Πανεπιστήμιο Αιγαίου

Κανονιστικές και Κοινωνικές Διαστάσεις της Κοινωνίας της Πληροφορίας

Privacy by….. Design

Λίλιαν Μήτρου (L.Mitrou@aegean.gr)

Αναπληρώτρια Καθηγήτρια

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ
2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

cc BY NC ND

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ
2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Structure

- Privacy and Informational privacy
- Data protection
- Law and technological challenges
- Privacy Enhancing Technologies
- Privacy by/ in Design
- Privacy by Default
- Right to be forgotten (and right to be forgotten)

Security

- Information security: preservation of confidentiality, integrity and availability of information
- Information Systems security refers to the protection of all elements constituting an IS (i.e. hardware, software, information, people, processes)
- Security is not a pure technical issue!

Security and Privacy

- An attack may not necessarily breach confidentiality or privacy of the data
- Adequate security protects more than just privacy; it also protects the integrity and availability of information resources
- Ensuring data privacy requires implementing adequate security measures and introducing security mechanisms including authentication, secure access control, encryption and security management practices

Privacy Invasive Security?

- Inherent tension between privacy and security. Security measures are not identified with privacy protective and enhancing measures
- Anonymity and pseudonymity are not included in any security definition!
- All the current authentication technologies needed for authorisation and accountability of users involve the use of personal information or attributes that can be linked to personally identifiable information
- Risk analysis tools focus on authentication and identification but make no provision to minimise the collection of personal data during these procedures

Technological Challenges/1

- The Data Protection Directive was conceived and adopted before the explosion of the Internet and its impacts on economy, society, life
- Technological and social phenomena pose crucial challenges for data protection
  - Convergence of the network around a single interoperable platform
  - Appearance and explosive growth of the “semantic web” and Web 2.0
  - Changes in identification and authentication techniques
  - Identity management and profiling
  - RFIDs and geo-location devices and applications
  - Cloud computing and globalisation of processing

Technological Challenges/2

- Ambient intelligence: through technology and network into day-to-day life
- ICTs: ubiquitous and autonomous systems
- Information society no longer a parallel environment where individuals can participate on a voluntary basis, but an integrated part of our everyday lives

Technological Challenges/3

- BIG DATA and “The data deluge” ! Computer processing power and computer storage capacity have continued to follow Moore’s Law
  - Shift from quantity to quality: There is virtually no limit to the amount of Information that can be recorded and there is virtually no limit to the scope of analysis that can be done.
- Temporal shift: stored virtually forever – at least longer than the circle in which processing was legitimate
  - In connection with the wide availability this persistency undermines the principles of purpose limitation and proportionality or the rights of individuals, like the right to oblivion
- Spatial shift: Location and distance has little or no impact on the availability, accessibility and processing of information.
  - Vast quantities of personal data move between jurisdictions.
  - Data - or “lost ? - in the clouds…..

Legal Challenges

- Can the current European regulatory framework be effective in
  - an environment of ubiquitous computing, profiling, user generated content and social networks, internet of things
  - in a new environment, where traditional dichotomies for space, person, and time are easily deconstructed?
- Technological evolution may require legal protections of privacy to evolve.
- The current data protection regime in Europe needs to be reviewed and rethought.
- Several approaches to choose -Discussions of the instruments are (sometimes) partisan, reflecting, for example, preferences for or against state control and pressures for self-regulation or for technological solutions.
- Defining the options, designing the instruments, considering the involved actors, users individuals is not a dispassionate technocratic process but a political process.

Global standards?

- Broad applicability of EU law
- Transfer to third countries on the ground of adequacy decisions
- A cumbersome and slow procedure: app. 130 years for only 78 potential adequacy candidate countries to be "audited" and considered adequate
- Madrid Resolution: a Joint Proposal on International Standards adopted by the International Conference of Data Protection and Privacy Commissioners on 6 November 2009 considers international standards as indispensable
- Draft of a global standard, which brings together all the approaches possible in the protection of personal data and privacy, integrating legislation from five continents
- Concerns about the level of protection: a high level or a lowest common denominator?

