



Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?

*Financial Information
Systems and Cybersecurity:
A Public Policy Perspective*

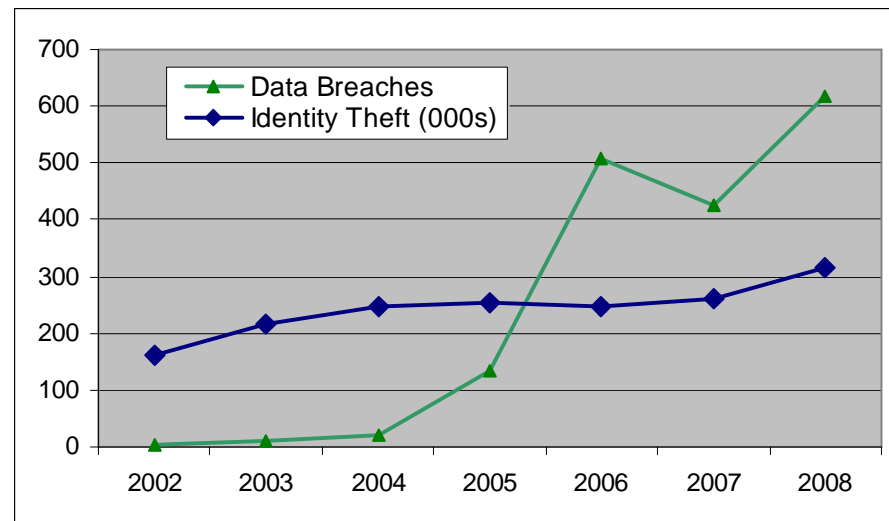


Sasha Romanosky,
Alessandro Acquisti
October 29, 2009

Problem: Data breaches and Identity theft

- A data breach occurs when personally identifiable consumer information is lost / stolen. It happens to retail stores, financial institutions, schools, hospitals and govt.
- Information used to commit identity theft: medical, tax, financial, social security fraud.

- Both breaches and idtheft are increasing



Solution: Data Breach Disclosure Laws?

Many countries have responded by requiring firms disclose the loss or theft of personal information

- Sunlight Effect: “drives performance through transparency and oversight” (Mulligan, 2007)
- Right-to-Know: consumers can take action to lower risk

BUT:

- Firms may already bear most of the cost of breaches (Lenard and Rubin, 2005)
- May inflict unnecessary costs if risk is low (Majoras, 2007)
- Laws appear to reduce idtheft by only about 2% (Romanosky, Acquisti, Telang, 2008)

Net Social Cost?

Research Question: Can mandatory data breach disclosure reduce social costs? **Why social cost?**

We find that:

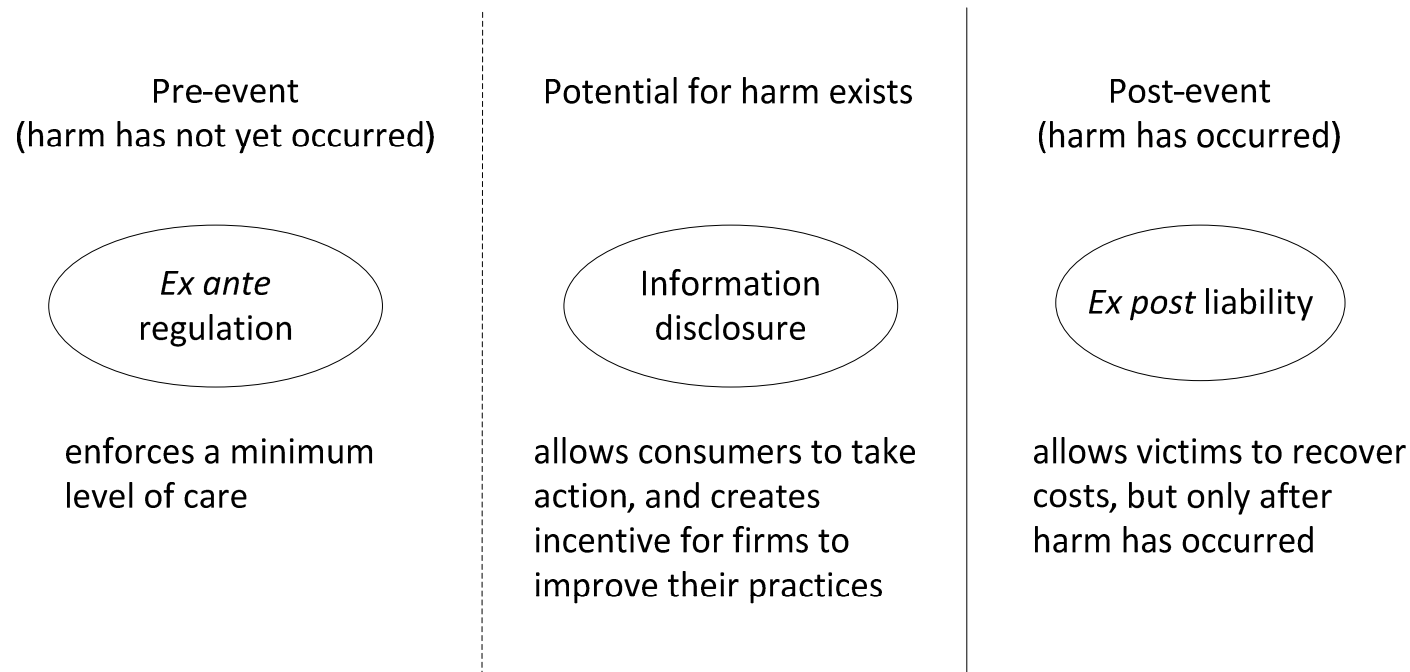
- Social costs will always be lower when the *costs* (of disclosure) are less than the *benefit* (of reduced consumer harm)

