Protecting Personal Information: Obstacles and Directions

Rachel Greenstadt and Mike Smith

{greenie,smith}@eecs.harvard.edu

WEIS 2005

Harvard University

June 3, 2005

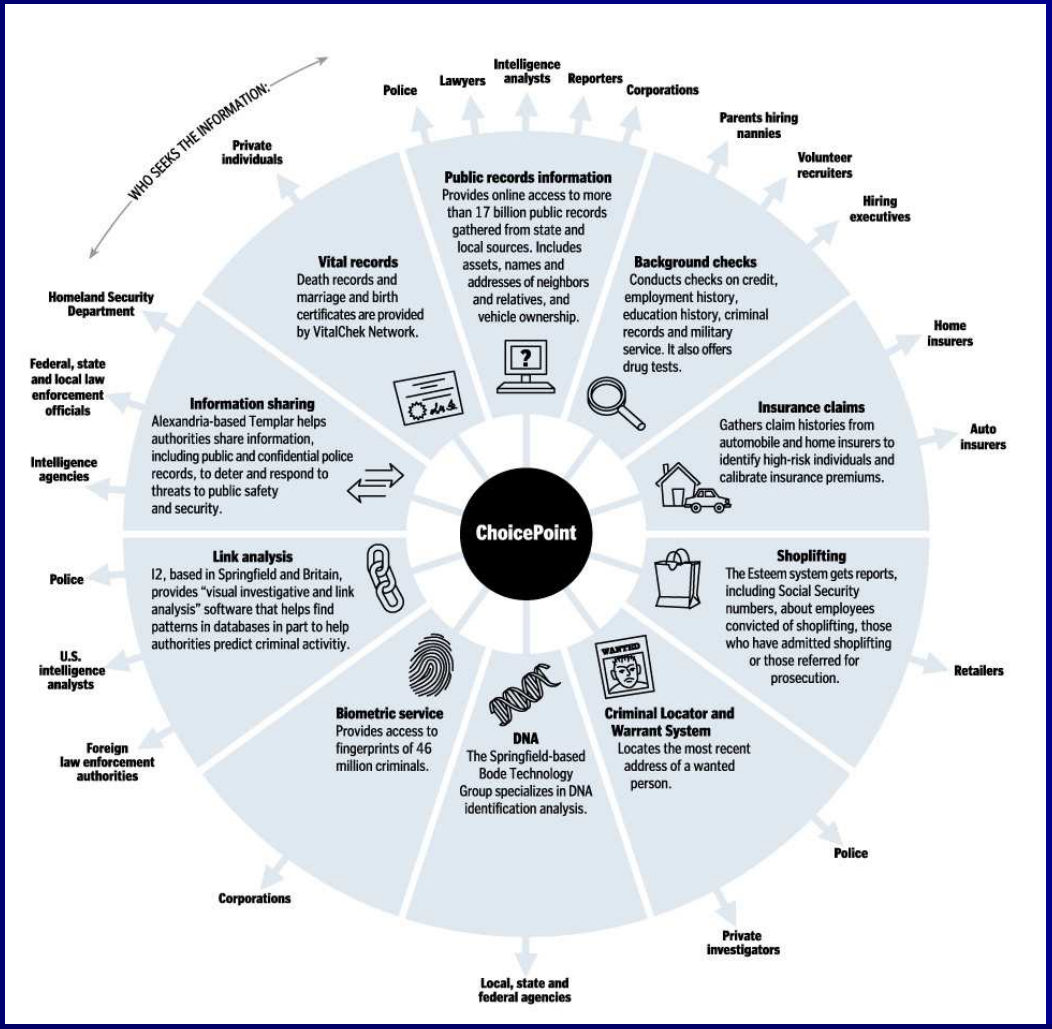
Overview

- Introduce privacy problem
- Present our framework
- Apply policy models
- Cross-cutting issues
- Recommendations and research agenda