Is Law enough?
Privacy by technology ?

- Rules and principles alone cannot guarantee adequate protection
- Privacy cannot be assured solely by ex-post compliance with regulatory frameworks and "ticking off" compliance boxes
- *Privacy Enhancing Technologies*
  - to reduce the risk of contravening privacy principles and legislation
  - to minimize the amount of personal data
  - to provide individuals with control over their personal information

Privacy Enhancing Technologies

- PETs as a system of technological measures that minimize or eliminate the collection of data, without damaging the system itself
- The term PETS should be reserved for technological systems that are intentionally developed to promote privacy
- We should distinguish PETs from respectively security enhancing technologies (i.e.mechanisms aimed primarily at ensuring the confidentiality, integrity and/or availability of data/information (though not necessarily in order to promote personal privacy) and from patterns of mere behaviour , though there are considerable overlaps

- PETs have been described as Technical and organizational concepts that aim at protecting personal identity (Burkert, 1997). Burkert differentiates between four different PET functionalities:
- 1. Subject-oriented PET: aim is to anonymise a data-subject or to offer a pseudo-identity
- 2. Object-oriented PET: aim is to conceal what is exchanged
- 3. Transaction-oriented PET: aim is to conceal occurrence of a transaction
- 4. System-oriented PET: any combination of the three previous orientations

- Four different functionalities of PET are discerned (Cvrcˇek and Matya´sˇ, 2007):
- 1. anonymity (the state of being not identifiable within a set of subjects);
- 2. pseudonimity (being pseudonymous is the state of using a pseudonym as ID);
- 3. unlinkability (of two or more items of interest (e.g. subjects, messages, . . .) means that
- within the system from the attacker's perspective, these items are no more and no less
- related after his observation than they are related concerning his a priori knowledge); and
- 4. unobservability (the state of items of interest (IOIs) being indistinguishable from any IOI (of the same type) at all).

PETs, Security and User Empowerment

- Individuals should be placed in a position in which they are able to determine the use of technical and organizational protection tools themselves
- User empowerment as an alternative to protective regulation?
- The main objection to relying on user empowerment is simply, that PET’s as a tool to fend for himself/herself are often and simply difficult to use.

PETs as PITs?

- PETs can be Privacy Invasive Technologies?
  - Level of Privacy (pseudonymity where anonymity is arguably viable)
  - Character of technological standard setting process (transparency, legitimacy etc.)
  - Context in which PETs are applied and effect of application
- PETs as palliative for the introduction of a PIT *and for the disempowerment of rules and authorities*

Privacy Enhancing Technologies (PET's) instead of law ?

- Emphasis on Information and Awareness
- Self-determination and self-protection through technology
- Privacy à la carte?
- The myth of user empowerment: knowledge gap and market driven solutions

Shortcomings of PETs

- Limited use/limited success
- Limited by technological advances in privacy-invasive technologies and practices
- Not compulsory
- Not widely adopted
- More holistic approach: emphasis on the effort to address privacy concerns in all stages of systems development

From PETs to Privacy by Design

- *New tools, concepts and principles*
- Value sensitive design
- Proactive and social responsible design
- Normative design
- Privacy by Design: privacy and data protection embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal

Privacy by design
a definition

- PbD aims to identify potential privacy risks early in the design process of an ICT service/system and aims to avoid or minimise these risks, by embedding privacy and data protection within the entire life cycle of the service – from the early design stage to deployment, use and disposal (ICO, 2008)

- *Privacy by design means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal* [digital agenda]
- Privacy by design focuses not only on technological solutions, but requires accountable and privacy-friendly organisational practices and privacy-friendly physical design and infrastructure

- Issues to be clarified
  - integration into technological artifacts,
  - evaluation of its cost and effectiveness
  - impacts and implications for individuals, systems and organizations are open to discussion.
- the focus of the design context necessarily becomes the control of technology

Privacy by default

- Therefore it is crucial that the default settings offer a high level of privacy protection.
- Engineering specifications should embody policies for data protection
- Specific rules should be envisaged to impose "**privacy by default**" settings in a number of areas, such as RFID-applications and social networks