The European Network and Information Security Agency – An overview of the Digital Security Agenda in the EU

Demosthenes.Ikonomou@enisa.europa.eu

6th IT STAR Workshop on Digital Security

Bratislava, 30 March 2012

About ENISA

(European Network and Information Security Agency)

- Created in 2004
- Located in Heraklion / Greece
- Around 30 Experts (total number of staff ~55)
  - Centre of expertise
- Supports
  - EU institutions and
  - Member States
- Focus on prevention and preparedness
- Facilitator of information exchange
  - EU institutions,
  - public sector and
  - private sector
- Has an advisory role
  - the focus is
    - on prevention and preparedness
  - for NIS topics

Activities

- The Agency's principal activities are as follows:
  - Advising and assisting the Commission and the Member States on information security.
  - Collecting and analysing data on security practices in Europe and emerging risks.
  - Promoting risk assessment and risk management methods.
  - Awareness-raising and co-operation between different actors in the information security field.
- Areas of interest:
  - CERT;
  - CIIP;
  - Risk management, risk assessment;
  - Privacy, Accountability and Trust;

Snapshot of ENISA's Work Program for 2012

- **WS1 – Identifying & Responding to the Evolving Threat Environment**
  - WPK 1.1: Emerging Opportunities & Risks
  - WPK 1.2: Mitigation & Implementation Strategies
  - WPK 1.3: Knowledge Base
- **WS2 – Improving Pan-European CIIP & Resilience**
  - WPK 2.1: Further Securing EU's Critical Information Infrastructure and Services
  - WPK 2.2: Cyber Exercises
  - WPK 2.3: European Public Private Partnership for Resilience (EP3R) WPK 2.4.: Implementing Article 13a
- **WS3 – Supporting the CERT and other Operational Communities**
  - WPK 3.1: Support and enhance CERTs operational capabilities
  - WPK 3.2: Application of good practice
  - WPK 3.3: Support and enhance cooperation between CERTs, and with other communities
- **WS4 – Securing the Digital Economy**
  - WPK 4.1: Economics of Security
  - WPK 4.2: Security governance
  - WPK 4.3: Supporting the development of secure, interoperable services

Information Security / Cybersecurity

- From a technological perspective, there is little that separates classical information security from Cybersecurity.
- Cybersecurity is about securing data and systems in the global environment. It is just the perspective that changes.
- Adopting this point of view, Cybersecurity is by definition a global concern.
- Due to the nature of the problem, advances in Cybersecurity are most likely to be achieved through political cooperation.

The Basics Are Still Valid

- What we have already learned remains valid.
- It's still all about securing how people interact with process and technology.
- Fundamental principles still apply:
  - Defence in depth.
  - The need for End-to-End security….
- The same methods and tools will be used:
  - Risk management.
  - Policy → Control Frameworks → Processes + Tools.
- There is a risk of reinventing the wheel.

So What is New?

- Information security can be implemented locally, cybersecurity is a shared responsibility.
- An effective approach to Cybersecurity will require a coherent policy approach at the international level.
- In addition, there is clearly a need to align the strategy and goals of different communities.
- In resolving both issues, it will be necessary to carefully balance the needs of the public and private sectors.

Aligning Communities

- The barriers to achieving a common approach to securing information are sometimes stronger between communities than they are between nations.
- It is critically important to align the goals and approaches of different communities:
  - Public domain and commercial entities.
  - Military organisations.
  - Law and Enforcement agencies.
  - Intelligence services….
- The Treaty of Lisbon has opened the door…
- But, what about the governance issues…

Conditions For Success

- Everybody must be involved.
  - All actors understand the role they are expected to play and are sufficiently knowledgeable to perform this role.
- Actions performed by the different actors must be mutually reinforcing.
  - This is the principle of defence in depth.
- The approach must be sufficiently scalable and flexible to cope with rapidly evolving constraints.
  - Approaches that are too rigid and that cannot adapt to changes in the socio-economic environment will not survive.

The Key Instruments/Issues that also need to be addressed

- High level policy statements, such as the Digital Agenda and the Internal Security Strategy.
- European Directives, such as the Data Protection Directive (95/46/EC).
- National laws – which may come about as a result of transposing a Directive.
- Standards – produced by international, European and national standards organisations.
- Good practice – developed by practitioners.
- Promoting awareness and training at all levels.

