Privacy in online services

Rodica Tirtea
rodica.tirtea@enisa.europa.eu

30 March 2011

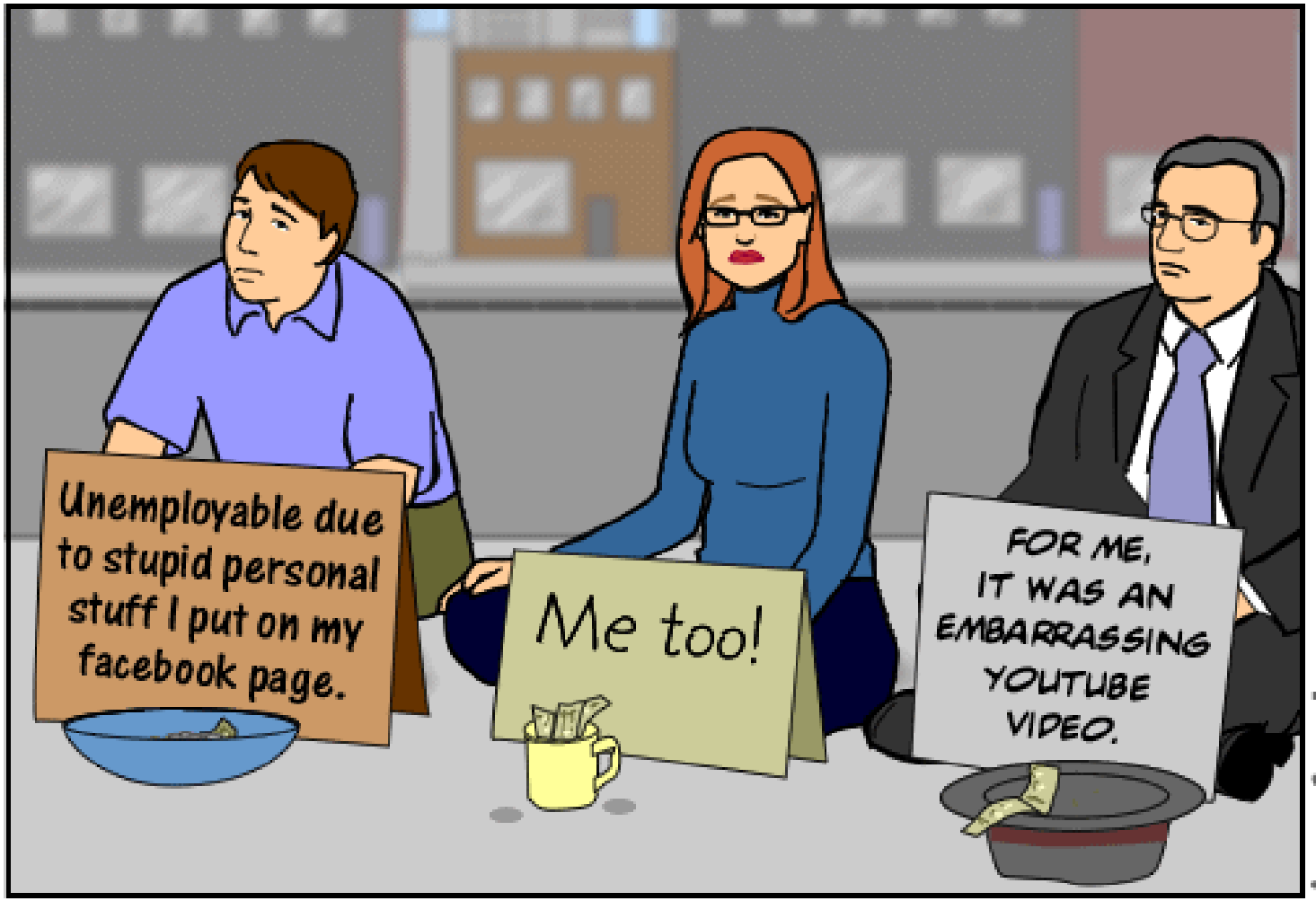
Overview

- Introduction & context of the work
  - About ENISA and its activities in ENISA
- 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

    ➢ http://www.enisa.europa.eu/act/it/library

- Privacy related activities in 2011
- Findings and issues to be further addressed

The Joy of Tech™ by Nitrozac & Snaggy



Privacy, Accountability and Trust – Context

- Internet is open and distributed without authoritative control
- In terms of privacy a number of challenges are posed
  - Data ‘pollution’ - data disseminated without control and is replicated on multiple servers
  - Contrary to humans, data lives forever
    - emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs)
- Contradictory positions
  - governments
    - Demand accountability, data protection, data minimization, better privacy protection
    - But also more access control to data, data retention, lawful interception
  - Users
    - Expressing concerns regarding privacy
    - Willing to drop all of the concerns when a benefit is offered

