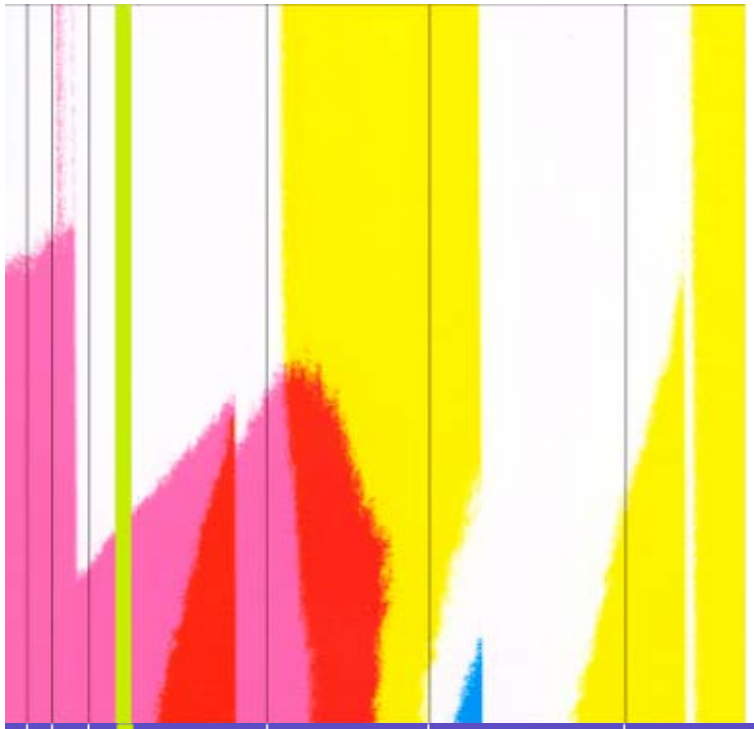

PRIAM
WP1 : Legal issues

Daniel Le Métayer

PRIAM Meeting 20/06/2007

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA
RHÔNE-ALPES

Plan

1. What do we mean by privacy ?

- Definitions
- Principles

2. Regulatory policies

- International instruments (UN, European Union, Council of Europe, etc.)
- National (Europe, USA)
- Comparative study (principles, efficiency)

3. Lessons and questions : legal side

4. Lessons and questions : technical side

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, forgetness, personal integrity (Quebec), etc.
  - Protection of personal data

Principles

Dominant view : benefits for individuals as individuals (“achieving individual goals of self-realization”): autonomy, dignity, trust, etc.

NB: potentially in tension with the need of society.

Privacy is a universal concern but :

- Levels and forms of privacy concerns vary a lot (culture, time, technology, context) even within a single country.

- Sociological factors: interest and loyalties to the group vs value of self-determination.

Regulatory policies

- International instruments (legally binding or not).
- National instruments.
- Guidelines, recommendations, codes of practice (by business sector).

International instruments: United Nations

- Universal Declaration of Human Rights (1948): “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks”.

- International Covenant on Civil and Political Rights (1976): same wording.

- Guidelines Concerning Computerized Data Files (1990): lawfulness, fairness, accuracy, purpose specification, interested person access, non discrimination, exceptions, security, supervision and sanction, transborder data flows.

International instruments: OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:

Motivations:

- Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.

- Automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices.

Definitions:

- "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf

- "personal data" means any information relating to an identified or identifiable individual (data subject).

Principles: limited collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, accountability.

International instruments: Council of Europe

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950):

- Everyone has the right to respect for his private and family life, his home and correspondence (art. 8).
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others (art. 8).
- To ensure the observance of the engagements … thereto, there shall be set up a European Court of Human Rights (art. 19).
- The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation of the rights set forth in the Convention (art. 34).
- The Court may only deal with the matter after all domestic remedies have been exhausted (art. 35).

