Future Internet Ethics: Privacy Concerns for the Development of Fair Information Practices

5.3.2014

Hannakaisa Isomäki, PhD, Adjunct Professor, Senior Lecturer

Faculty of Information Technology & Methodology Centre for Human Sciences

University of Jyväskylä, Finland

Content

1. Definition
2. Elements
3. Legal view: Data protection
4. Behavioral view: Boundary control mechanisms
5. Technological privacy: Design implications

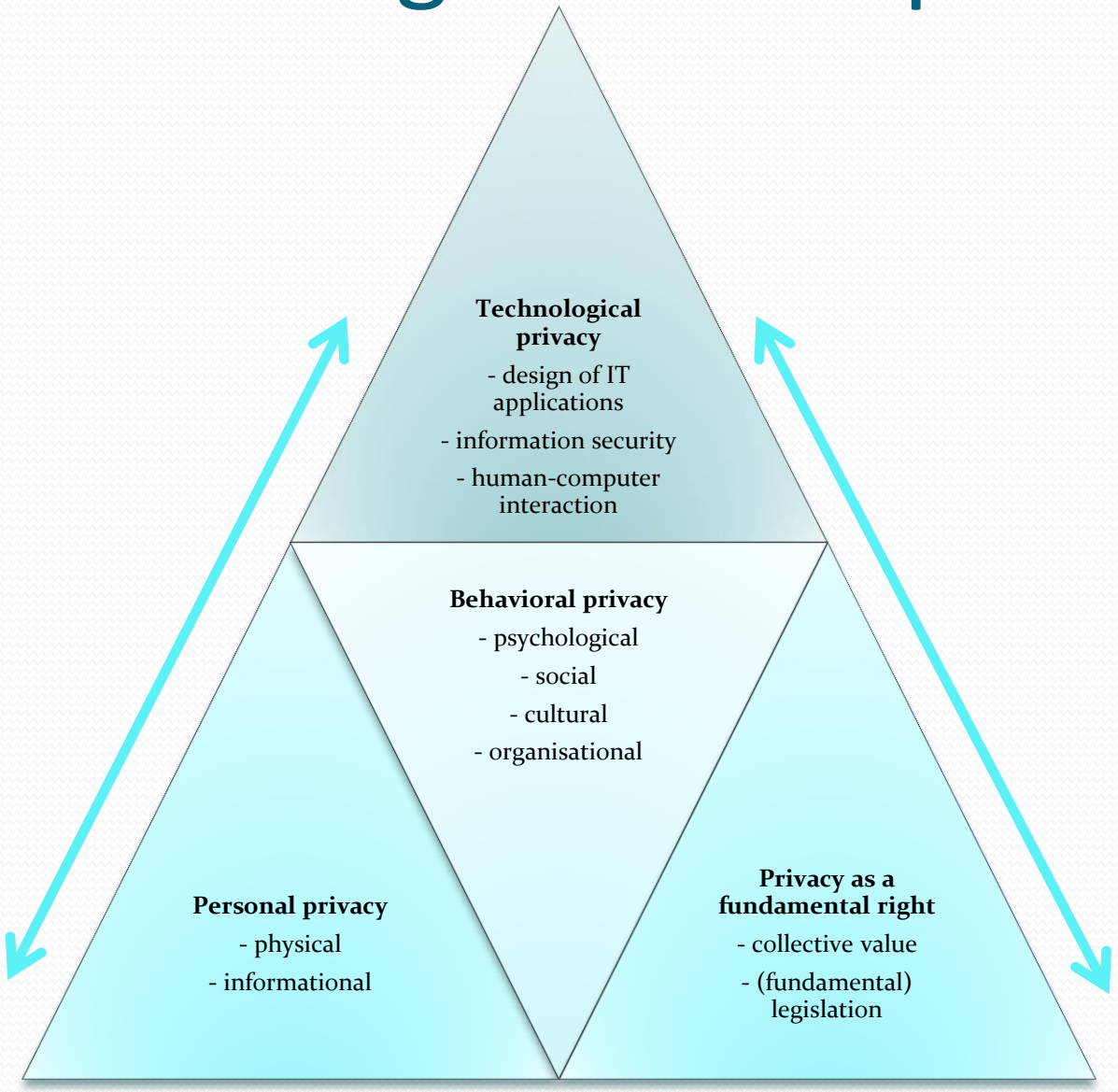
General definition (Wikipedia)