But that even when disclosure costs are greater:

- firm costs will be higher,
- which induces them to invest more in security,
- yet social costs may still be lower

A Familiar Externality Problem

- When firms don't bear the full cost of their actions, they impose costs (externality) on others.
- Common methods to reduce these costs:



Ex Ante Safety Regulation

Preferred when:

- harm may be catastrophic, distributed across many victims
- long delay between event and resulting loss
- harm can be demonstrated statistically but not individually
- Regulations mandate inputs to harm, not outputs. i.e. it regulates technologies, not actual harm; drive fine avoidance
- But easier to monitor compliance *ex ante*, than harm *ex post*

e.g. PCI, SOX, HIPAA, new state encryption laws, certifications, licenses to operate

Ex Post Liability

Preferred when:

- standard of due care exists, and is clear to the firm
- courts can properly measure firm's level of care
- probability of harm is low (admin costs)

- Liability (tort law) considered socially efficient (Posner, Shavell) and "self-corrective" (Bagby, 2007)
- But where is the duty of care with PII?
- Still need to overcome causality, economic loss doctrine

Information Disclosure

Preferred when:

- consumers heed warning
- information is actionable
- firms are driven to improve (competition, angry consumers)

- But consumers have enough to worry about and suffer from many behavioral limitations (Romanosky, Acquisti, 2009); tx costs, rational ignorance, bounded rationality
- Are consumer reactions incentive-compatible?

Related Research on Regulation / Liability

- Under which conditions is one policy more efficient than the other? (Shavell, 1984; Kolstad et al., 1990, Schmitz, 2000)
- Which liability rules are most efficient? (Shavell, 2005; Landes and Posner, 1987)
- These approaches leverage the economic analysis of accident (tort) law

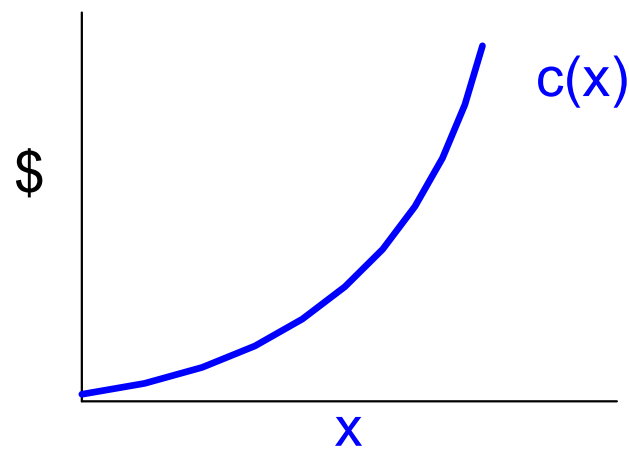
Economic Analysis of Tort Law

- Typically considers 2 actors, injurer and victim, and seeks to understand social costs under different liability conditions
- E.g. auto accidents.
- Each party wants to minimize their own (private) costs
- But the social planner wants to minimize everyone's costs by optimizing level of care.

Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x)$	
Consumer cost		
Social cost		

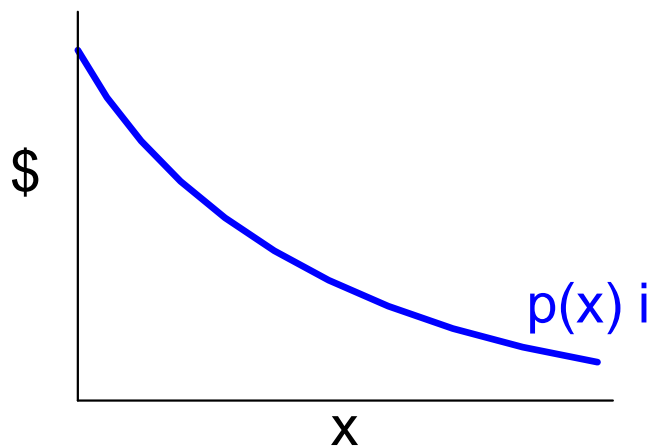
Firm invests in care, but that care has a cost



Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	
Consumer cost		
Social cost		

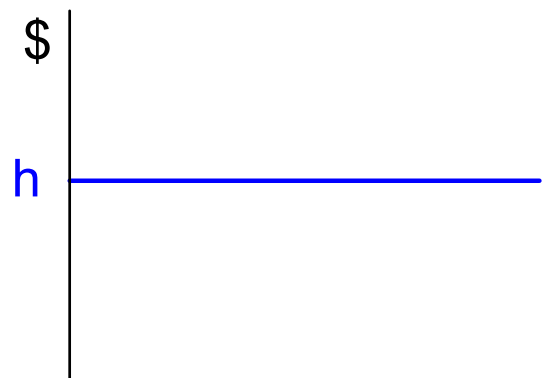
Accident occurs with some probability, $p(x)$



Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	
Consumer cost	$p(x) h$	
Social cost		

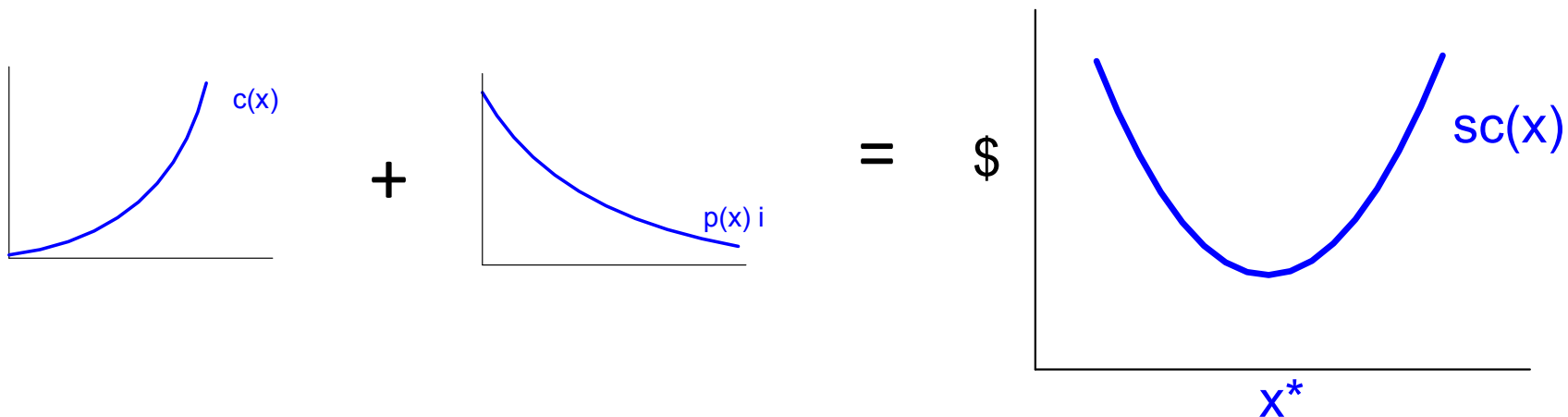
Consumers suffer all the harm



Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	
Consumer cost	$p(x) h$	
Social cost	$c(x) + p(x)[i + h]$	

Social cost is just the sum of firm and consumer costs



Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	$c(x) + p(x)[i + d +$
Consumer cost	$p(x) h$	
Social cost	$c(x) + p(x)[i + h]$	

Under Disclosure, firms incur an additional cost, d

- agency fines/sanctions (\$100k - \$10s of millions)
- legal fees (\$100k- millions)
- PR campaigns (\$100k- millions)
- “reputation” (?)
- forensic and “litigation hold” costs (??)

