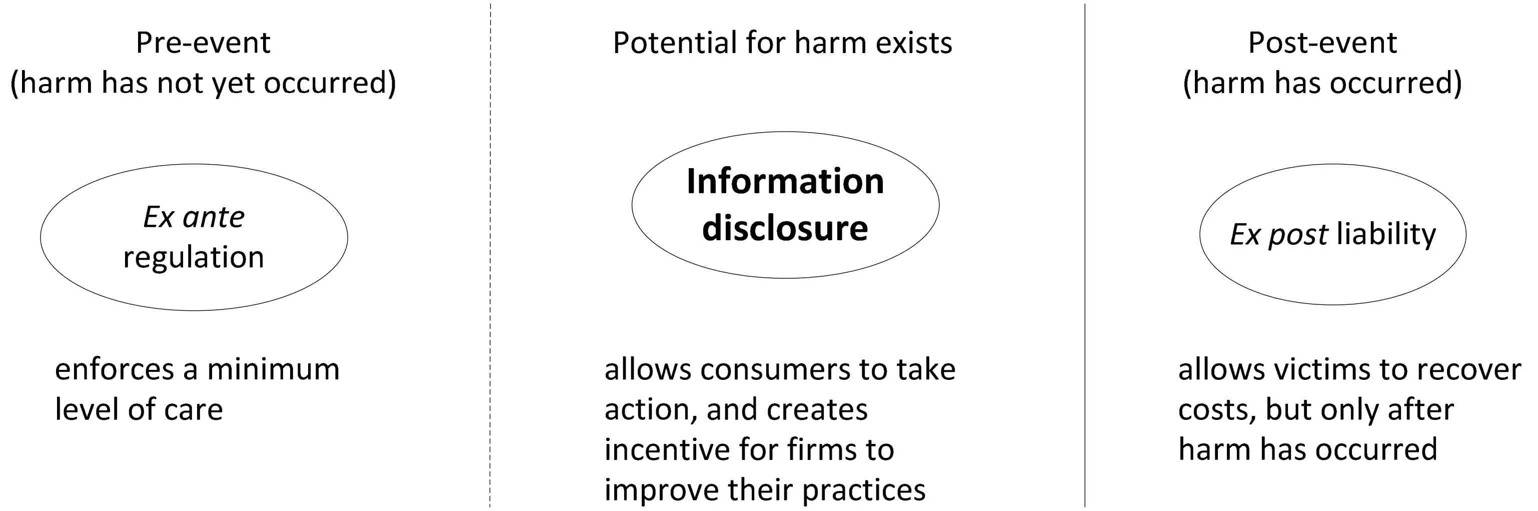
- Notice that Disclosure Tax represents a social loss while Consumer Redress represents simply a transfer of costs between firm and consumer

- Our research questions are:

  1. How is social cost under SBNs affected by…
     - Disclosure Tax
     - Consumer Redress
  2. Under what conditions can SBNs reduce social cost?

Economic Analysis of Tort Law:

Three Alternative Policy Mechanisms



Pre-event
(harm has not yet occurred)

Ex ante regulation

enforces a minimum level of care

Potential for harm exists

Information disclosure

allows consumers to take action, and creates incentive for firms to improve their practices

Post-event
(harm has occurred)

Ex post liability

allows victims to recover costs, but only after harm has occurred

- Commonly used to compare/contrast *ex ante* safety regulation and *ex post* liability. (Social efficiency as complements or substitutes (Shavell, 1984; Kolstad et al., 1990, Schmitz, 2000). Comparing liability rules (Shavell, 2005; Landes and Posner, 1987))

Disclosure Literature is Diverse

- Notification must be actionable (Viscusi, 1992)
- Disclosure works when market inefficiencies are result of inadequate or erroneous information (not apathy) (Beales et al, 1981)
- Disclosure reduces incentive for firms to reveal product risk (Shavell & Polinsky, 2006)
- Bilateral-care accidents requires additional motivation to avoid moral hazard (Polinsky, 1980)
- Consumer outcomes can improve (restaurant hygiene, Jin & Leslie, 2003; in salad dressing nutrition labels, Mathios, 2000),
- But most disclosure policies appear not to work (Schneider & Ben-Shahar, 2010)

