

Infomediaries, as a privacy- enabling technology



Dimitris Gritzalis

Spring Conference of European Data Protection Commissioners
Athens, Greece, May 2001

Infomediaries, as a privacy-enabling technology



Prof. Dr. Dimitris Gritzalis
Associate Member of the Board
Data Protection Authority of Greece

Online Privacy Concerns

- ✓ The **lack of privacy and security** in communications is the main reason of a consumer being off the Internet.

[Harris poll, 1998]

59% of consumers in the United States are most worried about Web sites collecting personal information, without the consent of the involved persons.

Online Privacy Concerns

- ✓ Consumers are worrying about **how their personal data will be used** and how this data can be protected against unauthorized access.

[National Consumers League, 1999]

64% said they were most worried about Web sites providing personal information to others without their knowledge

[US Dept. of Commerce, 2000]

86% said they are concerned about businesses or people they don't know getting access to their personal information.

Typical examples of how personal information is collected on-line

- **Personally-identifiable information (PII)** provided by users (e.g. from purchase, form-filling, registering, etc.).
- **Browser information** (e.g. IP address, domain name, operating system, search terms, etc.).
- **Cookies** (i.e. text files stored in a user hard disk, identifying user identity every time he is connected to a Web site).
- **Web bugs** (i.e. accidental or on purpose flaws in Web browser design and implementation).

Privacy-enhancing means and technologies (PET)

- **Anonymizing tools** (e.g. www.anonymizer.com)
- **Pseudonymity tools** (e.g. www.iPrivacy.com)
- **Cookie Managers**
- **Privacy Preferences Project (P3P) user-agents** (www.w3.org/p3p/)
- **Encryption tools**
- **Infomediaries**
- **Others** (e.g. access tools, privacy policy generators)

PET inefficiencies

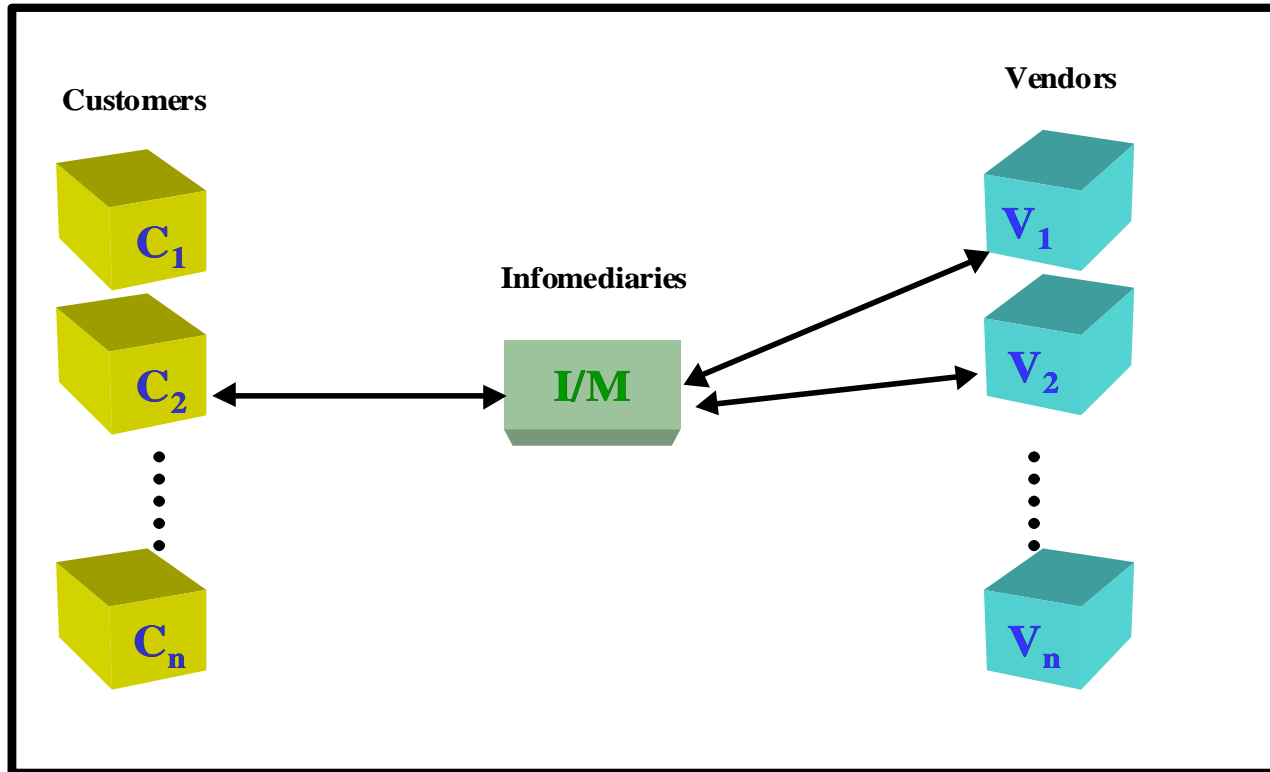
- × PET fail to protect authenticity and integrity of the exchanged messages.
- × PET exploit confidentiality mechanisms only to provide anonymity, but fail to control access to user personal data.
- × PET are more privacy-enhancing tools than models oriented to support global and anonymous e-commerce purchases, so they do not integrate technologies helping users explore and make use of the electronic marketplace.
- × PET cannot encounter collusion attacks (corrupt coalition of users or parts of a system, in order to trace certain users)

