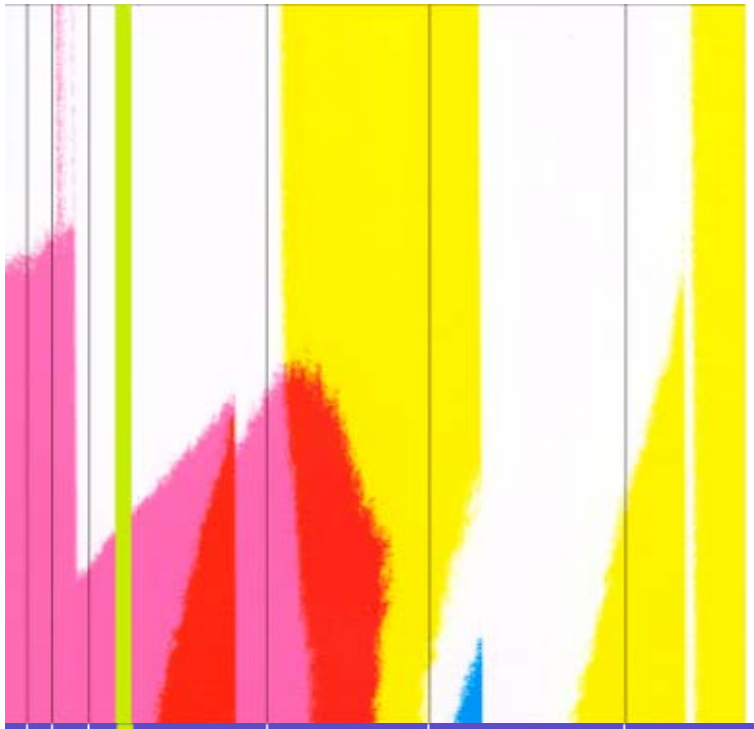

Third PRIAM Workshop

December 6-7 2007

Daniel Le Métayer

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA
RHÔNE-ALPES

December 6

9h15 - 10h: Daniel Le Métayer

Welcome - Overview of the project and objectives of the workshop

10h - 10h45: Joël Moret-Bailly

Efficiency/effectiveness of privacy protection regulations: definition and evaluation

10h45 - 11h : Coffee break

11h - 11h45: Daniel Le Métayer

Towards a privacy specification model

11h45 - 12h30: Jerry den Hartog

A posteriori compliance control

12h30 - 14h: Lunch

December 6

14h - 15h30: Boris Balatcheff, HPLabs Bristol

TPM: fundamentals, main applications and criticisms (talk followed by a discussion)

15h30 - 16h15: Ciaran Bryce

Message quality for security in wireless network systems

16h15 - 16h30: Coffee break

16h30 - 17h15: Frédéric Le Mouël

Trust protocol integrating services' semantics

20h: Dinner

December 7

9h - 10h45: WP parallel working sessions:

- Legal issues and formal models: Joël, Shara, Daniel, Jerry

- Architecture and implementation: Ciaran, Frédéric, Stéphane

10h45 - 11h: Coffee break

11h - 12h00: Ciaran Bryce, Frédéric Le Mouël

PRIAM functional architecture

12h - 12h30:

Wrap up and plans for 2008

Context

PRIAM : Privacy Issues in AMbient intelligence

Partners:

- Inria
- University of Twente
- University of Saint-Etienne

Multidisciplinary project: lawyers and computer scientists

Motivation

Starting point of the project:

- Need to consider the legal issues raised by new technologies

But technology should not necessarily be confined to the role of the villain

- Technology can also be used to protect individual rights

But technology alone will never be enough

⇒ Need for tight collaboration between lawyers and computer scientists

Methodology

Pragmatic approach:

- What is the current state of affairs? Is privacy **effectively** protected today ?

- If not, why ?

- In any case, what is really new with ubiquitous computing with respect to privacy ?

- Considering all the above, what can we do to improve the situation (we = lawyers and computer scientists) ?

Definitions of privacy

Warren-Brandeis: “right to be let alone” (non interference).

Gavison: “secrecy, solitude and anonymity” (limited accessibility).

Westin: “individual determine when how and to what extent information about them is communicated to others” (information control).

Related concepts: rights of personality (honour, image, voice, forgetness, moral author rights, personal integrity, etc.), protection of personal data

Usually considered as a fundamental right even though it is not absolute and its perception varies over times, countries, cultures, individuals, etc.