- **Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby express themselves selectively.** The boundaries and content of what is considered private differ among cultures and individuals, but share common themes.
- When something is private to a *person*, it usually means there is something to them inherently special or sensitive. A person will go to extreme lengths to protect his/her privacy.
- The domain of privacy partially overlaps security, including for instance the concepts of appropriate use, as well as protection of information.

Why privacy is important?

- **Future Internet**: vastly increasing amount of information about people, advanced methods for collecting and processing data
- **Ethics**: privacy requires ethical sensitivity due to its complex and fundamental nature in human existence. A narrow moral sense of 'right and wrong' is not enough but more complex deliberation is required for ethically sustainable privacy practices and designs. Law vs. ethics.
- **Fair information practices**: just and honest collection and use of identifiable information about people. As an IT professional, you have to be able to justify (at least to yourself) your actions concerning privacy (cf. Amitai Etzioni: "corporate data miners, or "Privacy Merchants," stand to profit by selling massive dossiers personal information, including purchasing decisions and Internet traffic, to the highest bidder").
- Privacy can also be seen as an indicator of the level of cultivation (education, civilisation) of a country/government, group of people, professions or even individuals

The building blocks of privacy



Personal privacy: physical

- Physical: intrusion into one's physical space or solitude
- preventing intimate acts or hiding one's body from others for the purpose of modesty; apart from being dressed this can be achieved by walls, fences, privacy screens, or by being far away from others
- e.g., video, or aptly named graphic, or intimate, acts, behaviors or body parts
- preventing unwelcome searching of one's personal possessions
- preventing unauthorized access to one's home or vehicle
- medical privacy, the right to make fundamental medical decisions without governmental coercion or third party review
- the US Fourth Amendment: "the right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". Most countries have laws regarding trespassing and property rights to determine the right of physical privacy. Gun laws.
- Physical privacy may be a matter of cultural sensitivity, personal dignity, and/or shyness. There may also be concerns about safety, if for example one is wary of becoming the victim of crime or stalking. Civil inattention is a process whereby individuals are able to maintain their privacy within a crowd.

Personal privacy: informational

- Usually concerns the evolving relationship between technology and the legal right to privacy in collection and sharing of personal data
- May be contradictory requiring contextual deliberation, e.g. on the one hand freedom of speech/activity in a protected space (e-learning), on the other hand strict privacy legislation/personal privacy needs (e.g. introvert/extrovert)
- Regulated in most countries by data protection legislation; need to know if working with data

Privacy as individuals' right

- The right not to be subjected to unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' privacy laws, and in some cases, constitutions; to ensure human dignity and autonomy.
- the human right to privacy has precedent in the United Nations Declaration of Human Rights: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."
- new technologies alter the balance between privacy and disclosure, and privacy rights may limit government surveillance to protect democratic processes.

Privacy: Legal view (1/4)

- Laws for protecting and preserving of privacy rights of individuals
- Universal Declaration of Human Rights, article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- For Europe, Article 8 of the European Convention on Human Rights guarantees the right to respect for private and family life, one's home and correspondence. The European Court of Human Rights in Strasbourg has developed a large body of jurisprudence defining this fundamental right to privacy. The European Union requires all member states to legislate to ensure that citizens have a right to privacy, through directives such as the 1995 Directive 95/46/EC on the protection of personal data

Privacy: Legal view (2/4)

