

Privacy, Accountability and Trust – An EU perspective

SMARTEVENT'10

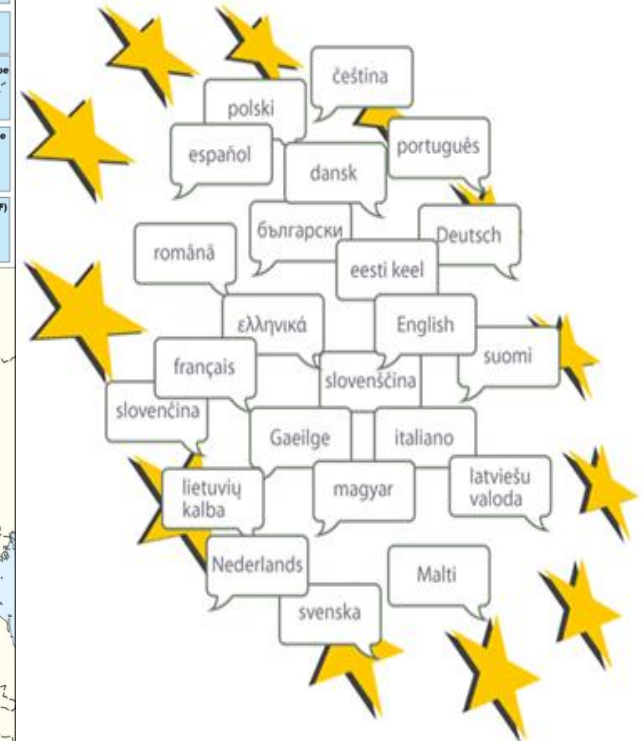
September 21-24, 2010, Sophia-Antipolis, France

Udo Helmbrecht
Executive Director
European Network & Information Security Agency - ENISA