International instruments: Council of Europe

- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981-1985):
  - Preamble: recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.
  - Art. 5: Personal data undergoing automatic processing shall be:
    - obtained and processed fairly and lawfully;
    - stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
    - adequate, relevant and not excessive in relation to the purposes for which they are stored;
    - accurate and, where necessary, kept up to date;
    - preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

- Council of Europe Recommendations Regulating the Use of Personal Data in the Police Sector (1987), for Employment Purpose (1989), etc.

International instruments: European Union (1/3)

- Treaty of the European Union (1992): incorporates the European Convention for the Protection of Human Rights and Fundamental Freedoms.

- Charter of the fundamental rights of the European Union (2000):
  - Everyone has the right to respect for his or her private and family life, home and communication (art. 7).
  - Everyone has the right to the protection of personal data concerning him or her (art. 8).
  - Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (art. 8).
  - Compliance with these rules shall be subject to control by an independent authority (art. 8).

International instruments: European Union (2/3)

- 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.

- Regulation No 45/2001 (EC) on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies 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.

International instruments: European Union (3/3)

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.

- Two goals: enforcement of privacy rules and harmonization to facilitate flow of personal data within Europe:
  - *… respect their fundamental rights and freedoms, notably the right to privacy…* (preamble)
  - *…require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded…* (preamble)
- *A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.* (art. 29).

  NB: WP recommendations on RFID technology, questions to Google, etc.
- Great influence over countries (non European as well as European): restriction on data flow towards countries which do not provide adequate levels of data privacy).

National instruments: Europe (1/4)

Focus on transposition of Directive 95/46/EC in members of EU

Personal data in the Directive: *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*.

- Belgium: verbatim translation.
- France: consider all the identification means available to the controller, or that can be accessed by the controller or any other party.
- United Kingdom: data which relate to a living individual who can be identified from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

National instruments: Europe (2/4)

- Data should be
  - Processed for legitimate purpose
  - Adequate, relevant, not excessive
  - Accurate, up to date
  - Kept for no longer than necessary

- Unambiguous consent of the data subject (with derogations: contractual or legal obligations, vital interest of the data owner, legitimate interest of the controller provided the fundamental rights of the data owner are not jeopardized).

- More stringent constraints for sensitive data (about ethnic origins, religion, political opinions, health, etc.): prohibition by default.

National instruments: Europe (3/4)

- Information to be provided to the data subject (identity, purpose, recipients, access right, optional answers, etc.).

- Right of access: confirmation, communication of data, logic of the processing, rectification, notification to recipients.

- Right to object: at any time, “on compelling legitimate grounds” in certain cases, on request in case of direct marketing.

- No decision producing legal effects based solely on automated processing of personal data (performance, creditworthiness, conduct, etc.).

National instruments: Europe (4/4)

- Liability of the controller (person who determines the purposes and means of the processing of personal data).

- The controller is in charge (inter alia) of ensuring the confidentiality of personal data and the security of processing.

- Limitations on the transfer of personal data to third countries (but as few as possible within EU).

- Independent privacy agencies with great powers (authorization, notification, control, injunction, arbitration, sanction, etc.).

National instruments: USA

- Comprehensive legislation for federal government agencies (Privacy Act, 1982).

-“Omnibus” legislative solutions for the private sector.

- “Safe harbour” agreement between the USA and Europe for the flow of personal data from EU to US-based companies abiding by a set of “fair information” principles.

Comparative study

- Differences in terms of perception of conflicting interests (public safety, national security, free speech, etc.).

- Differences w.r.t. the role of the state (USA: regulation only when market has failed, Europe: the state should protect individuals).

Relative efficiency

- Consensus on the fact that the USA data protection regime is weaker (lack of federal data privacy agency, gaps in the legislation for the private sector, insufficient self-regulation, opt-out rather than opt-in, etc.).

- Stringent regulations and agencies with strong formal powers does not necessarily imply greater success (balance between strong or heavy procedures which cannot be applied and too weak protections).