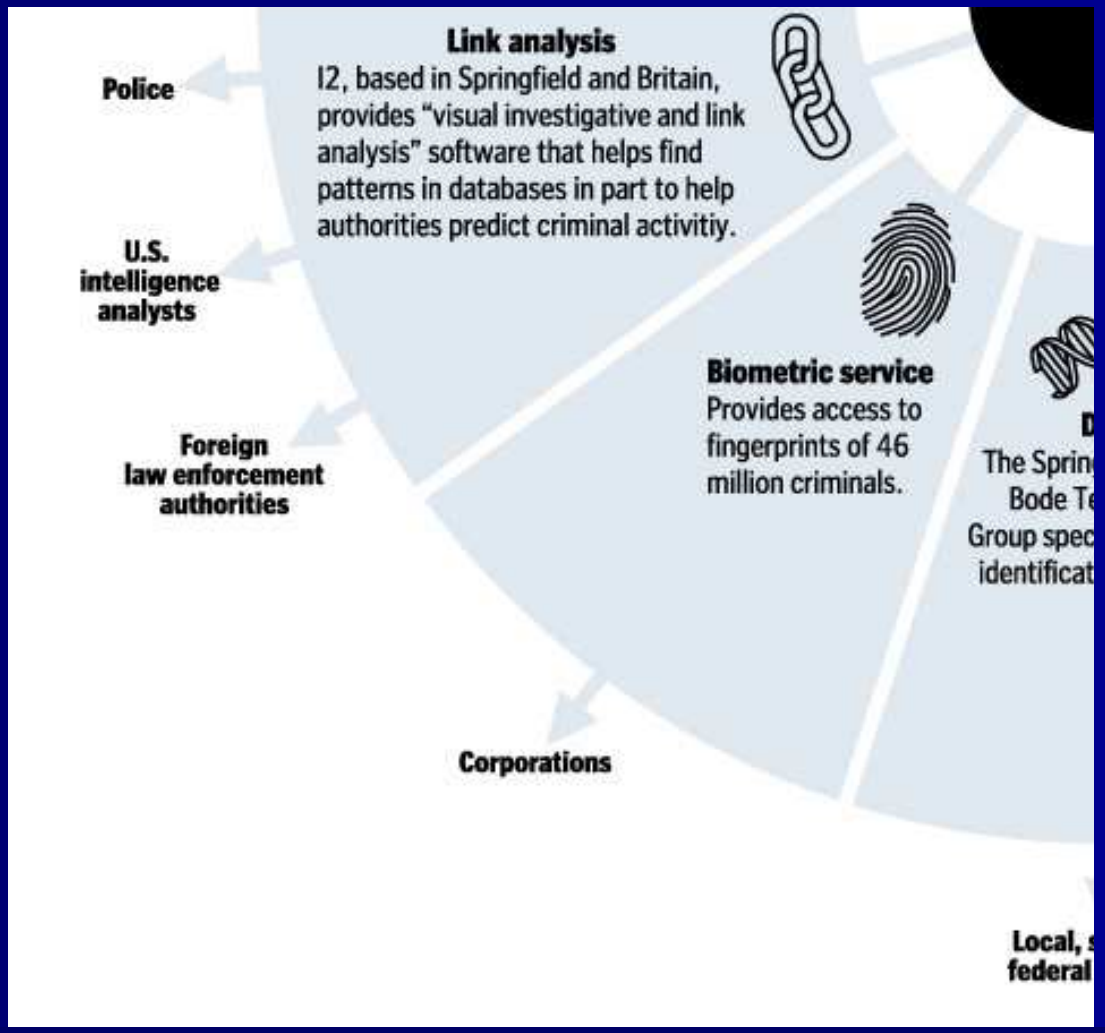
Personal Information Today

- Information technology makes it easy to collect, store, search and access personal information
  - Increased efficiency
  - Driven by market research, increasingly used by law enforcement
  - But individuals suffer a cost in loss of privacy