Prevention vs. Execution

- We should distinguish between prevention and execution at the European level.
  - Institutions/agencies such as Europol and Member States agencies fight cybercrime in an operational manner.
  - Agencies like ENISA work on prevention and probably in the future “civil” detection (i.e. early warning) and supporting other agencies in the area of law enforcement.
  - Collaboration or Service Centres for special tasks could be build between agencies, e.g. ENISA and Europol including MS’s agencies.

Concluding remarks (part 1)

- ENISA's core business is to facilitate dialogue:
  - Between Member States, Between the EU institutions and the Member States, Between the public and the private sector.
- We will support the Commission and MS in formulating Cybersecurity policy.
- We are ideally placed to facilitate the exchange of information between different communities.
- As an Agency that deals extensively with good practice, we can also help industry face the day-to-day challenges of the changing threat environment.

Privacy and Trust

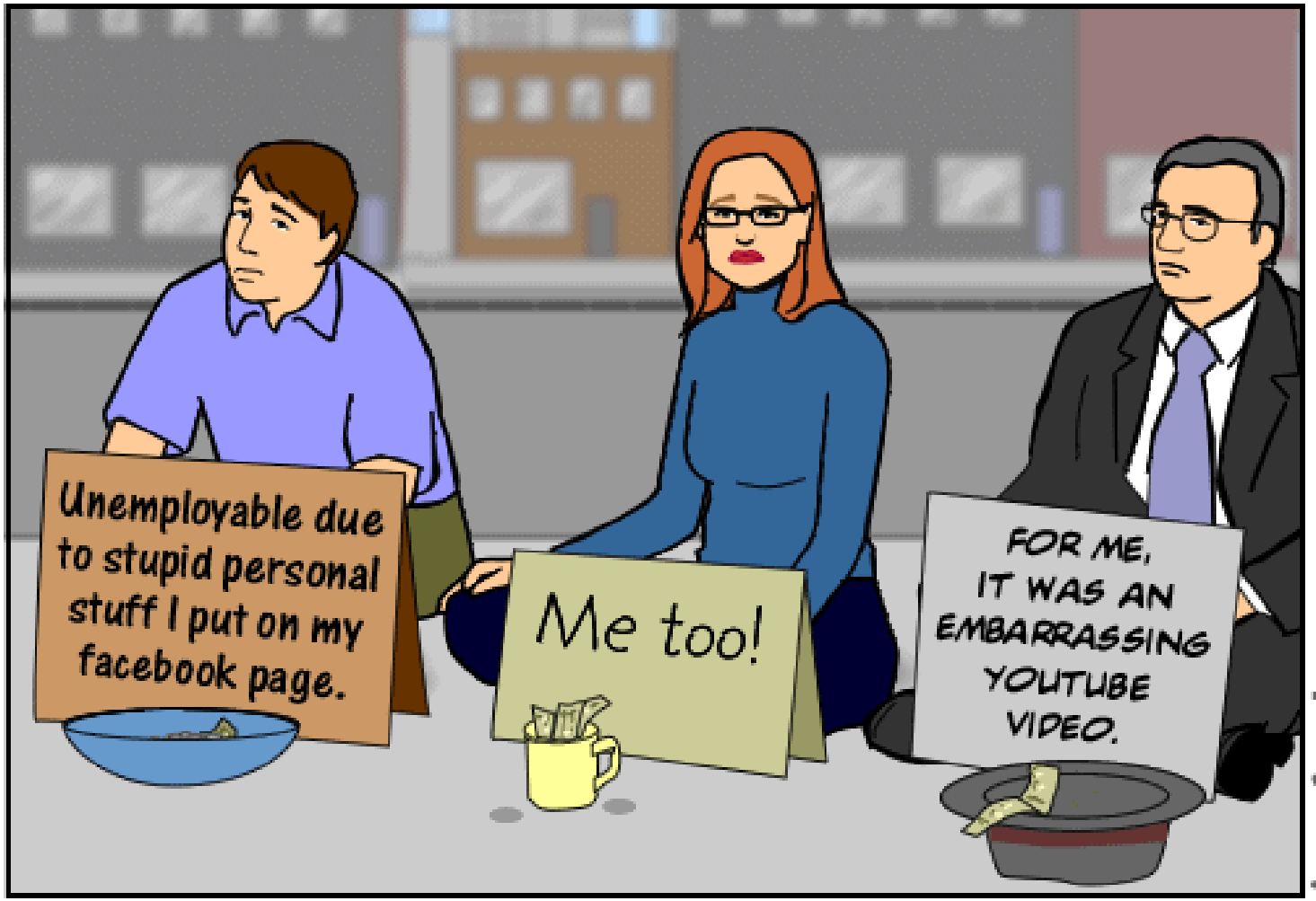
- Privacy is about handling of data about or of persons according to accepted social norms,
  - valid in a particular context;
- Privacy & Trust need joint consideration of technology with
  - social science;
  - economics, ethics;
  - law and other disciplines;
- Needs to be addressed from a pan-European perspective;

