Implementing privacy in online service models

ENISA panel at CPDP
25 January 2011
Panel

- Rodica TIRTEA (ENISA) and Claudia DIAZ, K.U.Leuven (BE)
- Simone FISCHER-HUEBNER, Karlstad University (SE)
  - Transparency enhancing tools, HCI for policy display & informed consent
- Claire VISHIK, Intel (UK)
  - Adjusting privacy and trust technologies to today's complex and dynamic computing environments
- Jacques BUS, University of Luxembourg (LU)
  - On the need for a multidisciplinary approach
- Jesus VILLASANTE, European Commission DG INFSO (EU)
  - Privacy and Trust in the Digital Agenda for Europe

Objectives

- Present results of ENISA work during 2010 in the field
- Discuss and gather ideas for future activities
Introduction

• About ENISA and its activities

2010 activities on privacy and data protection topics

• Data Breach Notification in Europe
• Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
• Privacy, Accountability and Trust – Challenges and Opportunities
• Bittersweet cookies. Some security and privacy considerations

Privacy related activities in 2011

Findings and issues to be further addressed
About ENISA
(European Network and Information Security Agency)

★ Created in 2004
★ Located in Heraklion / Greece
★ Around 30 Experts
  ★ Centre of expertise
★ Supports
  ★ EU institutions and
  ★ Member States
★ Facilitator of information exchange
  ★ EU institutions,
  ★ public sector &
  ★ private sector
★ Has an advisory role
  ★ the focus is
    • on prevention and preparedness
  ★ for NIS topics
Context of the work

• ENISA work programme 2010
  • PA1: Identity, accountability and trust in the future Internet
    ➢ New topic
      o Preparatory Action, extended activities in future year(s)
  • Two parts
    ➢ WPK PA1.1: Stock taking of authentication and privacy mechanisms
      o Studies on management of multiple identities and on existing practices in data breach notification (DBN) in various sectors
    ➢ WPK PA1.2: Stock taking of security models supporting electronic services
      o Focus on privacy, accountability and trust
      o Survey of current service models and recommendations
        o Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
        o Privacy, Accountability and Trust –Challenges and Opportunities
        o Bittersweet cookies. Some security and privacy considerations
PA 1.1 Study on existing practices in data breach notification (DBN) in various sectors

- **Policy context**
  - Review of ePrivacy Directive (2002/58/EC), Article 4

- **Target and aims**
  - Public authorities/private bodies
  - Support those lacking experience
  - Tool for improvement
  - Basis for discussions

- **Follow up**
  - ENISA workshop - 24 January 2011 – “DBN. The way forward”
Survey of mechanisms in online environments (I)

- Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments
  - Catalogue of current service models, topics covered in questions
    - Online service provided, accountability, trust, consent, tracking, security, privacy
  - Objective – 20 companies, 18 responses used for the study
    - About 200 companies contacted

<table>
<thead>
<tr>
<th>Simplified Online Service Model taxonomy</th>
<th>Baseline distinction</th>
<th>Stepping in social interactivity</th>
<th>Non-exhaustive examples of organisations operating with these online service models</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Commercial</td>
<td>Platform</td>
<td>Social Networking Sites (SNS), E-Auction, “Internet of things”, Online collaboration, ...</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>Infomediaries</td>
<td>E-Banking, Media storage, ...</td>
</tr>
<tr>
<td></td>
<td>Product</td>
<td>E-tailer (e.g. Electronics), E-bookshop, ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-commercial</td>
<td>Platform</td>
<td>Knowledge sharing, E-Procurement, Hospitality networks, Donation gathering, ...</td>
</tr>
<tr>
<td></td>
<td>Service</td>
<td>Open Source Software (OSS), National news service, E-health / E-government, ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Product</td>
<td>Social housing, Public transportation, ...</td>
<td></td>
</tr>
</tbody>
</table>
Survey of mechanisms in online environments. Remarks (I)

- Privacy in online environment; defining personal data given current context of data mining
  - Clear privacy principles and personal data definitions valid in an evolving online environment should be promoted
  - Privacy enhancing technologies and a user centric approach to privacy need to be encouraged. Best practice studies should be prepared and disseminated

