

Privacy Practices and Economics

From Privacy Policies to Privacy SLAs

Günter Karjoth
IBM Zurich Research Laboratory



Internet consumers pay for services with their
personal data exposure to advertisements.

Meglana Kuneva, EU Commissioner for Consumer Protection
(March 2009)

The Cost of Reading Privacy Policies

Per American Internet user (in 2005)

- Internet connection cost: \$500
- Reading privacy policies:
201 hours a year, worth about \$2,949

- Nation-wide a loss of \$652 billion
- Value of all on-line advertising: \$21 billion

- Is self-regulation out-of-balance?

A. McDonald and L. Faith Cranor (2008)

Example

The most fundamental economic transaction is that of *exchange*: two individuals engage in a trade.

→ How do privacy concerns enter this very basic transaction ?

Roughly speaking the buyer wants the seller to know his tastes about which products he may be interested in buying; but he doesn't want the seller to know how much he is willing to pay for those products.

Hal R. Varian: Economic Aspects of Personal Privacy (1996)

Profiling Individuals

The seller has to tell me about each of the different kinds of apples that he has to sell before I am able to purchase.

It is important to recognize that this form of annoyance--essentially **excess search costs**--arise because the seller has too little information about the buyer. If the seller knew precisely whether or not I was interested in buying insurance or refinancing my mortgage, he could make a much better decision about whether or not to provide me with information about his product.

→ seller is using information about me that is correlated with my likelihood of purchasing certain products (direct marketing)

→ “right not to be annoyed”

⇒ **no price discrimination**



www.turbulence.org/Works/swipe/calculator.html

Secondary users of information

- When a mailing list is sold to a third party, the relationship between the buyer's original interests and the seller's interest may become more tenuous.
- Economists would say that an *externality* is present. The actions of the party who buys the mailing list will potentially impose costs on the individuals on that list, but the seller of the mailing list ignores those costs when selling it.
- These costs could be mitigated, to some degree, if the individual who is on the mailing list has a voice in the transaction. For example, the individual could forbid all secondary transactions in his personal information. Or, more generally, the individual could allow his information to be distributed to companies who would send him information about X, but not about Y.
- These considerations suggest that the difficulty in the “annoyance” component of privacy could be significantly improved if
 - the communications channels between the buyers and the sellers were clearer,
 - the information conveyed was more accurate, and
 - third-party transactions were restricted only to those transactions that the original consumers authorized.

Incentives involving payment

- Cases where the buyer's revealing information about himself is detrimental
 - smoker & life insurance
→ non-smoker ?

- More generally, suppose that the price that the seller would like to charge is higher for people with some characteristic C. Then people who have that characteristic have bad incentives to reveal it, but people who don't have that characteristic have good incentives to reveal it. It is in the interests of the seller to construct the transaction in a way that the information is revealed.

Contracts

“Check here if you would like your name distributed to other parties who will provide you with information about computer peripherals until 12/31/98. After that, name and address will be destroyed. In exchange you will be paid \$5.00 for each list to whom your name and address is distributed.”

An individual might provide information about himself to a company that aggregates it with 999 other individuals with similar demographic and marketing characteristics. Such groups could be described by titles such as “20-30 year old males in California who are interested computers,” or “20-30 year old married couples interested in home purchase.”

Those who wanted to sell to such groups could purchase rights to use these mailing lists for limited periods of time. The payments they made would flow back to the individual users as “dividends.” Individuals who found the annoyance cost of being on such lists greater than the financial compensation could remove their names. Individuals who felt appropriately compensated could remain on the lists.

→ Information about individuals is commonly bought and sold today by third parties in market-like environments

→ Above arrangement simply gives individuals an economic stake in those transactions that they currently do not have.

The cost of COPPA

- US Federal Trade Commission (FTC)
 - Xanga, \$1,000,000, 2006
 - UMG Recordings, \$400,000, 2006
 - Mrs. Fields Cookies, \$100,000, 2003
 - FTC has brought 12 COPPA enforcement actions through 2007, assessing more than \$1.8 million in civil penalties.
 - Courts can hold companies failing to comply with the requirements of COPPA liable for civil penalties of up to \$11,000 per violation.

- \$200'000/year to employ chat-room supervisors, monitor phone lines to answer parents' questions and process COPPA permission forms
 - Zeeks.com, 2000

California Senate Bill 1386

- The law requires those who own or license personal information of California residents to notify them if their data has been breached (effective since July 1, 2003).
- A company must notify those affected by written or electronic notice when it believes an unauthorized person has obtained personal information. In cases where notification costs more than \$250,000 or affects more than 500,000 people, substitute notice measures may be employed: notification to major statewide media, posting on the company's website, notification by email.
- The law does not impose fines or minimum prison sentences, but it does specifically allow civil lawsuits: "Any customer injured by a violation of this act may institute a civil action to recover damages."
- ID verification services vendor ChoicePoint's breach of personal financial data for more than 163,000 consumers in early 2006 will cost the company **\$15 million** in fines to FTC.

