INFORMATIONAL

SELF DETERMINATION IN AN INFORMATION SOCIETY – Privacy new challenges

SAO PAULO – Oktober 2011

Liberties in the Information Society

Professor Rector Yves Poullet (yves.poullet@fundp.ac.be)

Centre de Recherche Information, Droit et société (http://www.cridss.be)
University of Namur
Belgium

Table of Content

1. Technological Landscape and Actors

2. Towards a new generation of Data Protection Legislation? New scope, new principles, new rights, new alliances.

3. Conclusions

I. Technological Landscape

A. Characteristics of the « new » Information systems : between Tera and Nano

TERA: Tremendous increasing capacity

- **Ability to store speech, data, images or any combination: convergence of all networks (Cable TV, wifi, Mobile phone, …)**
- **Increasing capacity as regards the transmission (10Kb/sec.)**
- **Increasing capacity as regards the processing (Moore's Law)**
- **Increasing capacity as regards the storage capacity**

-> E.g. the desktop computer bought at the supermarket

Year	**1987**	**2007**	**2020 (x1000)**
Processor	**8 Mhertz**	**3 Ghertz (x 375)**	**3 TeraHz**
Memory	**640KB**	**512 MB(x 800)**	**512 Gbytes**
Hard Disk	**20 Mbytes**	**120 Gbytes (x 6000)**	**120 Terabytes**
Phone conn.	**10Kb/sec**	**3 Mb /sec**	**10 Gb/sec**

Consequences

- **Bruce Schneier is speaking about an individual life recorder**
- **Easy to store the National Register of Belgium on a DAT tape (big matches box)**
- **Possibility to record all outcoming international communication (phone/fax) with publicly available equipment (cfr Echelon)**
- **A single hard disk is nowadays sufficient to record all the words pronounced by a human being since his birth to his death (continuous speech during 80 years, 8 hours a day)**

CONSEQUENCE 1 : TO REGISTRATE THE « LIFE » OF ALL INDIVIDUALS BECAME MORE AND MORE POSSIBLE AND AT REASONABLE COSTS (Concept of Lifebraries)

- **NANO : Multiplication of terminal devices (as regards their mobility and their size): Ubiquity of terminals (GPS, RFID, Mobiles, etc…)**

B. New applications

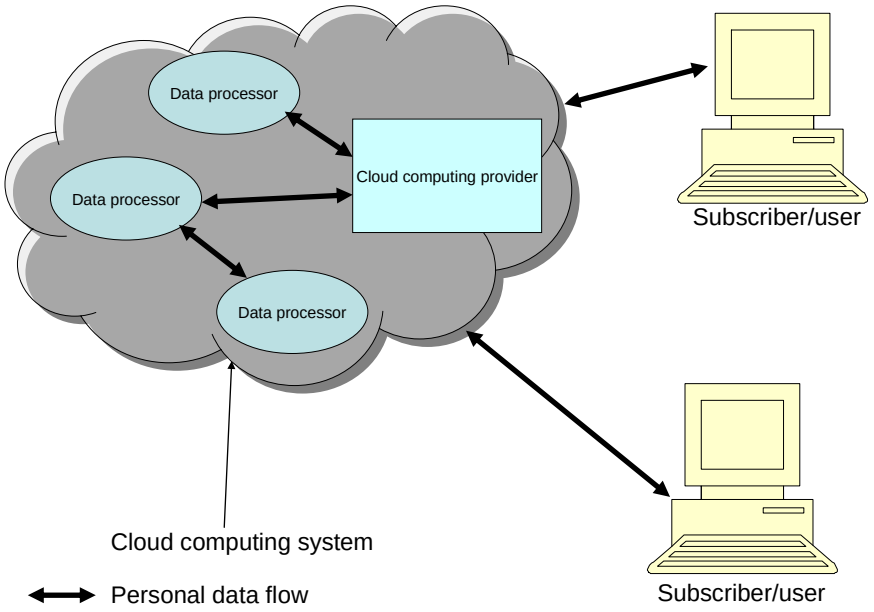
New ways of data collection

- **Web 2.0 platforms** (You Tube, Social networks): Extimacy: towards lifelogs…recording multiple events of my daily life including the life of my « friends »
  1. Opaque functioning…one to one publicity/ tags/ …
  2. Is consent a legitimate ground for processing by Web 2.0 platforms?

- **Ambient intelligence** (RFID, Bodies implant,…): *"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it."* (Weiser, 1991)."At the next level we find the elements of the real world around us. Currently we do not interact with them but in future we will expect that they take notice of us, that they start to interact with us and turn into personalised items rather than general purpose devices".
  1. Ubiquity of ICT technology
  2. Opacity of their functioning
  3. What's about the tags' security.