Our Methodology:
Economic Analysis of Tort (Accident) Law

Example: Consider two cars on a roadway

- Each driver engages in some level of care (prevention) and assumes some probability of an accident
    - costs to the drivers include 1) the cost of care and 2) the expected cost of an accident
    - naturally, each driver will engage in a level of care that minimizes their private costs
- Policy objective: devise rules that induce all parties to take the optimal care, thereby minimizing social costs

Objective Functions Without Disclosure

Firm $\min_{x} F(x) = c(x) + p(x)i$

Consumer $C(x) = p(x)h$

Social $S(x) = c(x) + p(x)[i + h]$

x: level of firm care (security measures), $x \geq 0$

c(x): cost of care, $c'(x) > 0$, $c''(x) > 0$, $c(0) = 0$

p(x): prob of breach, $p'(x) < 0$, $p''(x) > 0$, $p(0) = 1$, $\lim_{x \to \infty} p(x) = 0$

i: firm costs (cost of breach investigation, repairing IT systems, etc), $i > 0$

h: consumer loss (identity theft), $h > 0$

Objective Functions With Disclosure

Firm $$\min_{x} F_D(x) = c(x) + p(x)[i + \underline{d} + \underline{\lambda h(y)}]$$

Consumer $$\min_{y} C_D = p(x)[1 - \lambda]\underline{h(y)}$$

Social $$S_D(x) = c(x) + p(x)[i + d + h(y)]$$

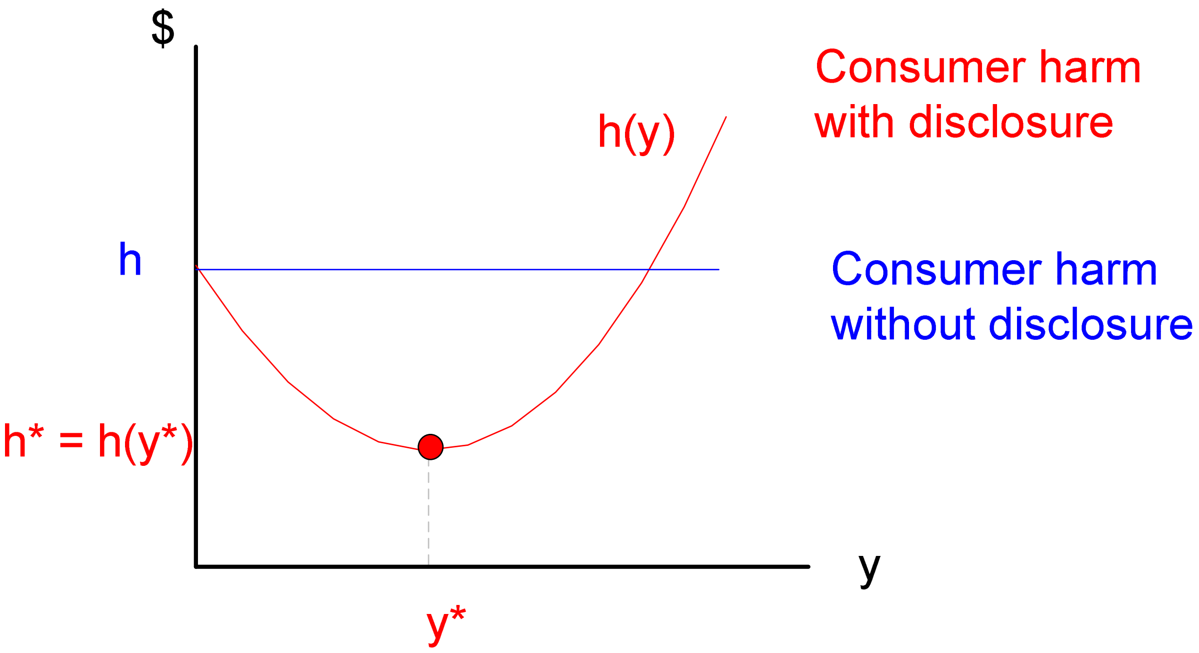
λ: portion of consumer harm borne by the firm, $0 \leq \lambda \leq 1$

d: costs of disclosure (disclosure “tax”), $d > 0$

y: consumer care (prevention), $y \geq 0$

$h(y)$: new consumer harm under disclosure, $h^* < h$, $h'' > 0$

Consumer Harm



- y: level of consumer care
- Consumer harm without SBN is just h
- h(y): is composite function, representing cost and benefit of care