Risks of not Addressing Privacy

□ Legal Risks

- Fines, lawsuits, imprisonment, ...
- Seizure of files and data
- Injunctive measures (e.g. blocking of data flow)

□ Business Risks

- Damage to reputation, public/consumer trust
- Press “goes negative”, brand name tarnished
- Loss of business products and opportunities
- Inability to transfer data across national boundaries
- Loss of customers and market share



Organizations seek to minimize the sum of the costs of privacy breaches plus the cost of information protection expenditures !

➤ under/over invest in protection mechanisms

Privacy as a Market (Baumer, 2005)

- Organizations that collect & store personal data largely supply security, which of course costs resources
- Consumers, costumers and users are purchasers of privacy
- The intersection of supply and demand at a price is normally thought to be an efficient solution.
- However, there is more accurate information about the costs of providing security than there is about the demand for privacy.

Privacy Benefits

Privacy economics is about

- costs of compliance (technology, legal measures, enforcement)
 - benefits (soft values, economic or social rewards),
- which together allow an individual to accept or refuse solicitations of access to private information.

Identification of benefits is highly context and situation dependent

- identification of privacy attributes of importance to each party
- benefit and cost evaluations according to these attributes; metrics are often indirect, derived, and almost always qualitatively defined.
- risk evaluation linked to trust evaluation between the parties
- negotiation, ranging from a one step accept / refuse / opt-out decision, to n -step negotiations with termination rules.
- monitoring and escalation processes

Negotiation is key!

⇒ negotiation algorithms are needed to automate service discovery

Requirements

- Without a means to accurately and understandably measure it, privacy fails to provide a competitive advantage !

Effective metrics

- the cost to protect personal data
- the cost & benefit of disclosing personal data
- ?

Privacy Attributes & Metrics

- Data
(sensitivity, aggregation, purpose, quantity, age)
- Retention (time)
- Disclosure (k-anonymity, purpose)
- Consent (strength)
- Obligation (notification)

- Information channel (“individual participation”)
- Reputation (e.g., seals)

- ⇒ interpretation possible wrt cost

Service Level Agreements

An SLA is typically signed between two parties, which have the role of provider and consumer respectively, and has the following components:

- purpose
- parties
- validity period
- scope
- restrictions
- service level objectives
- penalties
- exclusions
- administration

Service Level Agreements (cont'd)

- An SLA is specified over a set of data that is measurable !
- It has a validity period and a set of Service Level Objectives:
 - day-time constraint
 - a set of clauses based on measured data
- It defines
 - how services are monitored,
 - liabilities on the part of provider/consumer,
 - what actions are taken in specific circumstances.

Privacy Processes & Negotiations

- **Negotiation** processes rely on SLAs established in the context of (long term) contracts between multiple parties; these SLAs have high dynamics and exception handling.
- Handling of private information is not just between one individual (or organization) (with/without economic interests) and another individual or organization
→ **chain of SLAs**
- Different **metrics / values** and dissemination processes attached to SLAs may create breaches in privacy to all or some parties without they even know about such risks.

Conclusion

- ❑ Privacy is more than a compliance issue - it is a **business issue**.
- ❑ Security enables privacy, so the two must be aligned.
- ❑ **Cost** of security mechanisms & PETs must be made explicit
- ❑ Clarify what's **measurable** and what's not.
- ❑ Develop **Privacy SLAs** as a framework.

- to enable **negotiation** over the often competing demands of consumers and enterprises.

Conclusion (cont'd)

- An economic interpretation of the elements of privacy leads to more comprehensive privacy policies,
- which then may give an incentive to consumers to think about them twice.

Quantitative data is needed that reduces an organization's uncertainty about the costs faced by privacy breaches as well as by implementing appropriate protection mechanisms.

Literature

- Hal R. Varian: Economic Aspects of Personal Privacy. 1996
people.ischool.berkeley.edu/~hal/Papers/privacy/
- L. Jean Camp, Economics of identity theft: avoidance, causes and possible cures, Springer Science+Business Media, LLC, 2007.
- L.-F. Pau.
"Privacy Management Contracts And Economics, Using Service Level Agreements (SLA),"
Research Paper 1566-5283, Erasmus Research Institute of Management (ERIM), RSM Érasmus University, revised 22 Feb 2006.
- G. Karjoth, B. Pfitzmann, M. Schunter, M. Waidner.
Service-oriented Assurance - Comprehensive Security by Explicit Assurances.
In "Quality of Protection: Security Measurements and Metrics",
Advances in Information Security, pages 13-24. Springer, 2006.
- Baumer, New Uses of Experimental Economics in Estimating Privacy Behavior. 2005
- Tom Rosamilia. Privacy of Data, a business perspective.
www.almaden.ibm.com/institute/pdf/2003/TomRosamilia.pdf