

Breach Disclosure Laws Contribution to Data Protection and Security

Deirdre K. Mulligan
Assistant Professor
School of Information
UC Berkeley

American Association for the Advancement of Science, Annual
Meeting February 2010

Novel Developments in US Privacy Law

- Traditional story
 - US sectoral, piecemeal, weak
 - EU omnibus, comprehensive, DPAs, robust
- Last 15 years
 - FTC as privacy norm interpreter and enforcer
 - State Security Breach Notification Laws
- Any benefits from recent US developments?
 - Yes, definitional and management changes that may enhance corporate attention to privacy
 - This talk focuses on contributions of SBN laws specifically

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

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?

Intervention:

Security Breach Laws

- Notice to individuals whose...
“unencrypted personal information
(first name or initial and last name + SSN;
DL; CIGN; Account number, credit or debit
card number + PW)
was, or is reasonably believed to have been,
acquired by an unauthorized person”

Current Research:

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)

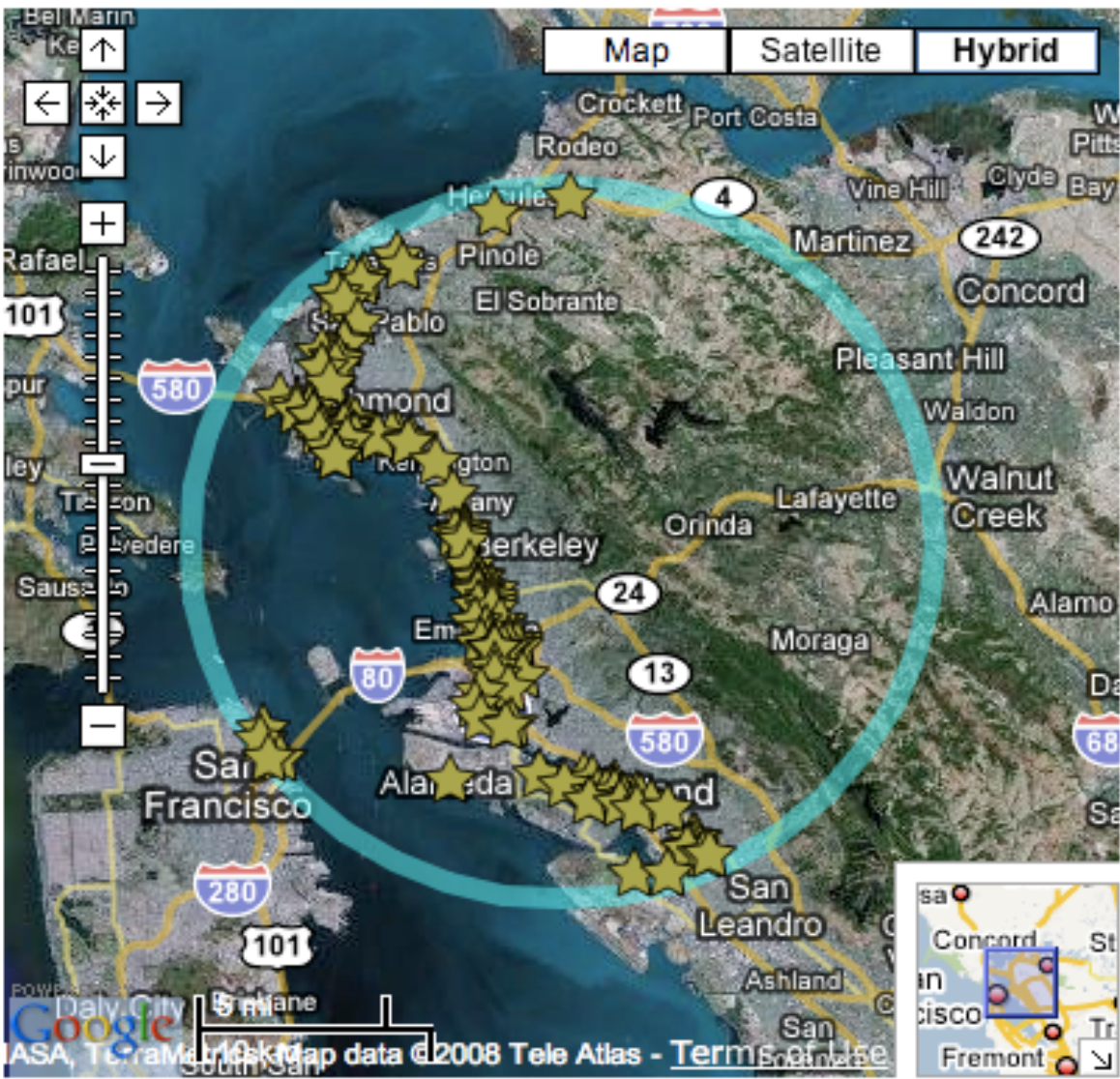
Political Activity

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



Map Satellite Hybrid

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: EPA TRI

Map State Zip Results

Enter a zip code and distance. Click Submit.

