

# Racing to the Top: Creating a Flexible Duty of Care to Secure Personal Information

Deirdre K. Mulligan

Assistant Professor

School of Information, UC Berkeley

Faculty Director

Berkeley Center for Law and Technology

If you build it they will come...  
or maybe not...

Security in the market place is “**remarkably below what “known best Practices”** could provide.”

The existence of technology solutions **on their own** does not improve security or privacy.

# Problem

- Security of personal information
  - Inadequate incentives to protect
    - Non-rivalrous
    - Externalized harm
    - Unknown harm from breach
    - Difficult to establish causality
  - Requires dynamic evolutionary response
    - Traditional legal responses ill-suited
      - Standards
      - Common law
      - Market

**Q: What public policies create incentives for firms to effectively secure personal information?**

# Metaphor

Pollution is to Industrial society  
as

Privacy Breaches are to Information  
society

# Environmental Law:

## Information Disclosure

### Emergency Planning and Community Right-to-Know Act (EPCRA)

- Huge drops in releases (EPA est. 40% likely less)
- Operational changes within companies

Remarkable changes from lighter, less costly  
approach

# How it works

- Catalyst for market activity
- Catalyst for political activity
- Source of power/pressure internal actors

**Breach as toxic release?**

# Effects of Security Breach Laws

- What information are they producing?
- Are they catalyzing
  - market activity?
  - political activity?
  - organizational behavior?
- What limits their effectiveness?
  - Informational limits
  - Subject matter limits

# New Information and Harms

- Consumers and public aware of breaches
- Fuller picture of problem
  - Absent legal requirement only 20% of firms will report serious breaches (FBI/CSI 2005)
- Particular vulnerabilities identified
  - Laptops, third-party vendors, tapes and other data in transit
- Creation of new harm
  - Harm to business reputation and brand flowing from report of breach
- Price tag on problem
  - Average cost \$182 per person (Ponemon 2006)

# Market Activity

## Some

- Individuals and self protection
  - 20% claim to have terminated relationship
  - 0-7% actual churn rate
- Stock market fluctuations

## Limitations

- Notices uninformative
- Unable to compare risks
- Limited opportunities for exit (Relationship-less)