Immediate findings

- *P1a: Under a disclosure regime, a (rational) consumer will take more care, but will incur lower costs*
- *P1b: A firm will under-invest in security either with or without a disclosure regime*
- *P1c: A firm will invest more in security when forced to disclose a data breach*
- *P1d: Firm costs will be higher under disclosure*

Social Costs Must Be Evaluated at the Firm’s Optimal Level of Care

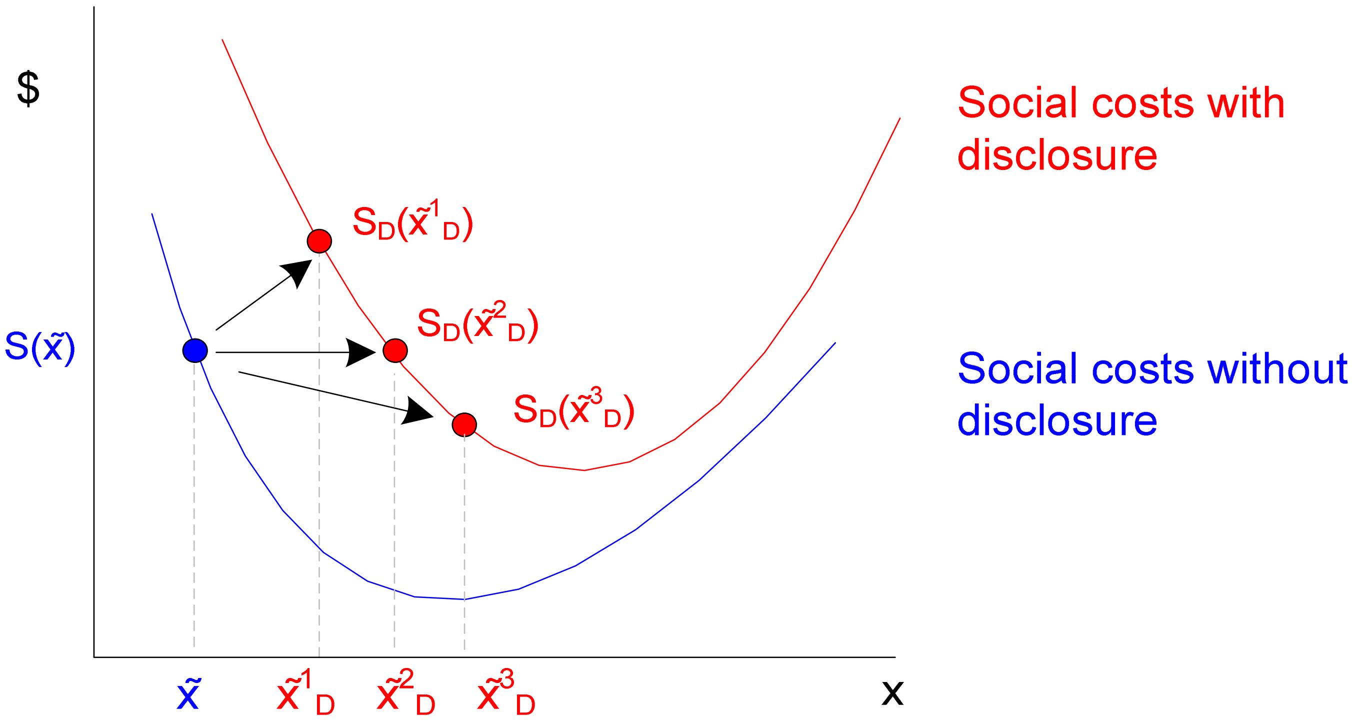
Consider:

- Policy Maker implements a breach disclosure policy
- Firm reacts by investing in its cost-minimizing level of care
- Consumer reacts by taking action to minimize their loss

We “solve” this sequential game using backward induction:

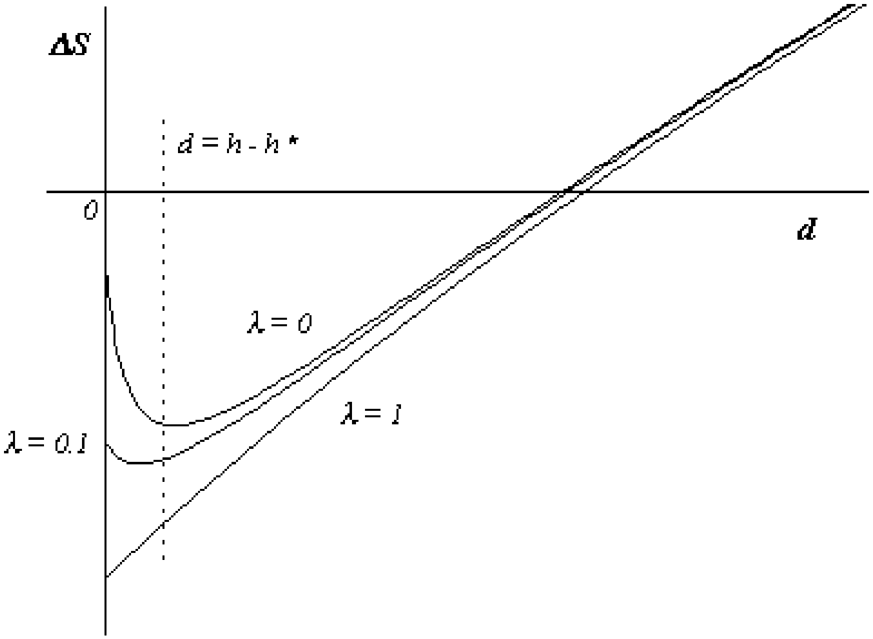
- Consumer acts optimally, taking action, $h^* < h$
- Given h^*, firm invests in care to minimize its costs
- Now, evaluate and compare social costs at firm’s cost-minimizing levels of care

Social Costs Must Be Evaluated at the Firm's Optimal Level of Care



We are, therefore, interested in the *change* in social costs: $\Delta S = S_D(\tilde{x}_D) - S(\tilde{x})$

When is SBN Optimal?



- *P2: First-best social cost when d = 0, λ = 1 (trivial)*
- *P3: When the firm bears a small portion of consumer loss, some disclosure tax is necessary to minimize social costs*

Comparing Disclosure Tax With Change in Consumer Harm

$$\Delta S = c(x) + p(x)\left[i + d + h^*\right] - \left(c(x) + p(x)\left[i + h\right]\right)$$

- One relevant comparison is $d + h^* <> h$
- Which we can rewrite as $d <> h - h^*$
- Or, more intuitively:

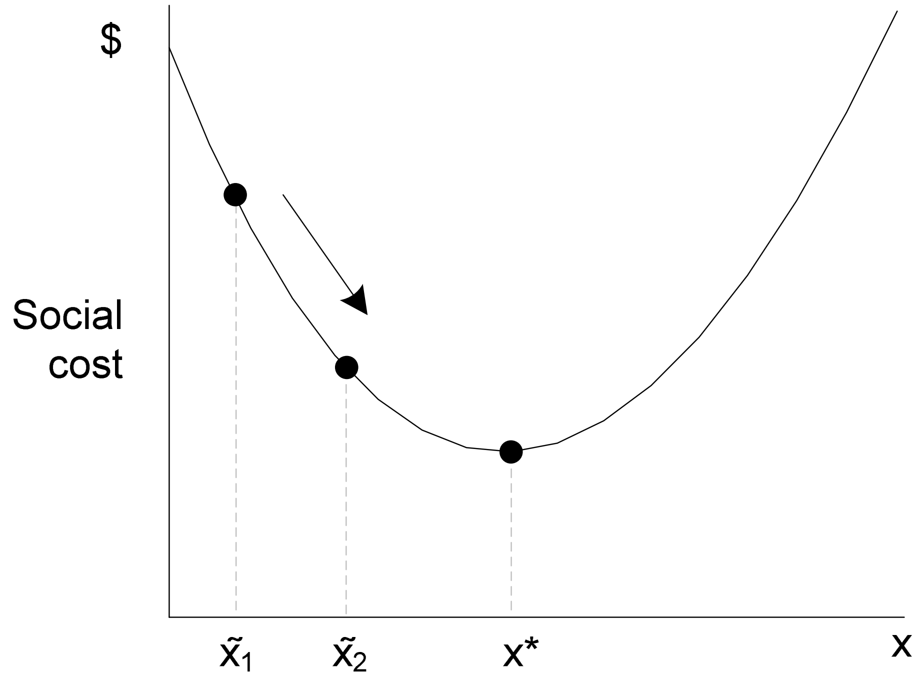
  disclosure tax <> change in consumer loss