- Data protection legislation (e.g. HetiL) essential tool for privacy protection: it offers solutions for needs to 1) protect personal data and 2) to process and use personal data. The aim is to maintain trust and to promote ethically sustainable information processing (www.tietosuojavaltuutettu.fi)
- Data protection for privacy (yksityisyys ja henkilötietojen tietosuoja) is in Finnish fundamental law (PL 10 §) and in the Charter of Fundamental Rights of the European Union (7,8)
- What is personal data (henkilötieto)?
  - All data describing a person in an identifying manner, i.e., which can be identified to that person or his/her family (HetiL 3 §)
  - For example, Name, registernumber (car), dynamic IP address, phone number, street address, picture, etc. Special case: biological material (blood, tissue, DNA etc.) if it is used to produce information about a person
- What it processing of personal data?
  - Collection, archiving, saving, organising, use, transfer, dissemination, preserving, giving, changing, deleting and other activities concerning personal data (HetiL 3 §)

Privacy: Legal view (3/4)

Summary of users' privacy rights:

- Privacy concerning personal information vs. privacy as freedom of action in the private sphere
- Self-determination over one's personal data:
  - Control over data collection
  - Control over data circulation
  - Control over data usage

  After agreeing to the treatment of one's information
  - View the data (right of access)
  - Control over the adequacy of the data
  - Control over the persistence of the data (right to oblivion)

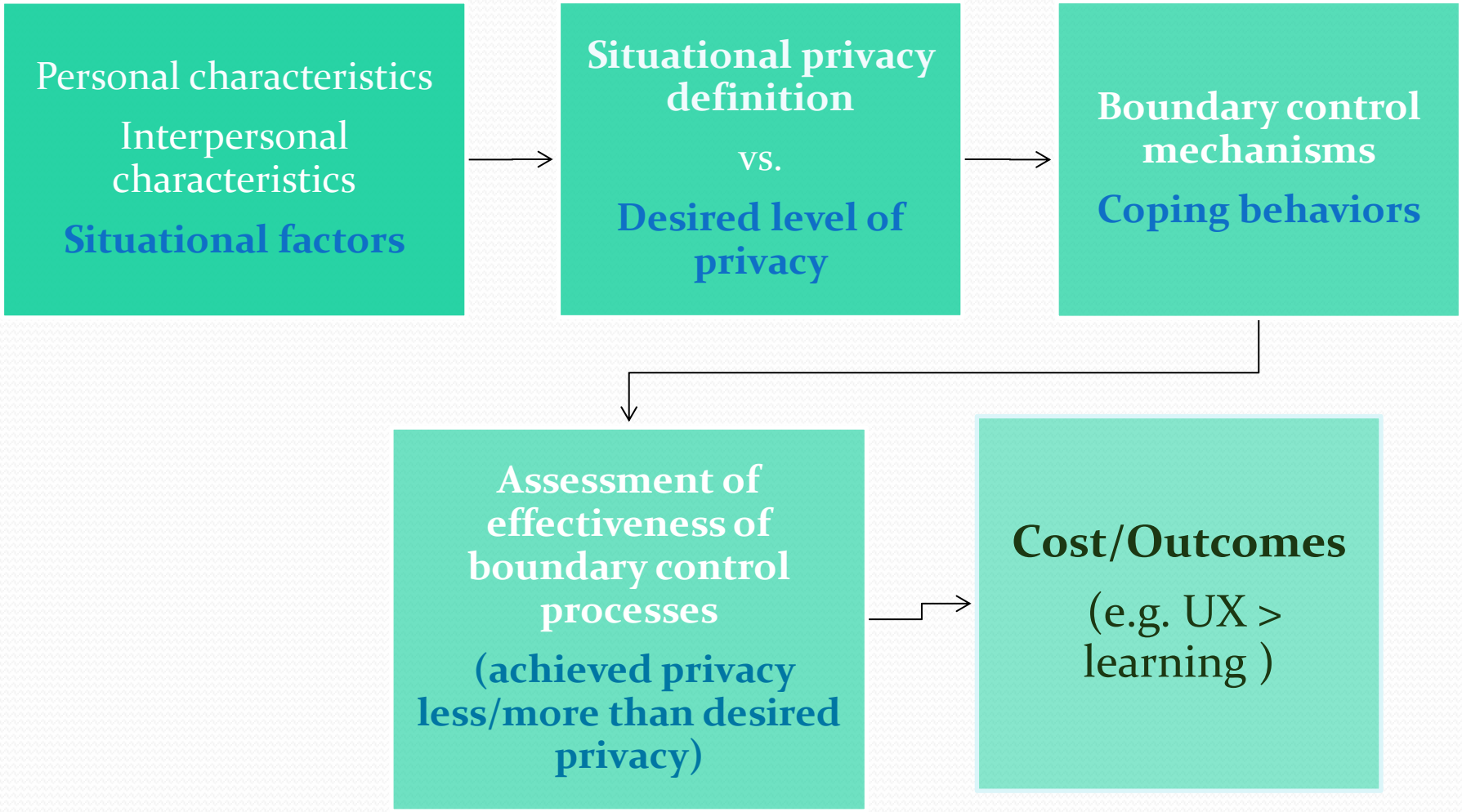
Privacy: Legal view (4/4)