Cost Functions

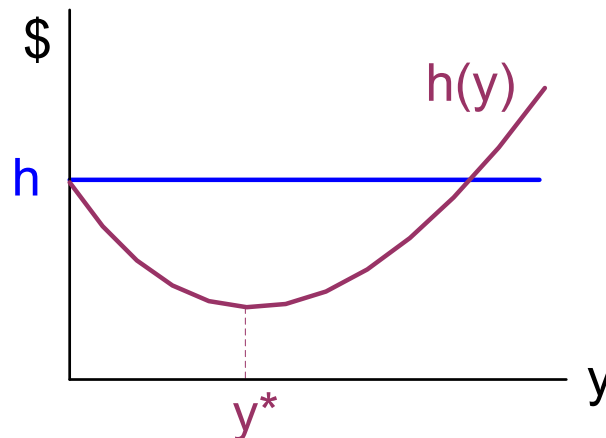
	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	$c(x) + p(x)[i + d + \lambda h(y)]$
Consumer cost	$p(x) h$	
Social cost	$c(x) + p(x)[i + h]$	

Plus some portion of consumer harm, $\lambda h(y)$, $\lambda [0,1]$

Cost Functions

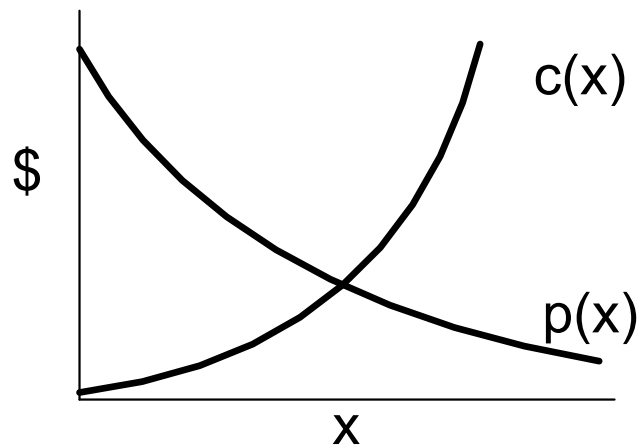
	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	$c(x) + p(x) [i + d + \lambda h(y)]$
Consumer cost	$p(x) h$	$p(x) [1-\lambda] h(y)$
Social cost	$c(x) + p(x)[i + h]$	

Consumer harm now a function of consumer care, $h(y)$

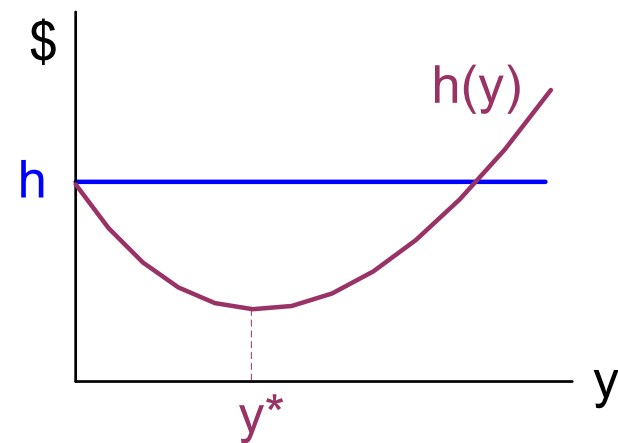


Cost Functions

	No Disclosure	Mandatory Disclosure
Firm cost	$c(x) + p(x) i$	$c(x) + p(x) [i + d + \lambda h(y)]$
Consumer cost	$p(x) h$	$p(x) [1-\lambda] h(y)$
Social cost	$c(x) + p(x) [i + h]$	$c(x) + p(x) [i + d + h(y)]$