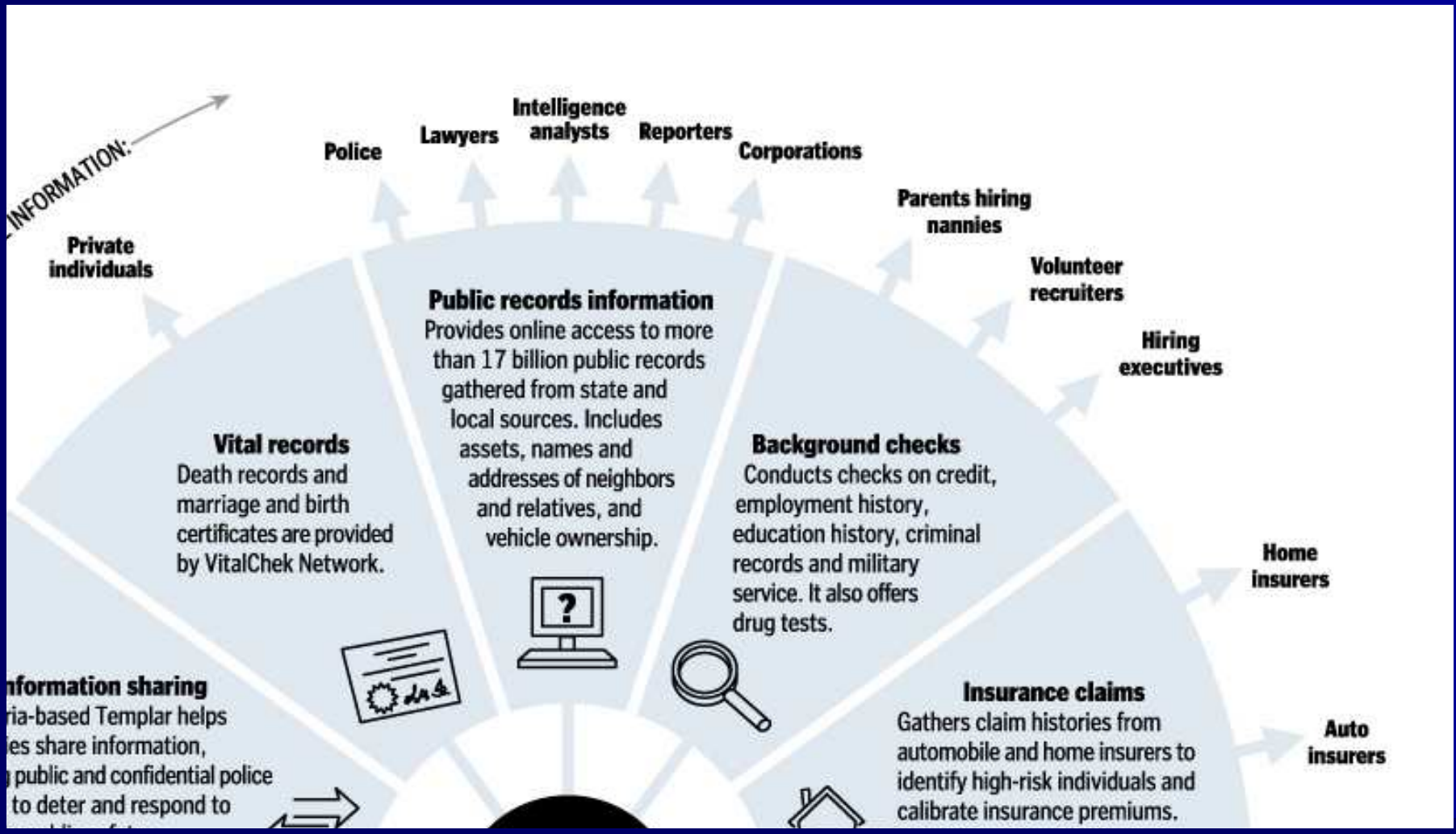
Some issues with this trend



Some issues with this trend



Some issues with this trend



Policy models

- Self-regulation
- Government regulation
- Third party regulation
- Markets for Personal Information

BUT

- No framework for comparing the viability of these approaches
- Policy papers tend to omit discussion of technical limitations and obstacles

Our Framework

Approaches to privacy must deal with three aspects of information control

- Decision-making
- Negotiation
- Enforcement

Decision-making

- Someone has to decide what information is worth protecting and controlling
- Who decides this? Individuals, government, industry groups or some combination?
- Do they have the information/ability to make good decisions?

Negotiation

- How do data users and data subjects reach agreements about the data?
- Bundling Issue
  - Info is collected for some primary use
    - An address to send a package
    - Credit card info to pay
  - Efficient to resell
  - Hard to agree to primary use without agreeing to the secondary use
  - Need for ways to separate these uses

Enforcement

Mechanisms to ensure data users abide by negotiated rights.

- *Transparency*—can data subjects see that the mechanism is effective?
- *Active*—are there mechanisms to make it hard to violate negotiated rights?
- *Strength*
  - Is it hard to avoid getting caught?
  - Are the penalties for getting caught severe?

Models Overview

	Decision-making	Negotiation	Enforcement
Self Reg			
Gov't Reg			
3rd party			
Markets			

- EASY - implementable, no major problems
- MED - implementable, but major problems
- HARD - not currently implementable and major problems

Self-regulation

- Most promoted by industry, status quo in U.S.
- The argument: Privacy-invasive practices will cause consumers who care about privacy to choose firms that protect personal data
- Decision-making: firms
- Negotiation: privacy policies
- Enforcement: reputation

Issues with Self-regulation

- Decision-making: No incentives for firms to have good policies
- Negotiation: Privacy policies make poor signals
- Enforcement: Consumer reputation doesn't matter as much for firms with a b2b business model

Models Overview

	Decision-making	Negotiation	Enforcement
Self Reg	HARD	HARD	HARD
Gov't Reg			
3rd party			
Markets			

- EASY - implementable, no major problems
- MED - implementable, but major problems
- HARD - not currently implementable and major problems

Government Regulation

- Government makes laws
  - Regulating the use of data
  - Specifying when consent is necessary
- Decision-making: Gov't
- Negotiation: Gov't decree
- Enforcement: Investigative and punitive powers of legal system