Zip Code: 94720

Lat/Long: 37.8739 / -122.254

Distance (miles): 10

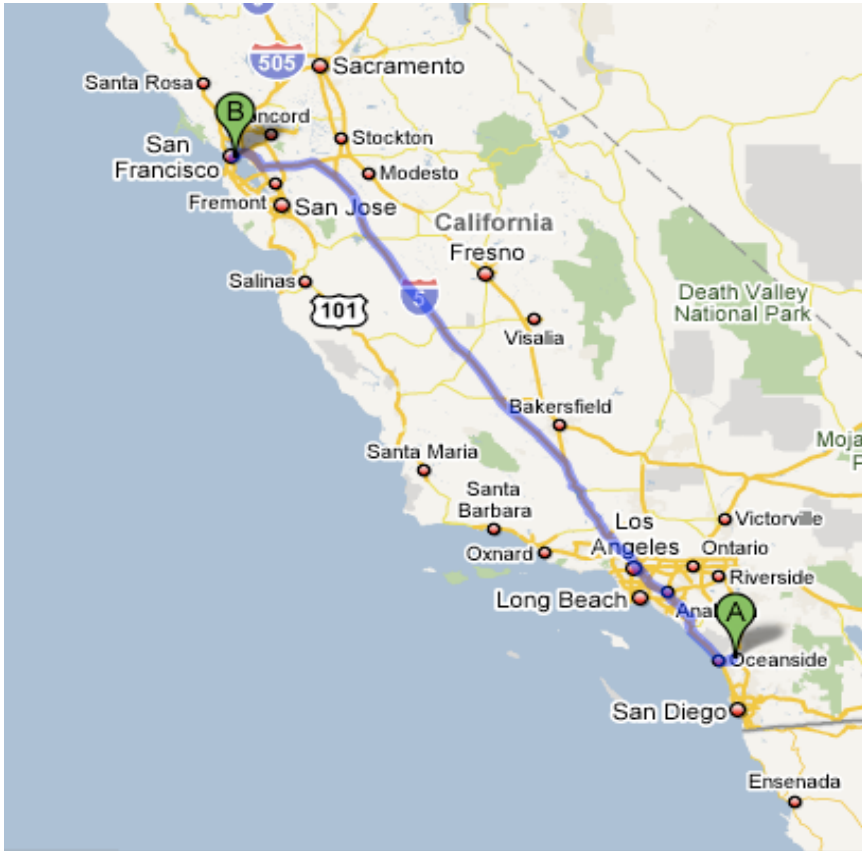
Submit

☆ EPA Sites of Concern ○ State Sites of Concern

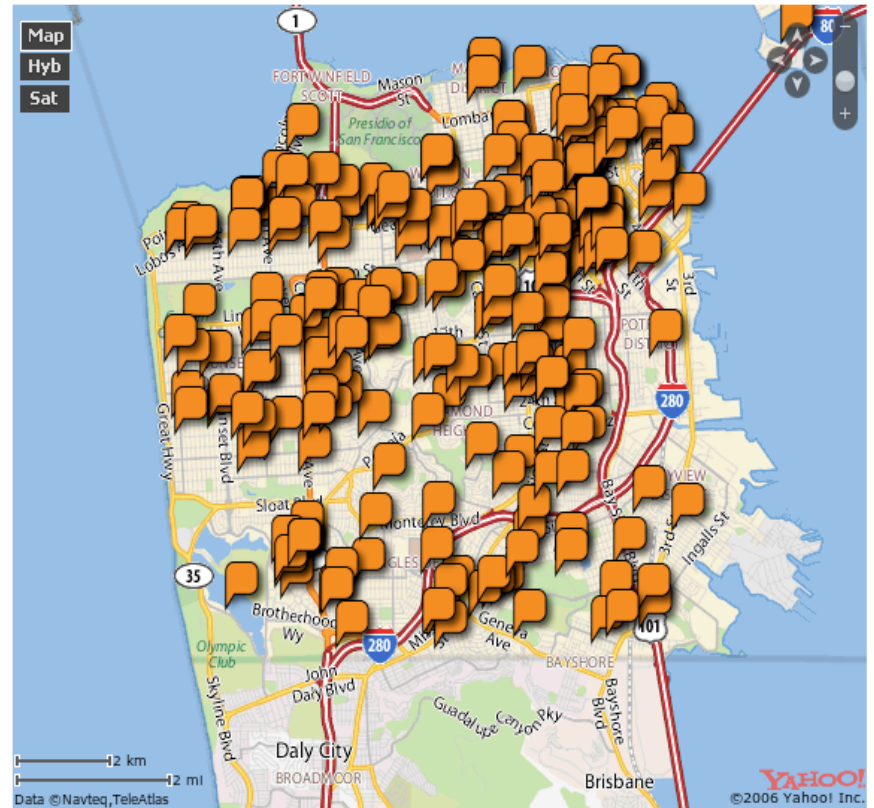
115 sites found!

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 effecting 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

Reforms

- Standardized, electronic, centralized reporting
- Does NOT create publicly available database

- Dual standard of notification?
- User based analysis of information
 - shifts in content, format and **timing**
- Metrics to determine risk, not just loss