Infomediaries are...

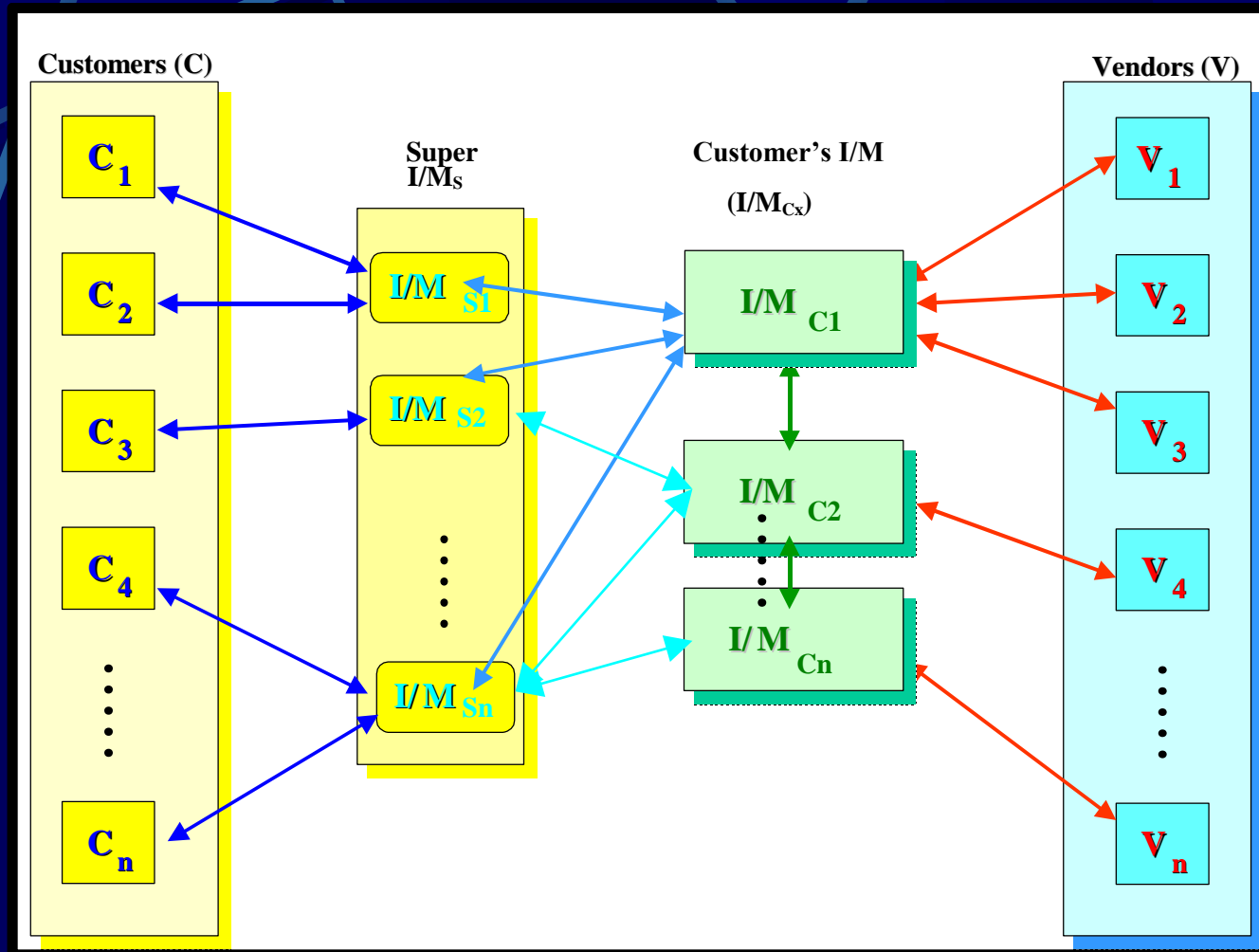
business entities
whose (sole or main) source of revenue
derives from collecting consumer information
and developing detailed profiles
of individual customers,
for use by selected third-party vendors.