Issues with Gov't Regulation

- Decision-making: Gov't *not* a disinterested third party
- Negotiation: Only possible through lobbying
- Enforcement: Limited by borders and jurisdiction

Models Overview

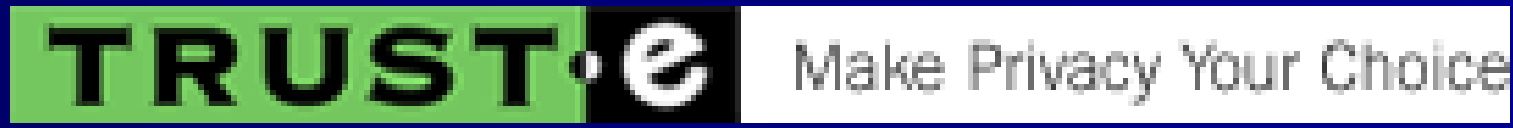
	Decision-making	Negotiation	Enforcement
Self Reg	HARD	HARD	HARD
Gov't Reg	MED	EASY	HARD
3rd party			
Markets			

- EASY - implementable, no major problems
- MED - implementable, but major problems
- HARD - not currently implementable and major problems

Third Party Regulation

Replace gov't with other (more trusted?) party

- Privacy seals



- Intermediaries using rights management technology

Third Party Regulation: Seals

- Third party provides a seal to companies that meet their privacy standard
- Consumers have a simple signal
- Aid to self-regulation
- Decision-making: seal providers decide the standards, firms decide if it's worth it to participate, consumers decide to patronize the company or not based on the seal
- Negotiation: Not needed
- Enforcement: Audits by seal provider

Issues with seals

- Limited enforcement ability (without coercive powers of gov't)
- Capture problem
  - Seal auditing is paid for by firms being audited
  - Pressure for audits to have a positive outcome
  - Seal loses meaning

Models Overview

	Decision-making	Negotiation	Enforcement
Self Reg	HARD	HARD	HARD
Gov't Reg	MED	EASY	HARD
3rd party	MED	EASY	HARD
Markets			

- EASY - implementable, no major problems
- MED - implementable, but major problems
- HARD - not currently implementable and major problems

Markets for Personal Information

- Give individuals property rights in their personal information
- Mitigates the privacy externality
- Information intermediaries (like banks) might help individuals manage their information rights

Markets in our Framework

- Decision-making: Gov’t decides what personal information is "owned" by individuals
- Negotiation: Contracts between subjects and users
- Enforcement: Federal Information Commission oversees the market, like the Securities Exchange Commission (Laudon)

Issues with Markets

- Decision-making
  - Individuals can and will still make lousy choices
- Negotiation
  - How do people enter the market? Primary vs. secondary uses and bundling
  - If information brokers would be so useful, why don't we have them today?
- Enforcement
  - Jurisdiction problem
  - No active enforcement

Models Overview

	Decision-making	Negotiation	Enforcement
Self Reg	HARD	HARD	HARD
Gov't Reg	MED	EASY	HARD
3rd party	MED	EASY	HARD
Markets	HARD	MED	HARD

- EASY - implementable, no major problems
- MED - implementable, but major problems
- HARD - not currently implementable and major problems

Institutionalization

- System needs to come into being somehow
- Entrenched status quo
- Ambiguity can be the death of policy
  - Example: Oregon genetic privacy law (1995-2001)

Technical Enforcement

- Idea: Use technology to prevent or audit misuse
- DRM technology very analogous: watermarks, traitor-tracing, hardware and software rights management systems
- Problems
  - Technology is immature
  - Personal data space is larger and more heterogeneous than the intellectual property space

Policy Enforcement

- Impossible to technically enforce policy on small data items (SSN, credit card numbers, HIV status, etc)
- Require data holders to have license to their data—prosecute if they don't
- Use traditional investigative and punitive measures
- This may be difficult—hard to track loss of information

Enforcement

Ultimately, you'll need both technology and policy

Regulation as an Interim Measure

- All the models require or benefit from regulation
- Still hard: need to figure out what to regulate, and how to enforce the regulations
  - But, you need to figure these things out for any model
- Markets require legislative and institutional support and more complex negotiation and enforcement mechanisms.

Research Agenda

There are a number of hard problems that the economic and cs community can work on to improve policy options and work toward more flexible solutions.

- Technically—better enforcement and auditing practices.
- Economically—explore the bundling situation and figure out how to improve the choices individuals have in dealing with their personal information.

Conclusion

Hopefully, this paper will encourage future authors of models to realistically analyze their viability and clarify assumptions about

- Decision-making
- Negotiation
- Enforcement