The problem(??)

- Internet is open and distributed without authoritative control;
- In many cases, service providers need to collect **some** data in order to better dimension their services;
- In terms of privacy a number of challenges are posed:
  1. Data 'pollution'
     - Data are disseminated without control and
     - **Replicated** on multiple servers and Peers;
  2. Contrary to humans, data lives forever
     - emails (not only web mail), social networking sites, online collaborative spaces (e.g. Google docs);
- In 2010 ENISA introduced a new area of work on Privacy, Accountability and Trust;

The Joy of Tech™

by Nitrozac & Snaggy



Areas of (possible) intervention

- Information/Education
  - People have to be aware and educated!
  - However, remember the example of the car industry (100+ years)
    - Safety as a competitive advantage;
    - Liability;
- 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) by introducing more traceability;
- Some examples follow…

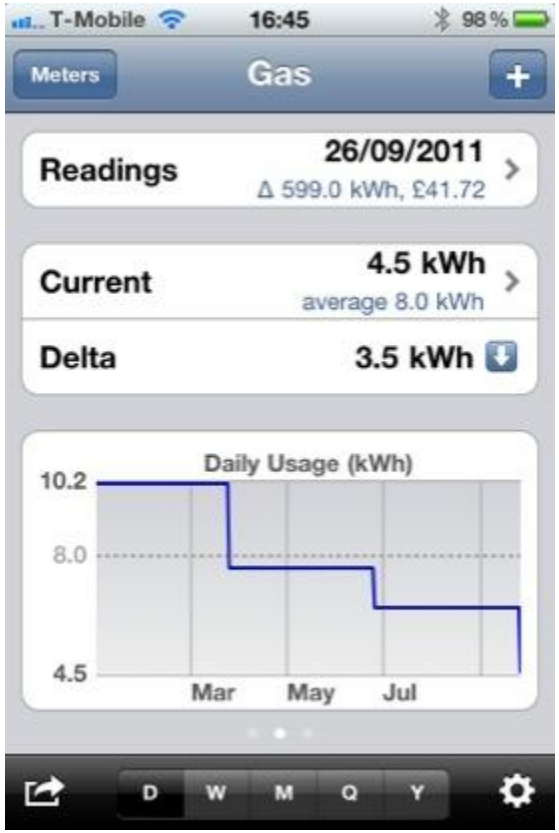
On ephemeral communications

- In such a scenario data owner can easily retrieve its data, and modify them if necessary;
- Some existing services partially implement this paradigm:
  - With Youtube, you watch video without downloading them (video streaming)
  - With Skype Chat service, a user can modify its past conversations.
- Researchers are working towards generalizing this paradigm to all Internet services (email, forum, web, social networks,..).
- Not a complete solution to Internet Privacy Issues
  - it does not prevent Google from collecting data from users;
  - Other solutions are also required (anonymizing network, e.g.TOR, encryption, minimal disclosure, etc.).