Firm care

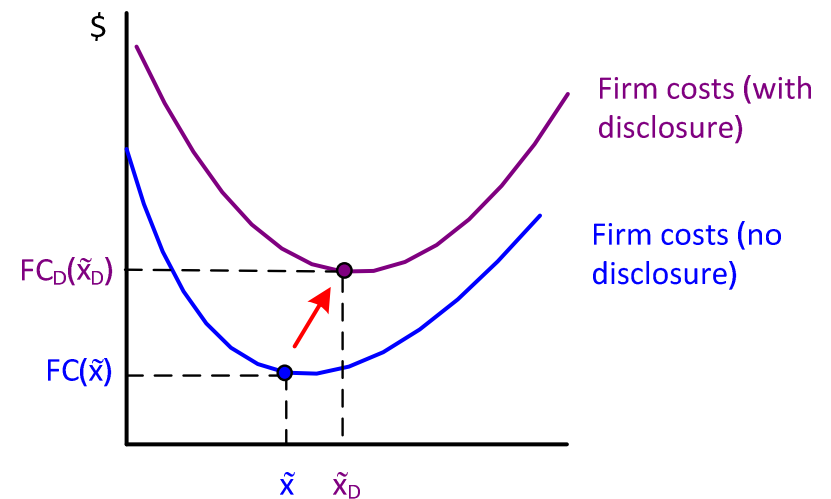
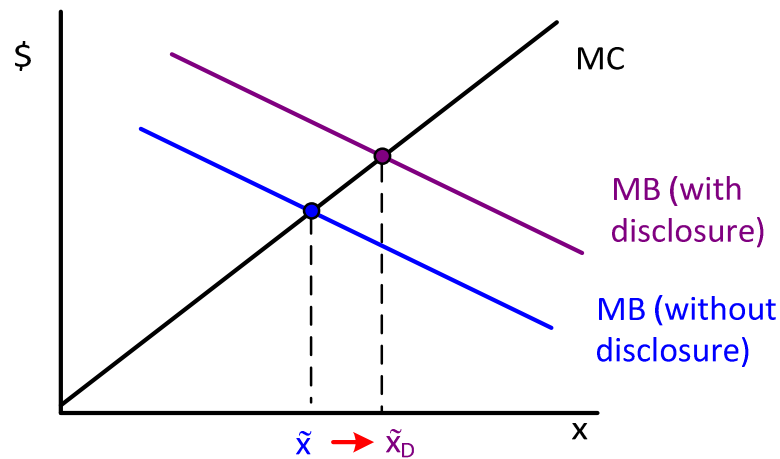


Consumer loss

Initial Propositions

P1: Firm takes more care when forced to disclose, $\tilde{x}_D > \tilde{x}$

P2: Firm costs are greater under disclosure, $FC(\tilde{x}_D) > FC(\tilde{x})$



Social costs (when firm chooses their care)

Consider:

- Social planner implements a disclosure policy
- Firm reacts by investing in *their* cost-minimizing level of care
- Consumer reacts by taking action to reduce *their* loss

We “solve” this sequential game using backward induction:

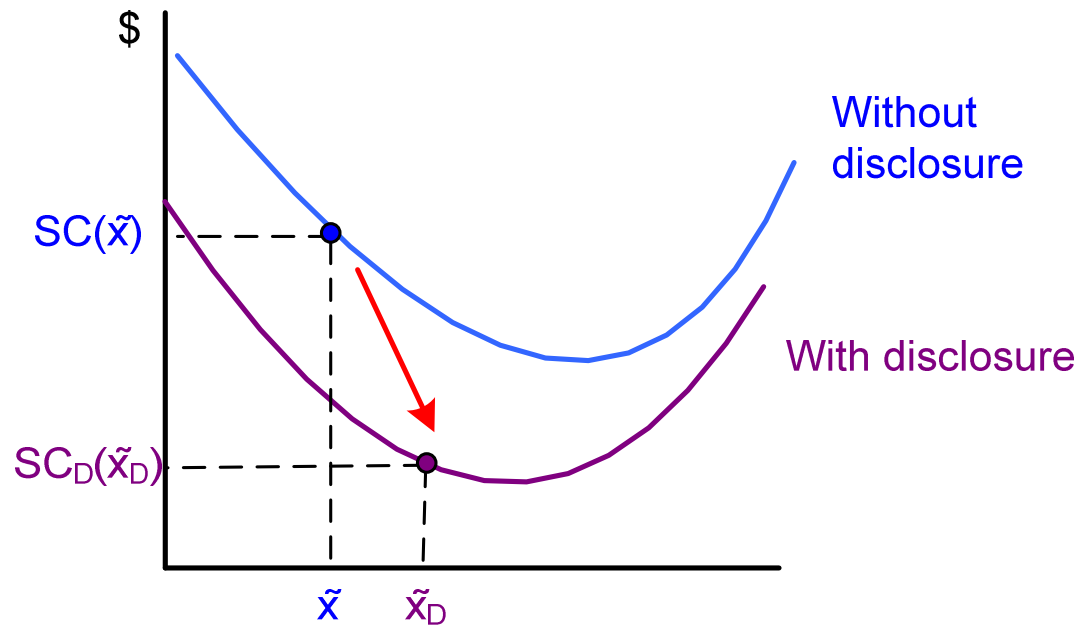
- Consumer acts optimally, taking action, y^*
- Given $h(y^*)$, firm invests in care to minimize its costs, \tilde{x}_D
- Now, evaluate social costs at firm’s cost-min care, $SC_D(\tilde{x}_D)$