Context of the work

- ENISA work programme 2010
  - PA1: Identity, accountability and trust in the future Internet
    - New topic
      - Preparatory Action, extended activities in future year(s)
- Results
  - Data breach notification (DBN) study
    - http://www.enisa.europa.eu/act/it/dbn
  - 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
    - http://www.enisa.europa.eu/act/it/pat
    - http://www.enisa.europa.eu/act/it/library/

Data Breach Notification study

- PA 1.1 Study on existing practices in data breach notification (DBN) in various sectors
  - ENISA workshop - 24 January 2011 –"DBN. The way forward"
- More issues to be considered:
  - Define thresholds that will activate the process;
    - Impact in terms of resources at DPA level;
  - Definition of "personal data" differentiation when considered in personal or professional/corporate context.
  - Similarities and differences between sectors (e.g. financial vs. telco).
  - Defined the statement of the Directive "without undue delay";
  - Beyond reporting
    - , is there a need for an audit mechanism?
  - Should DPAs play (would they like playing) the role o
  - the controller or to be outsourced to 3rd parties?
    - What about enforcement?

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
  - Storage 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 study. Findings (I)

- 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
  - A multidisciplinary approach that considers education, policy legal and technological aspects should be supported

Privacy, Accountability and Trust study. Findings (II)

- 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
    - 73% both persistent and non-persistent cookies
    - 9% only persistent
    - 18% only non-persistent

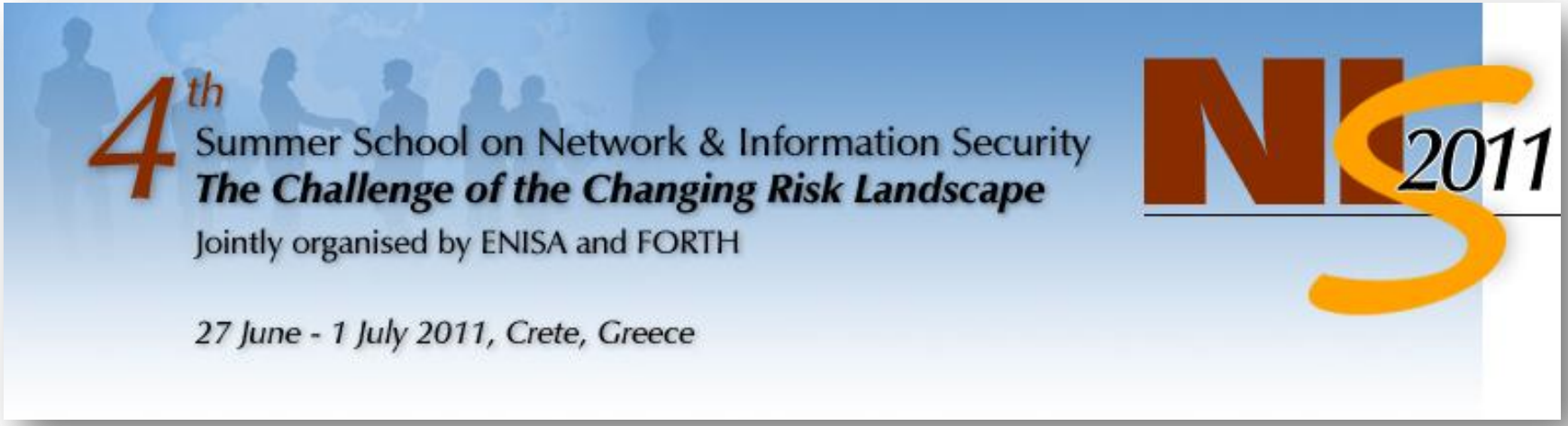
- Cookies
  - Useful in the stateless browser – server HTTP interaction to keep the state
  - Extensively used
  - New type of cookies
    - ie. .lsd (local stored data)
    - Stored outside the browser
    - Able to regenerate deleted cookies
- Privacy concerns
  - Ability to indentify and track users
- Security concerns
  - Vulnerabilities i.e. due to setting
- Legal framework
  - Allows for interpretation
    - i.e. Consent by default

Topics for discussions

- More work is needed
  - Security & privacy should be consider earlier in the design process
  - Multidisciplinary approach: education, training, legal, policy, technology
  - Clear definitions and guidelines
    - ➢ Legal framework and best practices
  - Aligning research to policy initiatives, moving research results in operational environment
    - ➢ Focus on the entire picture
      - i.e. not only at application level
  - Understanding the economic aspect of personal data protection and disclosure
  - Support & promote research & best practices in privacy friendly architectures

➢ http://www.enisa.europa.eu/act/it/library

Summer School on Network & Information Security



www.nis-summer-school.eu