

# Privacy & Trust Activities at ENISA

30th June 2011  
Rodica Tirtea

# ENISA summer school, Thursday, 30 JUNE - Privacy and Trust

- Deploying privacy and trust in operational environments
  - Jacques Bus, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
- ENISA Session on Privacy & Trust
  - ENISA presentation on previous & current work in the field
  - Data breach notifications, Slawomir Gorniak, ENISA
  - Trust frameworks and privacy, Hannes Tschofenig, NSN, Finland
- Minimal disclosure and anonymous credentials
  - Ioannis Krontiris, Mobile Business and Multilateral Security group, Goethe University, Frankfurt, Germany
- A. Economics of privacy & privacy
  - Economics of privacy, Nicola Jentzsch, DIW, Berlin, Germany
  - Research on economics of security, Angelo Marino, European Commission, REA
- B. Privacy & trust in architectures
  - Implementing privacy by design in architectures, Claudia Diaz, K.U.Leuven, Belgium
  - New approaches of digital trust, Abdullatif Shikfa, Alcatel-Lucent Bell Labs, France
- C. NIS in education
- Plenary discussions



- ★ 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

- Introduction & context of the work
  - About ENISA and its activities related to privacy & trust
- 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>
- Findings and issues to be further addressed
- Topics for discussions & Privacy & Trust topics in WP 2011 & 2012

# Privacy is a human right

- *“Everyone has the right to respect for his private and family life, his home and his correspondence.”*
  - Article 8 of The European Convention on Human Rights
    - adopted by states member of The Council of Europe
- *“Everyone has the right to the protection of personal data concerning them”.*
  - Article 16, The Treaty of Lisbon, The Treaty on the Functioning of the European Union states
- *“Everyone has the right to the protection of personal data concerning him or her”  
[..] *“Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.”**
- Article 8, the Charter of Fundamental Rights of the European Union



©2007 Geek Culture

joyoftech.com

# 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 the concerns when a benefit is offered

# Areas of (possible) intervention for ENISA

- On-line services, applications and transactions can assure benefits and competitive advantage for citizens and EU economy;
- The EU requires
  - Advocating and fostering a Pan-European approach to privacy;
  - Proposing new models for trust-establishment;
  - Developing of guidelines for regulatory review and interpretation.
- Areas of (possible) intervention
  - Information/Education - People have to be aware and educated!
  - Policy maker
    - Order to remove contents;
    - Promote availability of subscription based services in addition to free;
    - Avoid online service providers lock-in by fostering user profile portability;
    - Implement Data Breach Notification;
  - Technology
    - Limit data pollution (e.g. minimal disclosure);
    - Limit content's lifetime (e.g. ephemeral communication);
    - Limit data leakage by design (privacy by design)

- 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/>

- 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>

# Privacy & Trust in ENISA 2011 Work Programme

---

- WPK 2.1
  - Security & privacy of Future Internet technologies (partial)
- WPK 2.3
  - Secure architectures and technologies
- **WPK 3.2 - Deploying Privacy & Trust in Operational Environments**
  - **Outcome (Q4 2011)**
    - Report on minimal disclosure and other principles supporting privacy and security requirements
    - Report on trust and reputation models. Evaluation and guidelines
    - Study on monetizing privacy
- **WPK 3.3 - Supporting the implementation of the ePrivacy Directive (2002/58/EC)**
- Activities linked to
  - Digital Agenda
    - Policy dimension
  - FI Initiative
    - Research dimension

# Some proposal for 2012

- ENISA aims to put forward for the consideration of EU policy makers the use of alternative (subscription free) service models for online services.
- WPK 3.1/WP2012 : Economics of Security – possible considerations
  - Smart metering (FI) and privacy;
  - Economics aspects - impact of different types of secondary information use as well as behavioral impact of data breach notifications;
  - Promoting PETs and their possible economic benefits;
- WPK3.3 /WP2012: Supporting the development of secure, interoperable services
  - State of the art of certification schemes in the EU and beyond.
    - Exploring the feasibility of implementing a pan-European scheme for trustmarks;
    - Identifying criteria and levels of certifications for trustmarks;
- Activities in collaboration with EC (DG JUS, etc), supporting actions of the Digital Agenda for the EU.

# ENISA summer school, Thursday, 30 JUNE - Privacy and Trust

- Deploying privacy and trust in operational environments
  - Jacques Bus, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
- ENISA Session on Privacy & Trust
  - ENISA presentation on previous & current work in the field
  - Data breach notifications, Slawomir Gorniak, ENISA
  - Trust frameworks and privacy, Hannes Tschofenig, NSN, Finland
- Minimal disclosure and anonymous credentials
  - Ioannis Krontiris, Mobile Business and Multilateral Security group, Goethe University, Frankfurt, Germany
- A. Economics of privacy & privacy
  - Economics of privacy, Nicola Jentzsch, DIW, Berlin, Germany
  - Research on economics of security, Angelo Marino, European Commission, REA
- B. Privacy & trust in architectures
  - Implementing privacy by design in architectures, Claudia Diaz, K.U.Leuven, Belgium
  - New approaches of digital trust, Abdullatif Shikfa, Alcatel-Lucent Bell Labs, France
- C. NIS in education
- Plenary discussions

# Data breaches notification



- ENISA active in this area since WP2010;
- Currently a Working Group is formed with representatives from:
  - Industry,
  - EC (DG JUS, INFISO, SecGen, EDPS),
  - EU DPA's and Art.29 representatives.
- First meeting of the WG held last May agreeing on outline of work and milestones;
  - ENISA has also circulated to the group a skeleton of the various sections in order to 'start the process';
- Next meeting of the WG scheduled for July the 4<sup>th</sup> at Brussels;
- Next milestone producing by mid-July an executive summary that will serve as input to the online consultation of INFISO B1;
- **WPK 3.2 / WP 2012 Security governance:**
  - Facilitating Information Exchange. Art29 opinion (point 20) that the WP 29 will create a platform to exchange views on security breach with ultimate goal to provide advice to the Commission;
  - Extending beyond the eComms Sector;

# 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
- [www.enisa.europa.eu](http://www.enisa.europa.eu)

# ENISA summer school, Thursday, 30 JUNE - Privacy and Trust

- Deploying privacy and trust in operational environments
  - Jacques Bus, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg
- ENISA Session on Privacy & Trust
  - ENISA presentation on previous & current work in the field
  - Data breach notifications, Slawomir Gorniak, ENISA
  - Trust frameworks and privacy, Hannes Tschofenig, NSN, Finland
- Minimal disclosure and anonymous credentials
  - Ioannis Krontiris, Mobile Business and Multilateral Security group, Goethe University, Frankfurt, Germany
- A. Economics of privacy & privacy
  - Economics of privacy, Nicola Jentzsch, DIW, Berlin, Germany
  - Research on economics of security, Angelo Marino, European Commission, REA
- B. Privacy & trust in architectures
  - Implementing privacy by design in architectures, Claudia Diaz, K.U.Leuven, Belgium
  - New approaches of digital trust, Abdullatif Shikfa, Alcatel-Lucent Bell Labs, France
- C. NIS in education
- Plenary discussions