Current trends from the legal doctrine

- The public/private duality is no longer relevant
- Data protection as an intermediate instrument
- Self determination as the key concept
- From data to knowledge (profiling)

Main European Directives

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.

Directive 2002/58/EC concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Effectiveness - Efficiency

Effectiveness: are the rules really applied (fastened seat belts)?

Efficiency: are the ultimate social goals reached (less victims)?

Regulations can achieve efficiency in different ways:

- Prevention (e.g. engine power limitation)
- Enforcement (e.g. injunctions)
- Deterrence (sanctions)
- Incentives (symbolic value)

Effective regulations can be inefficient

Efficient regulations can be ineffective

Transposition of the European Directives in France: effectiveness

Unambiguous consent, right to access, right to object, no unsolicited communications : in most cases impossible to exercise individual rights whether directly (telecom operators, Internet access providers, banks, state services, etc.) or through the national authority (CNIL) [e.g. the survey conducted by Valérie Sedallian in December 2002]

CNIL figures (2006):

Complaints : 3 600 (about 600% increase in 3 years)

Access right requests : 1500 (about 600% increase in 3 years)

Pending requests: 2 800

Injunctions: 7 (1 per year until 2002)

Number of legal proceedings: 1 per year

Number of sanctions: 11

Controls: 130 (+35%)

Transposition of the European Directives in France: efficiency

Accurateness: average number of erroneous individual records in police files checked by the CNIL in 2006: 54%. How many job applications subject to unfair treatment ?

Awareness: 60% of individuals do not know what CNIL is, 70% feel not well informed about personal data protection. What impact on citizen's life and decisions ?

Other studies (R. Leenes, 2003):

- privacy fundamentalists : 25% (26% in 1995)
- privacy pragmatists: 65% (54% in 1995)
- unconcerned :10% (20% in 1995)

Gloomy situation

Tentative explanations:

- Lack of funding (CNIL: staff of about 100; German Authority : 400; British Authority: 300)
- Lack of concern from citizens
- Security wave
- Technological wave ⇐
- Lack of adequacy of the legal instruments ? ⇐

Current trend : lighter a priori controls, stronger a posteriori controls

Technological front:
Advent of ubiquitous computing

New issues w.r.t. privacy:

- New types of personal information : geographical, physical
- Invisible devices and interactions (anywhere, anytime)

Aggravating factors:

- Multiplicity of exchanges of little pieces of (harmless looking) information
- Dynamic and possibly untrusted (or unknown) environment
- Scarce resources

Legal front:
Adequacy of existing instruments ?

Personal data [Directive 95/46/EC] : *Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*.

Opinion 4/2007 on the concept of personal data [WP 29]: *It is better not to unduly restrict the interpretation of the definition of personal data but rather to note that there is considerable flexibility in the application of the rules to the data.*

Legal front:
Adequacy of existing instruments ?

Opinion 4/2007 on the concept of personal data [WP 29]:

Data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated…

… It is not necessary that the potential result be a major impact. It is sufficient if the individual may be treated differently from other persons as the result of processing such data.

Legal instruments and technological developments: a widening gap

- Very broad definition of personal data: virtually any data can be considered as personal

- Unambiguous consent of the data subject: impossible to implement on a case by case basis in the ubiquitous computing society (already a “virtual” right today)

- Data controller: can be any individual in an ubiquitous computing environment

⇒ Very high level standards but not adequate

How to reduce this gap ?
Suggestions from the legal side

- Need to define priorities: apply a priori controls to the most sensitive data and strengthen a posteriori controls for all data

- Focus more on the quality and the use of personal data than their collection (cf Pierre Trudel, 2006)

- Require data collectors to offer to data subjects automatic means to exercise their rights (access, rectification, erasure, etc.)

- Ensure protection by law of the above tools and sanctions in case of misuse or deceptive behaviour (accountability means and liability of data collectors) ??

- Official privacy certification process for tools (dedicated version of the security “Common Criteria” standard for privacy ?)

- Class actions ?

How to reduce this gap ?
Suggestions from the technical side

PRIAM top-down approach:

- Need to start from a clear definition of privacy policies and requirements ⇒ privacy policy language and formal semantics

- Refinement of the privacy policies ⇒ definition of the implementation means (a priori, a posteriori, technical, organizational, legal, etc.)

- Translation into a natural language to ensure understanding by all parties ⇒ liability, legal contract

PRIAM approach