New applications (2)

New ways of data storage: the cloud computing: *cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider*



C. New methods of data processing

- **Profiling : a method using three steps**

  1. DATA WAREHOUSING

  – Collect and store anonymous, coded or not « slices of life ».(biographical data;: colour of the car, place of residence, average fiscal revenue of the residents of my street, types of purchasing goods, webpages visited, etc).

  2. DATA MINING

  – Create statistical correlations between individuals characteristics recorded to deduce inference rules = building up of profiles

  3. PROFILING OF INDIVIDUALS

  – Apply that profile to identified or identifiable individuals in order to infer their characteristics….and to take the appropriate action (sending an advertisement or start a control) .

  Consequence: Reductionist approach of the Human

  – Signification given a priori to certain attitudes, movements ... and to the « Statistical truth »
  – Building up of profile apart from a large scale of data captured from different sources and analyzed statistically

  Which objectives? : reduction of uncertainty for economic reasons (one to one marketing or credit evaluation) or for security reasons.

D. New actors

- **Governments have lost the control on the net and its infrastructure**

- **Standardisation of terminals and of communication protocols and more generally Technical ICT standards are defined by Private organization or a consortium of private commercial bodies.**

- **From plain old public postal services to Internet Access providers and Internet gatekeepers (like Google).**

- **New emerging actor : the terminals' producers (in a wide meaning : hardware and software (see EU Directive 99/5))**

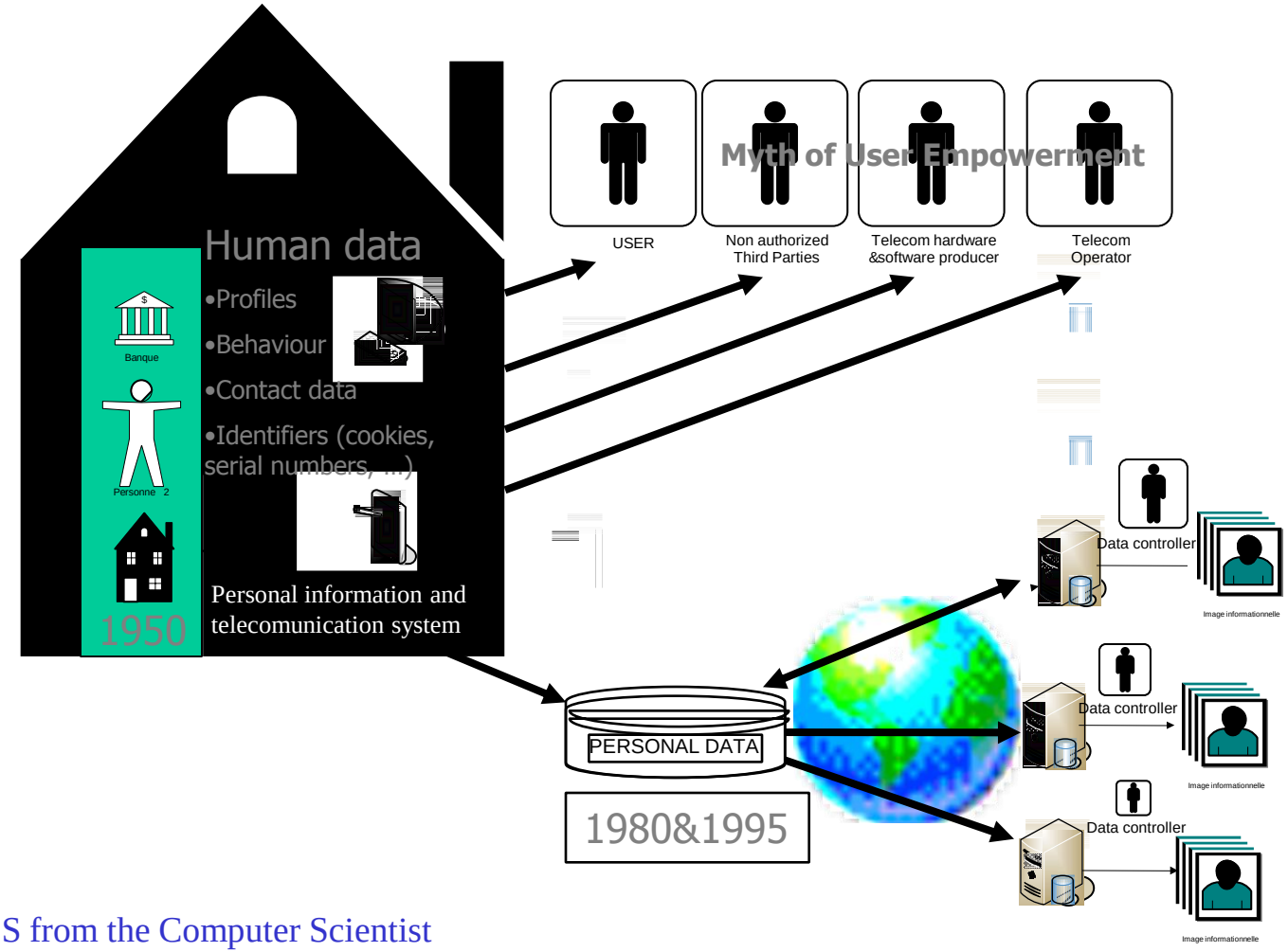
- **Lack of « regulation » regarding those new actors. Privacy legislation remain focused on « data controllers » and does not address the technology in itself. Where are the "technology's controllers" (IT producers or designers) regulated?**