- Issues with European regime: under-resourced agencies, marginalisation of data privacy (out of courts), lack of legislative encouragement for PETs.

- NB: regulations and agencies do not only solve conflicts, they also aim at “curbing the future” (deterrence, symbolic role, etc.).

- German regime is often regarded as one of the most efficient.

Lessons and questions: legal side (1/2)

Status of privacy

- Privacy goes further than the protection of personal data: “right to be let alone”, “autodetermination”, “self control of personal attributes”?

- Identity is at the core of the notion of privacy: but what is identity?

- Links between intellectual property and privacy.

- Privacy breaches as “breaches of an implied contract or of a trust or confidence”?

- Are privacy rights (or part of them) inalienable ?

- Balance between privacy and other rights such as free speech and right of citizens to be informed (secrecy favouring mistrust, transparency favouring trust ?)

Lessons and questions: legal side (2/2)

Privacy in the digital society

- Privacy goes further than the protection of personal data: “self control of personal attributes”, “autodetermination”? But does it make a difference in the digital world ?

- How much should individuals be protected against “consenting” renouncement (surreptitious invasion by technology and marketing)?

- Legal value of contracts executed using automated tools?

- Legal value of contracts executed with unknown parties (pseudonyms)?

- How to measure and improve the efficiency of regulations (economic, social, technical), especially w.r.t. new technologies?

Lessons and questions: technical side

- The notion of personal data itself is quite extensive (need to reason about various combinations or treatments of data, to take into account anonymisation, linkability, etc.)

- Integration of legal issues: precise definition of the actors involved, their technical responsibility and legal liability (including data subject). Legal or implied contracts?

- Several necessary conditions for unambiguous consent: unambiguous information, non discrimination, unambiguous acceptance.

- Close links with “traditional” security (confidentiality, integrity, authentication, denial of service, etc.).

- Automatic means to check (at least partially) compliance are desirable.

Expressing privacy policies : technical requirements (1/4)

- Purpose (statistics, patient health care, etc.).

- Conditional rights (read, use, etc.) and obligations (owner information, consent request, deletion, audit trace, etc.).

- Transfer (of rights and obligations).

- Revocation (of rights and obligations).

- Time (before/after, at occurrence of specific events, at specific times, etc.).

- Specific rights of the owner of personal data (access, modification, deletion, etc.) and means to exercise such rights (e.g. API).

- Notion of current context (esp. in AI), generalization of “private sphere”, localization, distance, etc.

Expressing privacy policies : technical requirements (2/4)

- Notion of liability / accountability.
- Commitments on the security measures to protect private data.
- Notion of trust (=> trade-offs, proportionality).
- Notion of data sensitivity (=> trade-offs, proportionality).
- Notion of data aggregation, linkability, anonymity.
- Options (parameterized policies).
- User interaction.
- Mandatory and discretionary rules (impact on responsibilities)?

Expressing privacy policies : technical requirements (3/4)

Privacy policy model:

- Non ambiguous (formal) semantics.
- User understanding (natural language or P3P-style translation ?)
- Decision algorithm to check (at least partially) the validity of actions (a priori / a posteriori).
- Negotiation of security policies.
- Comparison (or refinement) of security policies.
- Composition of security policies.

Expressing privacy policies : technical requirements (4/4)

Further technical challenge: identity

- Central notion for privacy.
- Related issues:
  - Pseudonymity, anonymity
  - Authentication
  - Trust
  - Incremental personal data disclosure, etc.
- Integration within the formal framework:
  - Specific notion of just a kind of sensitive data?
  - Two-level framework of single level?

PRIAM position

- Ambient Intelligence context:
  - No other solution than Flexibility + Responsibility
- To tighten the link between privacy rights and technology:
  - Top-down approach: Law → Formal Model → Implementation
- Reestablish the balance between data owners and controllers
  - Technology can also be used to strengthen citizen rights