Economics and Cryptography

Andrew Odlyzko
AT&T Labs - Research

amo@research.att.com
http://www.research.att.com/~amo

Motivation and outline:

- Basic question: Why hasn't cryptography lived up to its promise?
  - What crypto-related technologies are likely to succeed?

- Main points:
  - Strong economic reasons for crypto disappointments
  - People and formal methods don't mix well
  - Sellers have strong incentives to resist anonymity and small atomic transactions
  - Auctions, micropayments, DRM, automated agents, and "dynamic pricing" likely to play a smaller role than expected.

Honor System Virus

This virus works on the honor system.

Please forward this message to everyone you know and then delete all the files on your hard disk.

Thank you for your cooperation.

Major problem with secure systems:

secretaries could not forge their bosses' signatures

Ambiguity of human discourse:

Please let the plumber in to fix the leaky faucet.


WIZARD
ELECTRIC
ACE
PLUMBING


WIZARD
ELECTRIC
ACE
PLUMBING
2000

Another limitation on crypto: quantitative economic models

Most important: economic desirability of price discrimination:

Charlie: willing to prepare a report on digital cash for $1,500

Alice: willing to pay $700

Bob: willing to pay $1,000

Uniform pricing makes transaction impossible

Charging Alice $650 and Bob $950 makes everybody better off (in conventional economic model)

Modern economy is moving towards higher fixed costs and lower marginal costs, which increases the incentives to price discriminate

Information goods (software, music): prototypical example

Also true of other high-tech products:

Pharmaceuticals

Microprocessors

Pentium prices:	\$100–500
Marginal cost	$\sim$ \$30

Communication satellites

Cars: design and tooling costs of \$2–3B for each new model

Ecommerce is not about "frictionless capitalism," but about exploiting market power, creating barriers, ...

See

AO, "The bumpy road of electronic commerce," *Proc. WebNet 96*, available at ⟨http://www.research.att.com/∼amo⟩,

Shapiro and Varian, *Information Rules*, Harvard Business School Press, 1998,

or any of numerous papers on spectrum auctions.

Price discrimination through versioning:

> It is not because of the few thousand francs which would have to be spent to put a roof over the third-class carriages or to upholster the third-class seats that some company or other has open carriages with wooden benches. What the company is trying to do is to prevent the passengers who can pay the second class fare from traveling third class; it hits the poor, not because it wants to hurt them, but to frighten the rich. And it is again for the same reason that the companies, having proved almost cruel to the third-class passengers and mean to the second-class ones, become lavish in dealing with first-class passengers. Having refused the poor what is necessary, they give the rich what is superfluous.
>
> Jules Dupuit, 1849

Microsoft Office (for Windows 3.11)

components:

Access	\$225
Excel	\$225
Power Point	\$225
Word	\$175
	\$850

Office Pro bundle: \$389

Bundling is an alternative to price discrimination in reducing consumer surplus:

Willingness to pay:

	word processor	spreadsheet
Alice	\$100	\$300
Bob	\$300	\$100

Pricing and revenue:

\$100 for each program	$\rightarrow$	\$400
\$300 for each program	$\rightarrow$	\$600
\$400 for bundle	$\rightarrow$	\$800

Site licensing:

1000 employees

# employees	value
900	\$ 0
10	\$ 10
10	\$ 20
10	\$ 30
10	\$ 40
10	\$ 50
10	\$ 60
10	\$ 70
10	\$ 80
10	\$ 90
10	\$ 100

Sales to individuals: optimal price either \$50 or \$60

$$\text{revenue} = \$3,000$$

Site licensing: revenue = \$5,500

Behavioral economics: serious constraints on price discrimination, “dynamic pricing,” auctions, ..., because of negative public reactions:

Ultimatum game:

1. \$10 to be divided by Alice and Barbara

2. Alice proposes a split (for example, \$7 for Alice, \$3 for Barbara)

3. (a) Barbara accepts: each gets specified amount

   (b) Barbara rejects: neither gets anything

Railroads in the 19th century: extremely important, widely hated

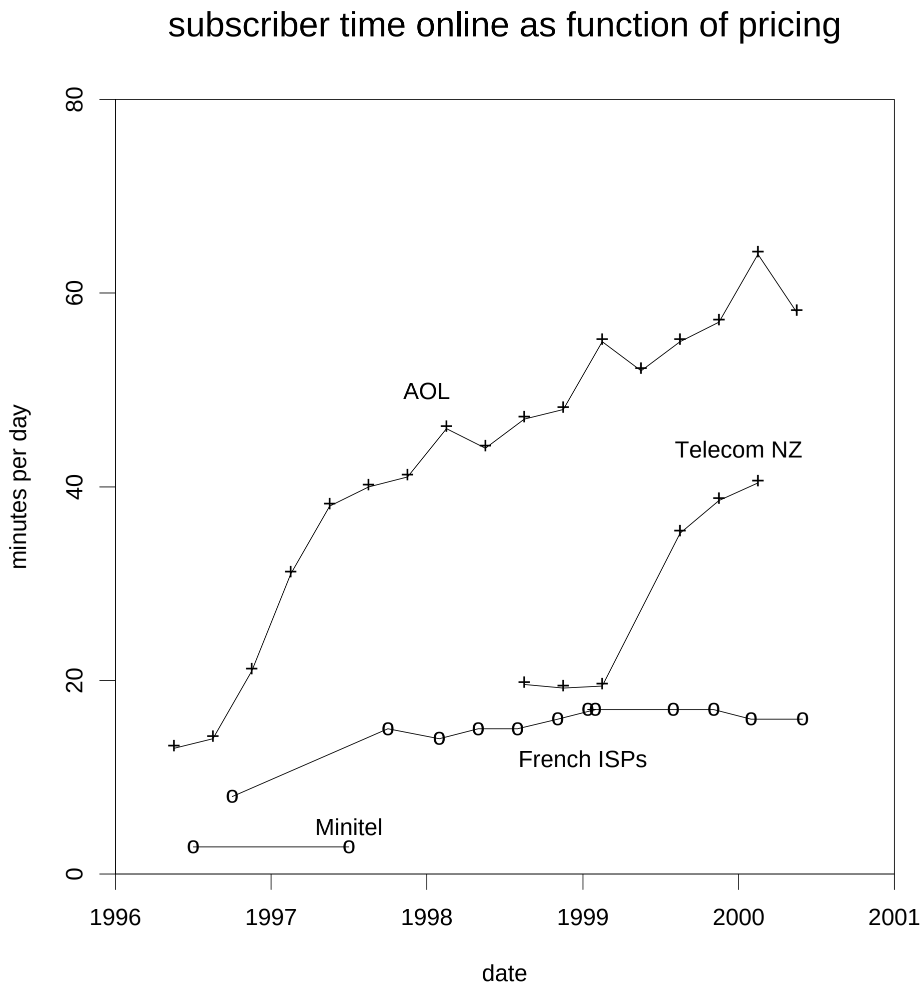
> The drama was over. The fight of Ranch and Railroad had been wrought out to its dreadful close. ... Yes, the Railroad had prevailed. The ranchers had been seized in the tentacles of the octopus; the iniquitous burden of extortionate freight rates had been imposed like a yoke of iron.
>
> "The Octopus"

Interstate Commerce Act of 1887: first serious federal regulation

Provisions:

- Rates to be “just and reasonable”
- Personal discrimination forbidden
- “Undue or unreasonable preference” forbidden
- Charging more for short than long haul on same line forbidden
- Pooling forbidden
- Rates to be published
- ...

Economics of networks: main imperative is often to increase usage, and nothing does this as well as flat rates



AO, “Tragic loss or good riddance: The impending demise of traditional scholarly journals,” 1994: predicted that pay-per-view in scholarly communication doomed to fail because of the deterrent effects of usage charges

[Elsevier’s] goal is to give people access to as much information as possible on a flat fee, unlimited use basis. [Elsevier’s] experience has been that as soon as the usage is metered on a per-article basis, there is an inhibition on use or a concern about exceeding some budget allocation.

K. Hunter of Elsevier, 2000

Incentives for sellers:

- price discriminate
- increase usage
- hide price discrimination

Most likely solutions: combination of techniques such as

- personalized bundles
- loyalty programs

Conclusions:

- Data mining to flourish, privacy to suffer
- Government role likely to be ambigous, since price discrimination is often socially desirable, but will likely be substantial
- DRM, auctions, micropayments to play minor role

References: several papers at
http://www.research.att.com/∼amo
including two not there yet, as they are in preparation ("Privacy, economics, and price discrimination on the Internet" and "Stronger copyright protection for cyberspace: Desirable, inevitable, and irrelevant")

Also:

- Ross Anderson, Liability and computer security - nine principles, 1994
- Dan Geer, Risk management is where the money is, 1998
- Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World," 2000
- Ross Anderson, "Security Engineering - A Guide to Building Dependable Distributed Systems," 2001