Social Costs

	No disclosure	Mandatory Disclosure
Social cost	$c(x) + p(x) [i + h]$	$c(x) + p(x) [i + d + h(y^*)]$

- Are social costs with mandatory disclosure less than social costs without disclosure: $SC_D(\tilde{x}_D) < SC(\tilde{x})$?
- Relevant comparison is: $d + h(y^*) <> h$
- Can rewrite as : $d <> h - h(y^*)$
- But this is just: cost of disclosure $<>$ benefit of reduced consumer loss

Social Costs: $d < h - h(y^*)$



- *P3: When the cost of notification is less than reduction in consumer loss, disclosure is always preferred*
- But this is the trivial case

Social costs, when $d > h - h(y^*)$

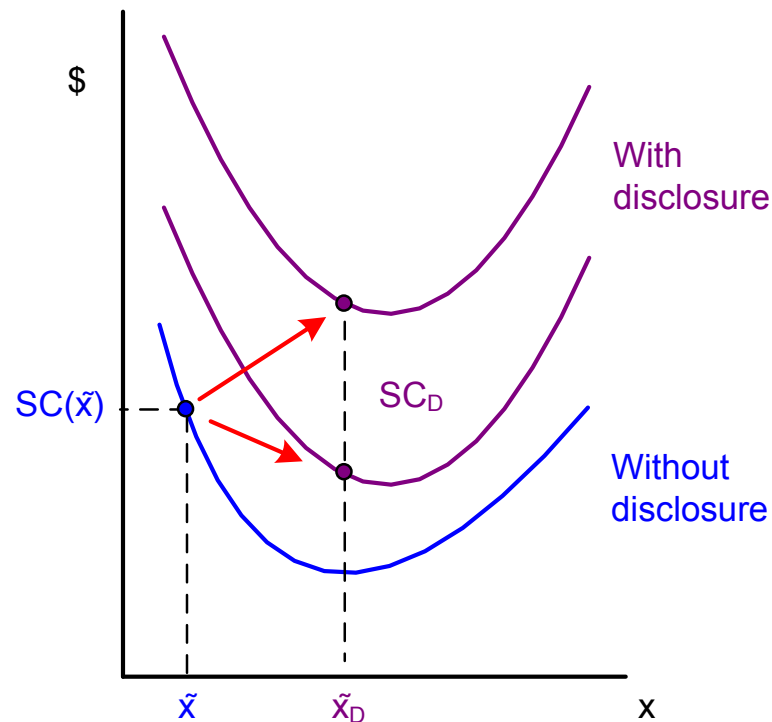
But is it always true that disclosure is bad when cost of disclosure is greater than the benefits?