Hagel J., Rayport J., «The new infomediaries»,
The McKinsey Quarterly, No. 4, November 1997.

Infomediaries: Existing architecture



An updated architecture



Involved entities, req's, functionalities

Entity

Requirements (expectations)

Functionality

Customer (C_x) Buy goods from vendors, Retain privacy and anonymity

Vendor (V_x) Dispose products to customers, Increase their sales, Reduce the advertising cost, Gain more revenues, Aware of customers preferences

Customer oriented Infomediary (I/M_{CX}) Act on customers' benefit, Own large databases, Increased marketing skills

Super Infomediary (I/M_S) Trusted by vendors and customers

Delivery of products to I/M_S

Collection of product offerings, Building of profiles, Matching of profiles with vendors' products, Gathering of customers requests from I/M_S, Reference to other I/M_{CX} when an I/M_{CX} request does not match an entry in the local database.

Supervision of model procedures, Setting up of the I/M PKI, Protection of anonymity, privacy, and authenticity, Collection of personal information, Collection of customer preferences

Updated model characteristics

- ☞ Users should **trust I/M**, as they are agents of their personal information. A **security infrastructure** (i.e. I/M PKI) should be provided to implement this trust (i.e. use of digital certificates to provide confidentiality and authentication).
- ☞ **No entity owns the pair** {user preferences, user identity}, at the same time (i.e. need to know principle).
- ☞ There can be **no collusion attacks**.
- ☞ **Need for a secure acquaintance mechanism** (e.g. I/M directory service) between the various I/M.

Infomediaries: Present - future

- Infomediaries support privacy, in its way to gain ground in the market.
- A business model cannot and should not replace legal rights.
- Support the right of a citizen to offer his personal data.
- Infomediaries must respect the OECD Fair Information Practice Principles.

Conclusions (1 of 3)

- No known PET satisfy all OECD Fair Information Practice Principles (Notice/Awareness, Choice/Consent, Access/ Participation, Integrity/Security, Enforcement/ Redress).
- Tools that provide Notice include: P3P, Cookie Managers.
- Tools that provide Choice include: P3P, Cookie Managers, Anonymity, and Pseudonymity tools.
- Several tools provide Access to data.

Conclusions (2 of 3)

- PET should be used in conjunction with:
 - Encryption tools that provide Security
 - Seal programs and regulations, which provide Enforcement
- A combination of PET may allow users to fulfill their own **privacy preferences**.
- Technologies are only **part** of the required solution.

Conclusions (3 of 3)

- There should be **no unnecessary obstacles** to the development of new technologies.
- Need for continuous **education and training** (mainly of **consumers** and **public policy-makers**) on the specific role technologies can play.

References

1. Gritzalis D., "A digital seal solution for deploying trust on commercial transactions", *Information Management & Computer Security*, Vol. 9, No. 2, pp. 71-79, March 2001.
2. Gritzalis D., "Enhancing security and supporting interoperability in healthcare information systems", *Medical Informatics*, Vol. 23, No. 4, pp. 309-324, 1998.
3. Gritzalis D., "A baseline security policy for distributed healthcare information systems", *Computers & Security*, Vol. 16, No. 8, pp. 709-719, 1997.
4. Gritzalis D., Kantzavelou I., Katsikas S., Patel A., "A classification of health information systems security flaws", Proc. of the 11th International Information Security Conference, pp. 453-464, Chapman & Hall, South Africa 1995.
5. Iliadis J., Gritzalis D., Spinellis D., Preneel B., Katsikas S., "Evaluating certificate status information mechanisms", *Proc. of the 7th ACM Computer and Communications Security Conference*, pp. 1-9, ACM Press, Greece, October 2000.
6. Katsikas S., Gritzalis D., Spirakis P., "Attack Modeling in Open Network Environments", *Proc. of the 2nd Communications and Multimedia Security Conference*, pp. 268-277, Chapman & Hall, Germany 1996.
7. Katsikas S., Spyrou T., Gritzalis D., Darzentas J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
8. Pangalos G., Gritzalis D., Khair M., Bozios L., "Improving Medical Database System Security", *Proc. of the 11th International Information Security Conference*, pp. 11-25, Chapman & Hall, South Africa 1995.
9. Tryfonas T., Gritzalis D., Kokolakis S., "A qualitative approach to information availability", Proc. of the 15th IFIP International Information Security Conference, pp. 37-48, Kluwer Academics, China, August 2000.