- *P4: Social cost is <u>always</u> lower when $d \leq h - h^*$*
- *P5: Even when $d > h - h^*$, social cost can still be lower*

$\Delta S = SC_D(\tilde{x}_D) - SC(\tilde{x})$

Understanding change in Social Cost:

movement along social cost curve

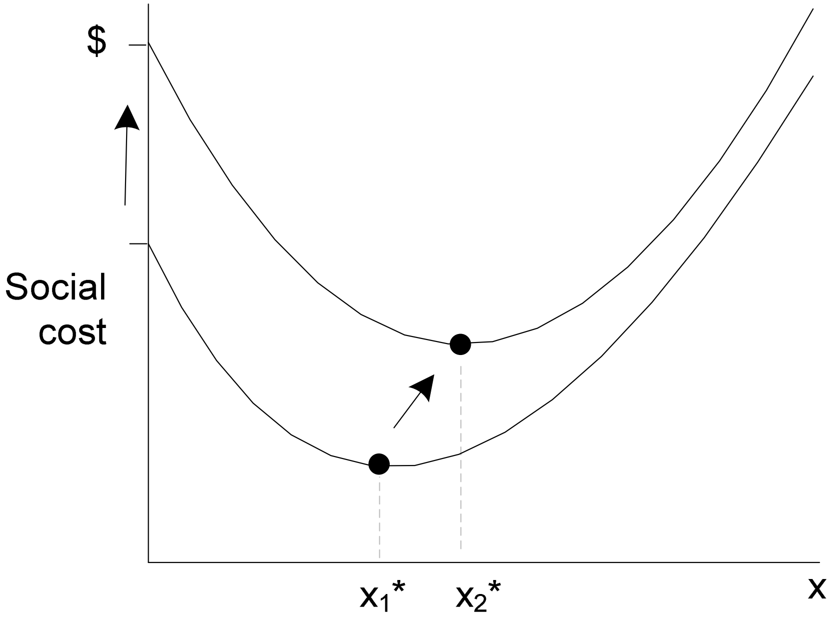


As firm bears more consumer loss, its level of care approaches socially optimal level of care (i.e., “sliding” down social cost curve)

$\Delta S = SC_D(\tilde{x}_D) - SC(\tilde{x})$

Understanding change in Social Cost:

movement of social cost curve



Increase in consumer costs, cost of investigation, disclosure tax each result in shifting the social cost curve up, to the right

e.g. increased cost of disclosure strictly raises social cost

Policy Implication for λ

- λ represents two components: voluntary redress, and some amount of forced compensation due to legal liability, or regulatory redress
- “The marketplace has already assigned responsibilities and liabilities that provide for the protection of consumers” (Schwarzenegger, 2007)
- It seems, however, that tort law is ill-equipped to affect λ too much
- This implies that --beyond token credit monitoring -- regulatory redress may be the only practical means to force firms to internalize consumer loss and reduce social cost

Summary

- From empirical validation, disclosure tax appears to be much larger than reduction in consumer harm (d >> Δh ≈ $200 > $1.4)

- However, the firm appears to already bear a large portion of consumer harm (λ = 0.4 - 0.7)

Since majority of disclosure tax is within control of the firm, they are in the best position to reduce it -- social incentives align with (private) firm incentives

- This suggests less of a role for mandated standards (*ex ante* regulation) and more of a role for light-handed policies (such as disclosure)

Thanks to CyLab!

sromanos@cmu.edu