We have 2 constraints:

- (C1): vertical position of social cost curve and
- (C2): relative increase in firm's care

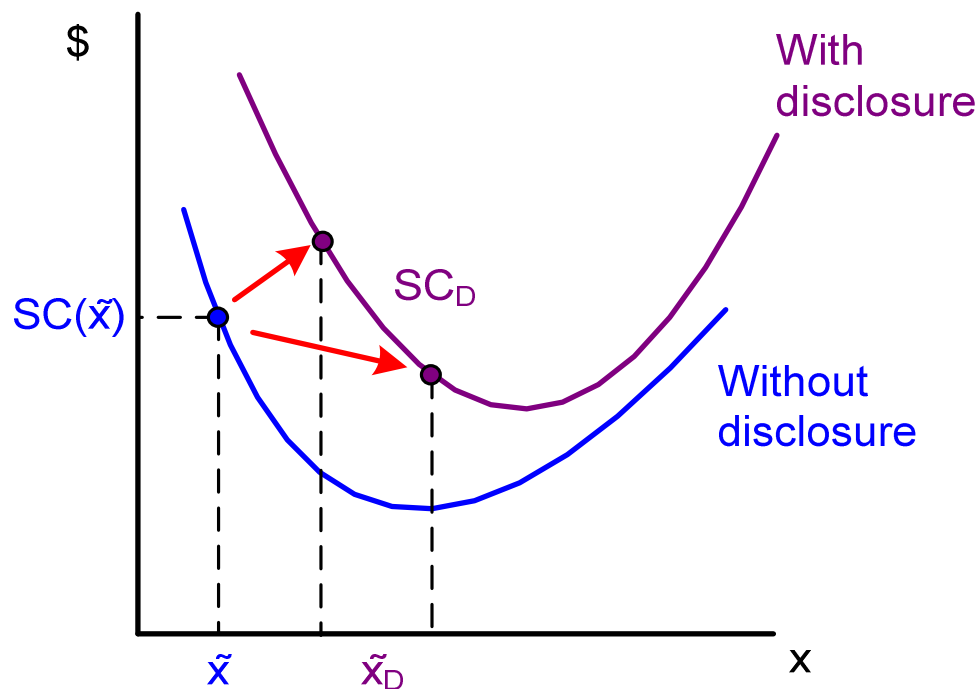
C1: Vertical position

- Social cost curve with disclosure needs to be “low enough”
- If d is driven too high, social costs would never be lower
- Places an upper bound on d



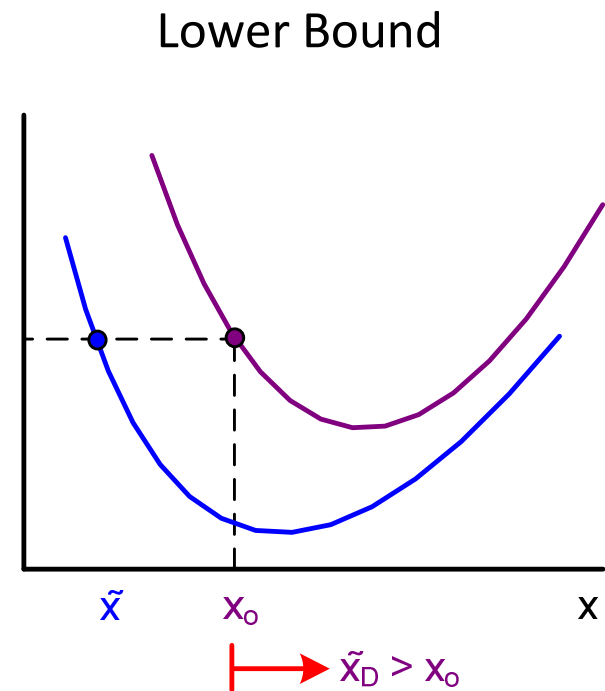
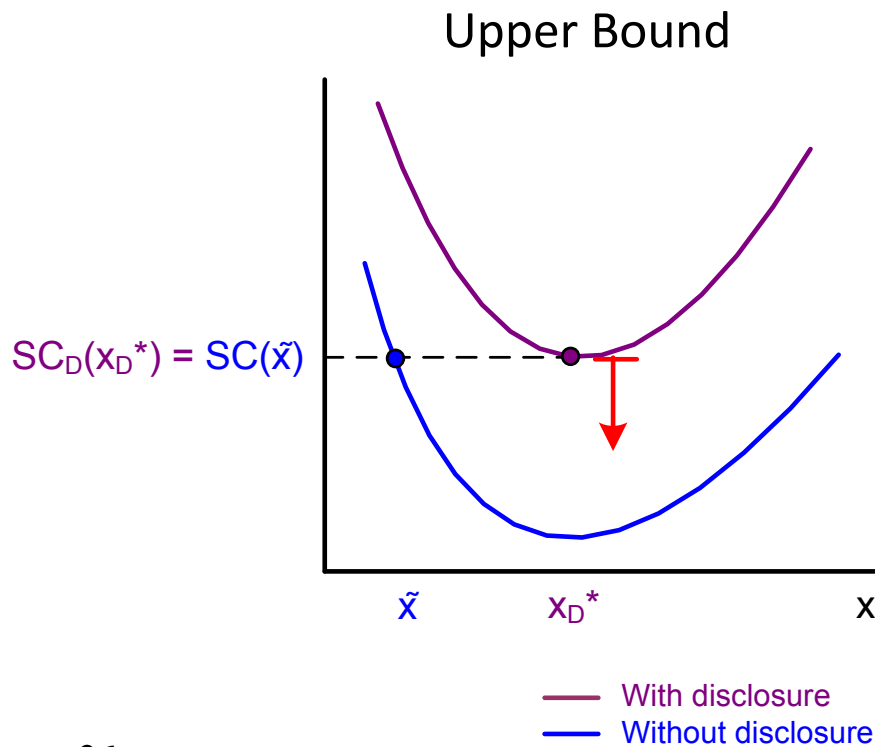
C2: Relative increase in care