[ref] Owner-Centric Networking: A New Architecture for a Pollution-Free Internet
[source] INRIA

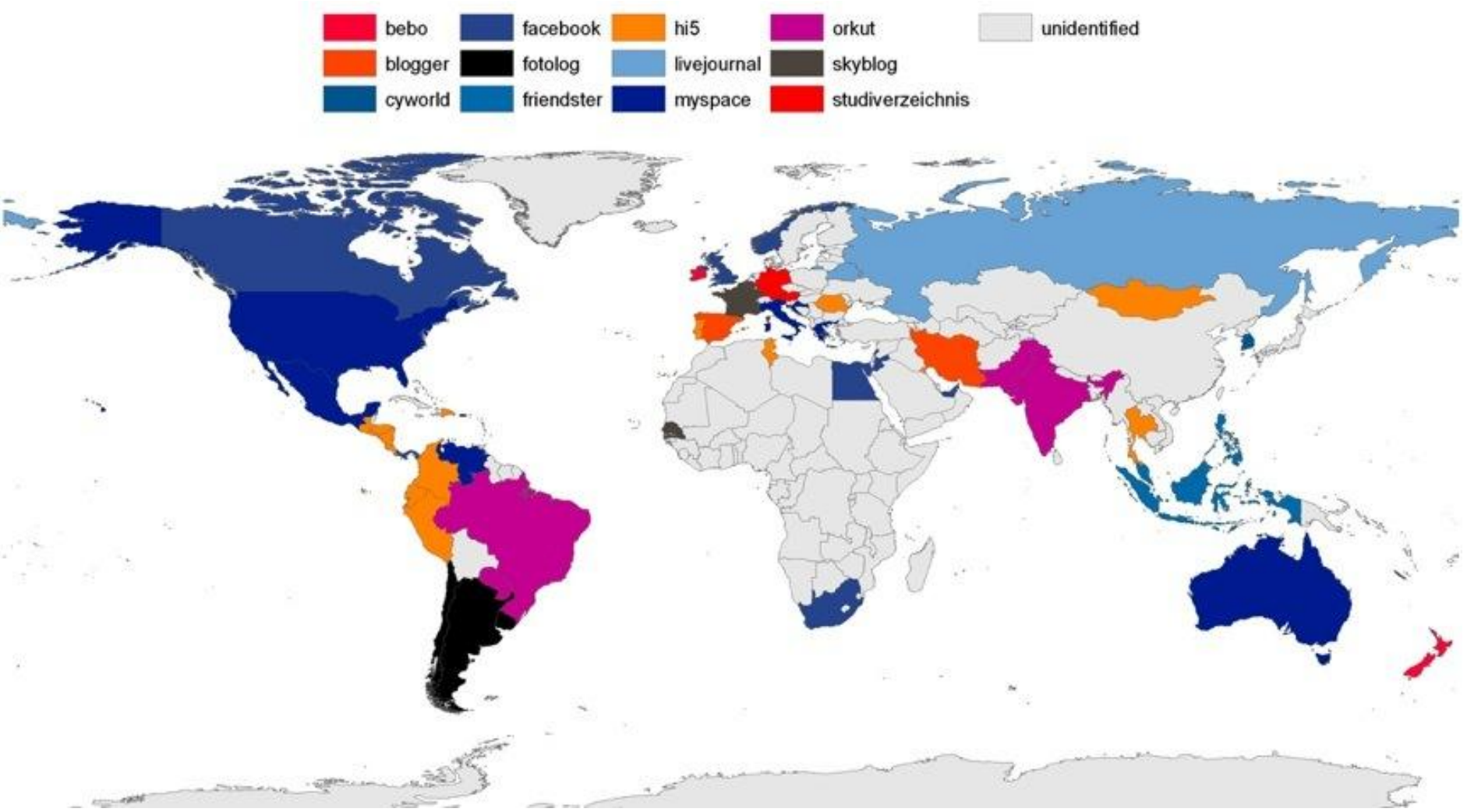
FI applications introduce new challenges

- Smart grids / metering;
- Sensor Networks;
- How can we trust a sensor reading?



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

Popularity of social networking websites in different countries



On Privacy by Design

- Widely used definition/term in recent years;
- Received support by data protection policy makers (FTC, EC Communication on ‘A comprehensive strategy on data protection in the European Union’);
- Privacy needs to be taken into account from the systems development stage, however
  - it is not clear how this can be translated into network design;
- We also need to accept the existence of a plethora legacy networks (3G, 4G, WiFi, GPRS, etc.);

Concluding Remarks (part 2)

- Private data are considered a competitive advantage;
- Difference of privacy perception across EU MSs;
- Lack of co-ordination at EU level;
- Regulations re-active than pro-active;
- Regulators are not yet prepared (e.g. EU MSs DPAs size);
- Perception of privacy risks depends on the users age group;

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