E. New Privacy risks

- OPACITY (The « Trial ») and the risks of « anticipatory conformism » (see BVerfG 1983)
- DECONTEXTUALISATION: data collected in one context might be used in another context (see Google)
- REDUCTIONISM : from individual to his or her data and finally to his or her profile by using data related to other people.
- INCREASING ASSYMETRY (« Big Brother ») between the informational powers of, from one part, the data subject and, from the other part, the data controller…
- TOWARDS A SURVEILLANCE OR OBSERVATION SOCIETY: possibility to forecast or predict a behavior.

II. FROM TECHNOLOGY TO an appropriate LEGAL FRAMEWORK

2011
Towards a new era of data and telecommunication protection



PS from the Computer Scientist

Security = Confidentiality+Integrity+Availability+Auditability

Three Privacy legislations' generations

- 1st generation: Council of Europe Convention (1950) : « **Privacy » as a Right to opacity (sensitive data, home and family protection) . Negative approach. « The right to be left alone » (Warren-Brandeis)**

- 2nd generation : from Conv. C of E.108 (1981) to Art. 8 of the E.U Charter on fundamental rights (2000) and Art. 17 of the Lisboa Treaty : **Data Protection as a new constitutional right beyond Privacy - a way for reestablish a certain equilibrium between the Informational powers of D.C and D.S – Positive approach: Right to self determination (control of the flows of my informational image).**
  - **Enlargement to all personal data**
  - **3 principles:**
    - *. Legitimacy of the processing*
    - *Right to a transparent processing for the DS*
    - *DPA as balance keeper*

Towards a Third Generation ???

- Four main extensions :
  - Enlargement to new data
  - Enlargement to new objects
  - Enlargement to new actors
  - Enlargement to new D.P. objectives

- EU directive on DP in the e-Communication sector (the e-Privacy directive) (Dir. 2002/58 revised in Nov. 2009) might be considered as a first recognizance of this new generation

1. The definition of personal data

❖ **A personal data is a data related to a person who is identified or identifiable notably by mean of an identification number**

1st remark : The need to distinguish between different kinds of personal data

Biographical Data : data linked with events of the individual life

- *E.g. a simple ticket describing the content of a shopping basket*

Anchorage point or identifier of an individual or of an object belonging to an individual and permitting to cross different data bases

- *E.g. The national registration number, the O.N.S. as regards RFID, my fingerprints,…*

Contact data : the data which permits to contact a person

- *E.g. an mobile phone number*

- **Purely conceptual abstraction. Traffic and location data are biographical, anchorage point and contact data**
- **Definitively, contact data and identifier are "sensitive data" in modern Information system (see the controversial debate about the use of IP addresses)**
-

1. The definition of personal data (2)

2. Second remark: are cookies, IP address or RFID numbers necessarily personal data?

Need for a specific regulation of identifiers e.g. RFID placed on a caddie allows the store to send appropriate advertisements through a small screen without need to "identify" the person in the traditional sense but to impact him (see Opinion Art 29 WP on personal data)?

3. Third remark: do we need a regulation on profiling even they are not working with personal data?

The recent Council of Europe Recommendation (Nov. 10, 2010) on that issue and the application of DP principles according to an holistic approach.

2. New objects : Towards a regulation of the infrastructure and terminals

- Preliminary statement: As regards terminals, they are more and more various (from laptop to RFID), ubiquitous (accompanying and revealing all events of our daily life) and functioning in an opaque way permitting to a lot of (third) parties to trace and/or profile the DS even if not directly or indirectly identifiable.