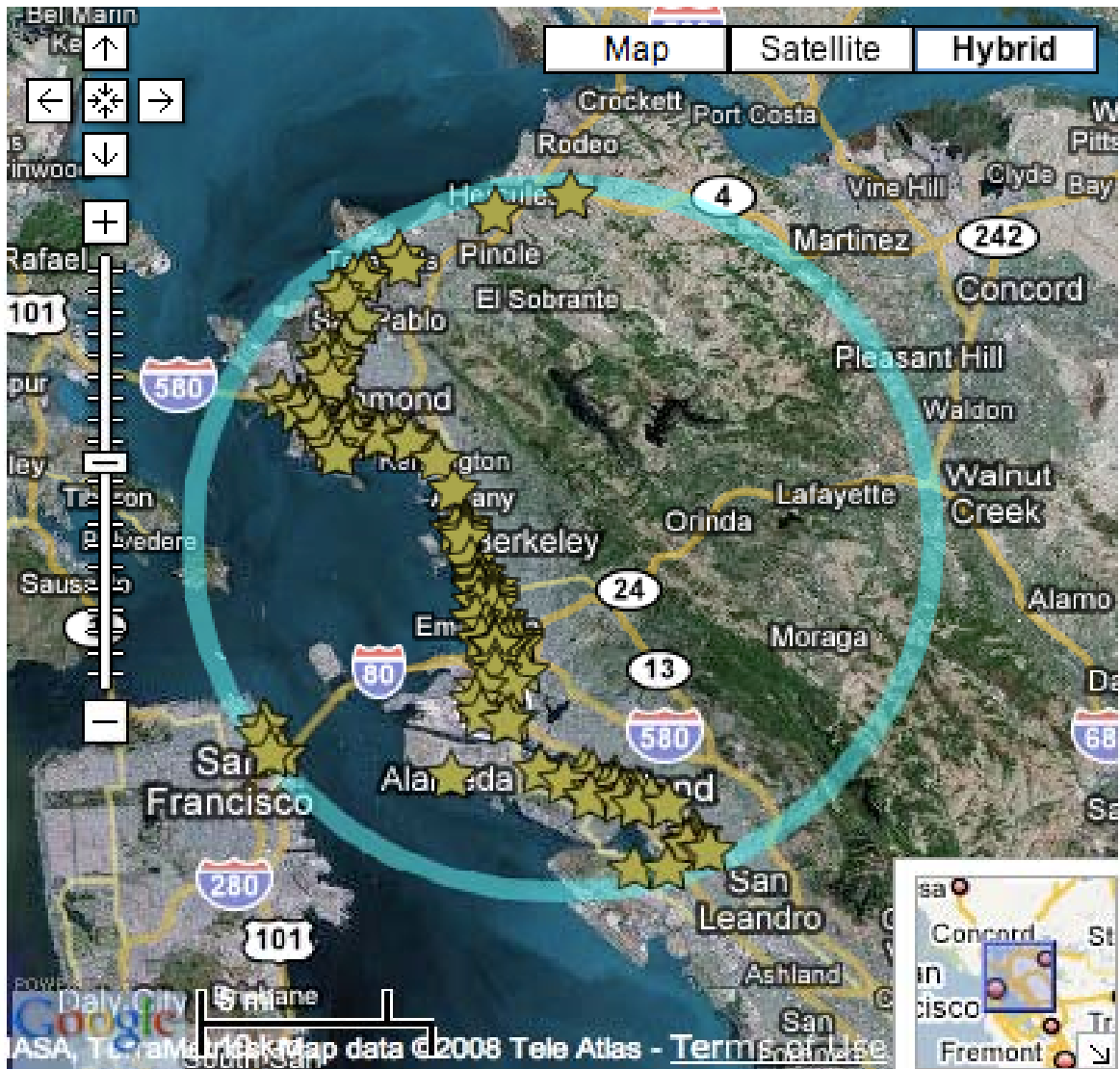
# Political Activity

Some

- Copycat laws
- Relation to other regulatory efforts
- Limited use by ngos

Limitations

- Location-less
- Mile wide, inch deep
- Technocratic
- Weak and fragmented legal framework



Select a desired program below or pick NO SELECTION for all programs. Then choose a search tab, enter your selection, and click **Submit**.

Click the **Results** tab to view found sites. Click the symbol to zoom to the site. Or, click the symbols on the map to get a popup with site details.

Use the slider and the arrow buttons to zoom and move the map. You also can move the map with the hand cursor when it is visible over the map.

Program:

Enter a zip code and distance. Click Submit.

Zip Code:

Lat/Long:  /

Distance (miles):

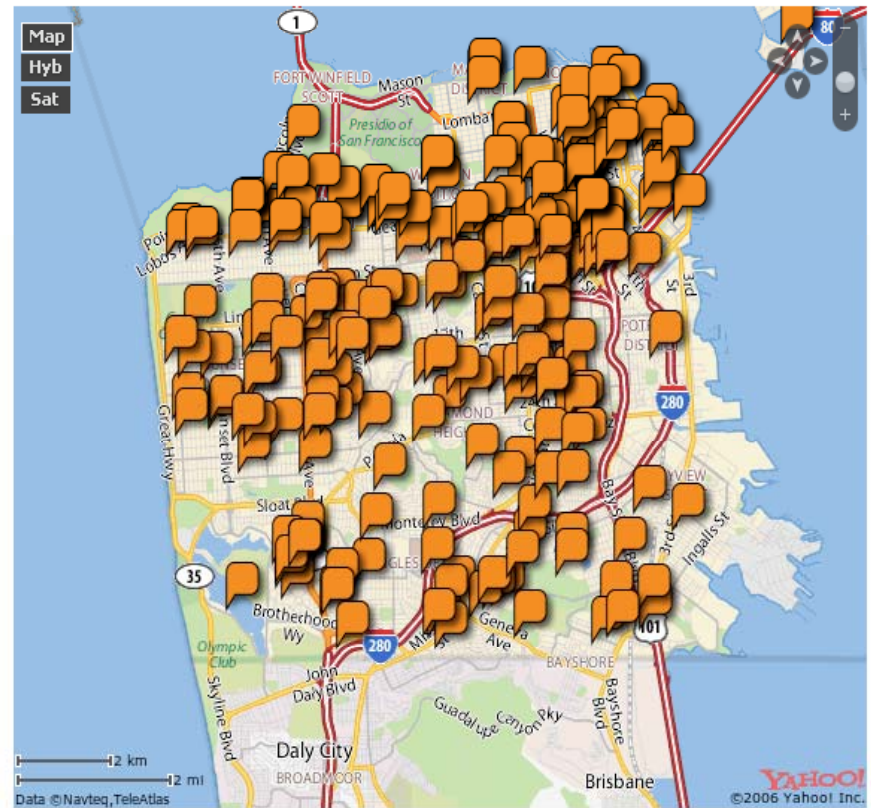
115 sites found!

EPA Sites of Concern
  State Sites of Concern

**You are searching through 73,402 sites.**  
**CA Geotracker search is only for the San Diego area.**

# Location-less

Astroglide Database Maps Mashup



Astroglide mashup: Christopher Soghoian & Sid Stamm, PhD candidates, Indiana University

# Organizational Behavior

“You manage what you measure”

- security and privacy bound to brand
- Heightened role of CPO
- Bridge between CPO/CSO/CISO
- drive information exchange among security professionals
- Altered paradigm—compliance to risk management

# Conclusions

Security Breach Laws are affecting markets, political activity and organizational behavior

Push towards risk management is likely to drive ongoing improvements

## **Some limitations**

- Information and reporting requirements of current laws
- inherent in characteristics of breaches

# Reforms and Future Research

- Standardized, electronic, centralized reporting
- Publicly available database
- Increase reporting requirements for other sorts of breaches
- Dual standard of notification?
- User based analysis of information
  - shifts in content, format and **timing**
- Metrics to determine risk, not just loss