- Consent and privacy policies
  - More transparency by organizations on how they handle personal data is needed
  - The way privacy policies are displayed and the issues regarding the changes of policies need further consideration; alternatives to lengthy privacy policies should be available to inform the user
  - Consent provided for a certain privacy policy must not be transferred to another (changed) version of privacy policy without clear understanding and acceptance of the user
Survey of mechanisms in online environments. Remarks (II)

- Profiling and tracking
  - Data retention time. Data should not be stored forever
    - Data minimization
- Personal data as a commercial asset; transfer of personal data between providers and outside EU
  - In line with the EU approach, ENISA considers privacy to be a basic Human Right
  - Economic effects of the use of personal data on both consumers and providers
    - and these effects should be analyzed
    - better understanding the effects and the risks could allow for solutions for protecting consumers’ privacy
  - The legal framework in 27 EU MS regarding the transfer of personal data should be surveyed; differences in legislation can encourage transfer of personal data to countries where the legal requirements allow for less privacy protection
  - The legal framework for transfer of personal data outside EU should be also analysed; equal treatment and same enforcement should exist for EU users’ personal data independent of the location of controllers/processors inside or outside EU
Privacy, Accountability and Trust – Challenges and Opportunities

- covering
  - Business & user perspective
    - Service value chain in Future internet
    - Behavioural tracking and profiling on the internet
    - On monetizing privacy
    - Transparency enhancing tools
    - HCI interaction for policy display and informed consent
  - Architecture side
    - Architecture and privacy
    - Identity management and privacy
    - Information accountability
    - Trust frameworks
    - Privacy preserving architectures
Promote technologies and initiatives addressing privacy

- Data minimization, privacy enhancing technologies and privacy by design concepts should be well understood and promoted in an effort to prevent rather than cure
  - evaluation of existing targeted (constructed on certain assumptions) solutions in the real environment
  - supporting the uptake of research result in the operational environment

- Research on information accountability technology should be promoted, aimed at the technical ability to hold information processors accountable for their storage, use and dissemination of third-party data

- Supporting informed user consent in a transparent and user friendly manner i.e. using transparent privacy policies with icons
Raise the level of awareness and education regarding privacy

- Concepts such as privacy certification could be supported; this would allow labeling sites and services according to their profiling activity.
- The risks associated to profiling and tracking, i.e. from economic perspective, should be assessed (dissemination of such studies should be supported).

Support policy initiatives in the field and the revision process of Data protection directive

- Clear legal provisions limiting behavior tracking and profiling should be promoted.
- Promoting clear definitions and guidelines in the field, by raise awareness on the data mining techniques and their possibilities to de-anonymize data and profiles (linking this way information that initially are not considered personal data).
Cookies. Some security and privacy considerations

- Collection of data from cookies
  - 78% in ENISA survey

- Cookies
  - Useful in the stateless browser – server HTTP interaction to keep the state
  - Extensively used
  - New type of cookies
    - ie. .lsd (local stored data)
    - Stored outside the browser
    - Able to regenerate deleted cookies

- Privacy concerns
  - Ability to indentify and track users

- Security concerns
  - Vulnerabilities i.e. due to setting

- Legal framework
  - Allows for interpretation
    - i.e. Consent by default

Collection of data from cookies: 78% in ENISA survey

Providers using both persistent and non-persistent cookies: 73%

Only persistent cookies: 9%

Only non-persistent cookies: 18%
Topics for the panel discussions

• More work is needed
  • Clear definitions and guidelines
    ➢ Legal framework and best practices
  • Understanding the economic aspect of personal data protection and disclosure
  • Aligning research to policy initiatives
  • Moving research results in operational environment
    ➢ Focus on the entire picture
      o i.e. not only at application level
Contact

European Network and Information Security Agency

Science and Technology Park of Crete (ITE)
P.O. Box 1309
71001 Heraklion - Crete – Greece

http://www.enisa.europa.eu