- Principle: « The answer to the machine is in the machine » (Ch. Clarke about IPR violations)

- Certain provisions of the EU e-privacy Directive 2002/58 about D.P. are regulating the terminal equipment.
  - Art. 14 : possibility to impose technical standards in order to impose the compliance of the functioning of the terminal equipments with the D.P. requirements
  - Art. 5.3 : prohibition of any intrusion (spyware, cookies) into the terminal equipment of a subscriber or user of a communication services, except with his or her consent

2. New objects : Towards a regulation of the infrastructure and terminals (2)

Towards two new Data Protection rights

- **Right to see our terminal equipment assimilated to virtual home (see: Terminal considered as a « virtual domicile » to be protected as a private home**
  - Confirmation of this approach by the B.Verf. G hof by creating a new constitutional right (Feb. 27 2008) against online searches by LEA (Trojan horse): The «*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*“ with only few exceptions in case of very serious crimes

- **Right to a transparent and proportionate functioning of the terminals**
  - **Data generated, stored and transmitted by the terminal must be reduced to what is technically necessary for the telecommunication (data minimization) and must be transparent (suppression of chattering).**
  - **Contact points may only be given by the user and further uses of this contact point must remain under the control of the user (right of revocation)**
  - **Terminal may not initiate a communication unless asked to do so by the user or unless this is strictly necessary for the good functioning of the telecommunication network.**

2. New objects : Towards a regulation of the infrastructure and terminals (3)

Four new principles

- **« privacy by design » principle**
  - Definition: to introduce (embedd) into the technological and organisational design of the I.S. the privacy requirement (ex Data minimization)
  - 6 core principles
    - ***Proactive not reactive attitude of the companies and call for the intervention of the standardisation bodies ISO/IEC JTC 1/SC 27: IT/Security techniques/Privacy Framework)***
    - ***Privacy by default***
    - ***Privacy embedded in the design***
    - ***Positive approach: to protect privacy is an asset***
    - ***End to end Lifecycle protection***
    - ***Visibility and transparency for the data subject***
  - Numerous examples: cookies/ blurring of faces/ Identity management/ online access.

3. New objects : Towards a regulation of the infrastructure and terminals (4)

- **Information Accountability Principle**: « Tell me what you are doing and please ensure that what you tell is effective ». From an *a posteriori* approach to an *a priori* approach.
  - Need to define privacy policies
  - Obligation to develop mechanisms ensuring their respect and their control (e.g. through external and internal audits)
  - Obligation to make your policy transparent towards data subjects.

- **« Privacy Impact assessment » obligation** : EU Recommandation on RFID (May 2009) and art. 29 WP's opinion (December 2009) on the Future of Privacy
  - Definition: Obligation for D.C. before implementing a I.S. to produce a document showing the risks of privacy threats incurred by D.S and the choices taken by the DC in order to minimize or avoid these risks.
  - Preventive approach and contradictory discussion about the technological options.

- **Towards a « mutual benefits » principle?:** Since Technology does represent a such advantage for DC to process data more efficiently, technology must also be designed in a way taht does represent an advantage for data subjects (e.g. on line access through cookies, on line access to my profile (see recently Google), etc.)

3. New Actors to be regulated

- Liability of IS designers or Terminal equipment producers and even standardisation bodies (2004 Warsaw Declaration): From liability of data controllers to liability of « IS. designers and terminal equipment producers » **:** the Article 29 W.P opinion on RFID (Jan. 19, 2005) and the EU Commission's Recommendation of May 2009) based on Preamble 2 of the Directive 95/46: « *Data processing systems are designed to serve man: (…) they must … respect their fundamental rights and freedoms, in particular the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of the individuals* ».

- Specific regulation about Public Communications services providers under EU directive 2002/58 revised in 2009:
  - art. 4 and 5 about their duty to provide secure services and ensure confidentiality + new provisions about the obligation to notify subscribers, NRA and DPA serious breaches of personal data
  - art. 6 and 9 about their use of traffic and location data + duties under EU directive on data retention (Feb. 3, 2006)

- What's about a regulation of Gatekeepers (Search engines and Web2.0 platforms)?

4. Reassertion of ethical values

- Dignity: not to be submitted continuously to advertisments, no continuous surveillance, no manipulation

- Social justice= non discrimination and solidarity (EU Parliament: Internet is definitively a public service corresponding to a public need like broad centuries ago)

- Autonomy: individual and collective mastership of my informational environment including the technical one (warning: **CONSENT is not the panacea)**.

5. Need for new alliances

- With environmental law: **Obligation for the legislator to launch 'Privacy impact assessment ' with all stakeholders: the precautionary principle and the essential role of the State (the recent EU Commission Communication (May 2011): « Strategy for the effective implementation of the Charter of fundamental rights by EU »**
- With criminal law : **Privacy Protection and Computer Crime Convention: an alliance (see intrusion into a terminal = hacking)**
- With consumer law:
  - **Class action and Privacy Protection**
  - **Education and awareness of the DS are needed**
  - **The application of consumer Protection legislative provisions to Privacy protection issues (reversal of the burden of proof)**
  - **Objective liability for defective products and non privacy compliant terminals**

Conclusions

- Privacy is a prerequisite for all our liberties (Right to move freely, Right of expression, Right not to be discriminated, etc..)
- Privacy is a condition for a participative democracy
- Privacy defence needs a collective action and a democratic deliberation: What do we want as Information society?