- Summary of mandatory information processing principles
  - Personal data is handled with diligence (HetiL 5 §)
  - Personal data processing needs to be planned well, (Hetil 6 §)
  - Quality requirements: no unnecessary data to be processed, data needs to be correct (HetiL 9 §)
  - Protection requirement (no unauthorised access/dissemination), non-disclosure, personal data register's disposal and archiving (HetiL 32-35 §)
  - Protection of registered people's rights

Behavioral privacy

- Interpersonal social & psychological boundary-control process, which paces and regulates interaction with others
- Dialectic process, which involves both a restriction of interaction and a seeking of interaction
- Optimizing process. Objective: desired level of balance between openness and closedness in a moment of time
- Input & output process. People try to regulate contacts coming from others and outputs they make to others
- Behavioral mechanisms to achieve privacy goals: *verbal behavior* (content & style of communication), *personal space* (distance & angle of orientation to others), *territory* (use & possession of objects & areas), *cultural mechanisms* (norms, rituals), *privacy functions* (control, roles, plans, features of self-identity)

Privacy process: behavioral example



Technological privacy

- Internet privacy is the ability to determine what information one reveals or withholds about oneself over the Internet, who has access to such information, and for what purposes one's information may or may not be used. For example, web users may be concerned to discover that many of the web sites which they visit collect, store, and possibly share personally identifiable information about them. Similarly, Internet email users generally consider their emails to be private and hence would be concerned if their email was being accessed, read, stored or forwarded by third parties without their consent. Tools used to protect privacy on the Internet include encryption tools and anonymizing services like I2P and Tor.
- The right to know when privacy rights are given away

Technological privacy: design implications

- Privacy by design
- Privacy and related data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal
- Privacy tools should be integrated into social media applications in terms of users' privacy regulation preferences (cf. Behavioral process + data protection)
- Quality of privacy features of software should be tested as one facet of usability/UX

Nielsenin lista (Nielsen & Molich 1990, Nielsen 1994) vs. SoMe/Privacy heuristiikka (Isomäki 2012)

Nielsen's usability heuristics	SoMe/Privacy heuristics (Isomäki)
1. Visibility of the system status	1. Visibility of the situational privacy features
2. Match between system and the real world	2. Degree of sociability
3. User control and freedom	3. User control over privacy mechanisms & personal information
4. Consistency and standards	4. Visual design supports privacy mechanisms
5. Error prevention	5. Error prevention and correction possibility
6. Recognition rather than recall	6. Minimised cognitive load
7. Flexibility and efficiency of use	7. Flexible options for boundary control management
8. Aesthetic and minimalist design	8. Minimalist design of boundary control features
9. Helping users recognise, diagnose, and recover from errors	9. Helping users to diagnose and recover errors in boundary control features
10. Help and documentation	10. Help and documentation

Thank you!

hannakaisa.isomaki@jyu.fi