- Increase in care needs to be large enough
- If d is too low, social costs will never be lower
- Places a lower bound on d



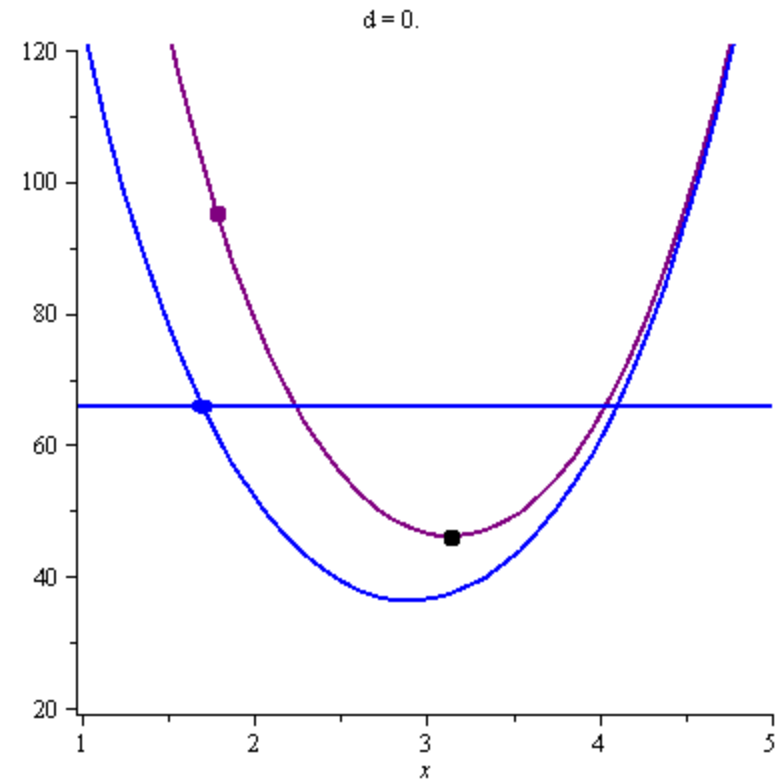
Bounds for d

- The upper bound determined by $SC_D(x^*) < SC(\tilde{x})$
- The lower bound determined by $\tilde{x}_D > x_0$
where $SC_D(x_0) = SC(\tilde{x})$



Visualizing Social Costs

- Social costs can still be lower under disclosure even when cost > benefit
- Social cost without disclosure
- Social cost with disclosure
- Optimal SC with disclosure



Visualizing Social Costs

See the animation at

<http://www.romanosky.net/pres/socialcost.gif>

Conclusion

- We sought to determine whether social costs could drop under a mandatory data breach disclosure policy

We found that:

- Social costs will always be lower when the benefit from lower consumer harm is less than the cost of notification: $d < h - h(y^*)$

But that even when disclosure costs are greater:

- Total firm costs will be higher,
- which induces firms to invest more in security,
- yet social costs may still be lower

Future Work

- Who is low cost avoider, firm or consumer?
- Moral hazard with consumer loss
- Level of Care vs Level of Activity



sromanos@cmu.edu