500 Million people in 27 Countries



23 languages



ENISA
Heraklion, Crete

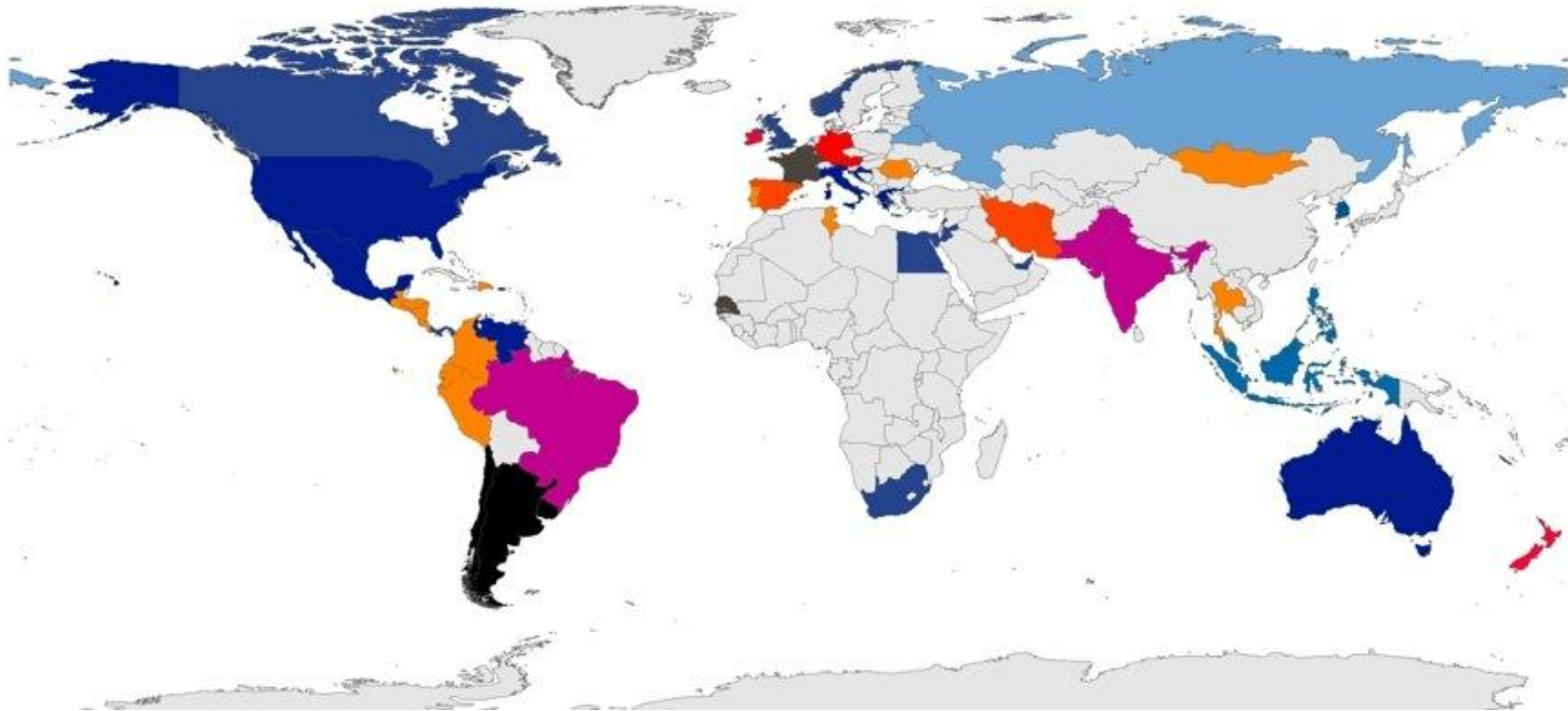
ENISA Overview

- ★ The European Network & Information Security Agency (ENISA) was formed in 2004, employs around 65 experts.
- ★ Develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market.
- ★ The Agency is a *Centre of Expertise* that supports the Commission and the EU Member States in the area of information security.
- ★ We facilitate the exchange of information between EU institutions, the public sector and the private sector.

The world map of social networking for 2010 (in millions of users)



Popularity of social networking websites in different countries



The problem(??)

- ★ Internet is open and distributed without authoritative control;
- ★ In terms of privacy two challenges are mainly posed:
 1. Data ‘pollution’
 - Data are disseminated without control and
 - Replicated on multiple servers and Peers;
 2. Contrary to humans, data lives forever
 - Examples in the WWW: emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs);
 - Retroactive disclosure of data has become commonplace (hackers, legal actions,...).



©2007 Geek Culture
joyoftech.com

ENISA's strategy

- ★ On-line services, applications and transactions can assure benefits and competitive advantage for citizens and EU economy;
- ★ This cannot be achieved without
 - ★ safeguarding the integrity of the information,
 - ★ Protecting the source of information,
 - ★ the genuine authentication (of entities or data, where required),
 - ★ establishment of trust (with persons, as well as objects and actuators) and
 - ★ protecting the personal data and securing the privacy of the individuals.
- ★ 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;
- ★ Technology
 - ★ Limit data pollution – Limiting the amount of data in exchange limits the potential for leakage (e.g. minimal disclosure);
 - ★ Limit content's lifetime;
 - ★ Limit data leakage by design (privacy by design) by introducing more traceability;
- ★ Some examples follow...

Monetising Privacy

- ★ Important ‘horizontal’ area of work supporting all activities in Privacy and Trust;
- ★ Until today most online service offers are offered for free with their business model being based on targeted advertising.
- ★ In the Future Internet it is important to establish confidence and trust between the EU citizens, businesses and the services offered.
- ★ This will be achieved through:
 - ★ sharing of revenues among all actors of the business chain and
 - ★ ensuring that users maintain full control over the ownership of their data within networked systems.
- ★ Assessing what is a *fair price* of a user’s profile and how this may vary if considered as part of a group (‘bargaining power of individual’) are important elements supporting this work as well as of policy makers in this area.
- ★ ENISA aims to put forward for the consideration of EU policy makers the use of alternative (subscription free) service models for online services.
 - ★ As examples prepay or subscription based systems will be considered.

EU policy background & International R&D agenda

- ★ European Commission strategy for a European Digital Agenda aiming to
 - ★ maximise the potential of Information and Communications Technologies (ICTs)
 - ★ Drive job creation, sustainability and social inclusion, and
 - ★ contribute to the overall goals of the Europe 2020 strategy
- ★ The Future Internet (FI) Assembly (FIA) and Private Public Partnership (FI PPP);
- ★ The Research & Innovation on Security, Privacy and Trustworthiness in the Information Society (RISEPTIS) report, notably the conclusions of the Conference on 'Trust in the Information Society', February 2010;
- ★ Directive 2002/58 on Privacy and Electronic Communications (ePrivacy Directive);
- ★ The EU Telecoms Package Reform;

Challenges for the policy maker

- ★ Today's regulatory model is more reactive than proactive;
 - ★ It addresses the eComms Sector (i.e. telco model) ignoring the latest developments;
 - ★ Need to avoid regulating the past;
- ★ Policy maker needs to evaluate the fraction of 'functionality/privacy';
- ★ Most of the possible initiatives in the area of Privacy and Trust (e.g. regulatory mandates for subscription based services, user profile portability) require first an evaluation of the underlying privacy economics;

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>

