Infomediaries, as a privacy-enabling technology

Dimitris Gritzalis
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»,  
Infomediaries: Existing architecture

Diagram showing the existing architecture of infomediaries with vendors and customers. The diagram includes nodes for customers ($C_1$, $C_2$, $C_n$) and vendors ($V_1$, $V_2$, $V_n$) connected through infomediaries ($I/M$).
An updated architecture

Customers (C)

Super I/Ms

I/M s1

I/M s2

I/M sn

Customer’s I/M
(I/M_{C\lambda})

I/M_{C1}

I/M_{C2}

I/M_{Cn}

Vendors (V)

V_1

V_2

V_3

V_4

V_n
# Involved entities, req’s, functionalities

<table>
<thead>
<tr>
<th>Entity</th>
<th>Requirements (expectations)</th>
<th>Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer ($C_X$)</td>
<td>Buy goods from vendors, Retain privacy and anonymity</td>
<td>Delivery of products to I/M$s$</td>
</tr>
<tr>
<td>Vendor ($V_X$)</td>
<td>Dispose products to customers, Increase their sales, Reduce the advertising cost, Gain more revenues, Aware of customers preferences</td>
<td>Collection of product offerings, Building of profiles, Matching of profiles with vendors’ products, Gathering of customers requests from I/M$<em>S$, Reference to other I/M$</em>{CX}$ when an I/M$_{CX}$ request does not match an entry in the local database.</td>
</tr>
<tr>
<td>Infomediary (I/M$_{CX}$)</td>
<td>Act on customers’ benefit, Own large databases, Increased marketing skills</td>
<td></td>
</tr>
<tr>
<td>Super Infomediary (I/M$_S$)</td>
<td>Trusted by vendors and customers</td>
<td>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</td>
</tr>
</tbody>
</table>
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