Ethical Aspects of Information Security

Elin Palm
Department of Philosophy,
The Royal Institute of Technology (KTH),
Stockholm, Sweden

Research project KTH: ”Assessing Public Acceptance of Privacy Invasive ICT-solutions”

(1) Two surveys investigating Swedish citizens’ awareness of- and attitudes towards data collection and trust in Information Security will be conduected.

(2) Parallell to the empirical studies, a normative analysis will be undertaken: what types of data should individuals keep to themselves and why? Under what conditions is informed consent a justifiable means of protecting personal data?

Aim of project

- Generate guidelines that can be used to predict and assess the public's acceptance of novel potentially privacy invasive ICT solutions and new uses of such technology.
- The steadily increasing societal dependence on ICT necessitates means and strategies for securing ICT-carried functions and systems such as e-services. This project provides a non-technical solution, examining the ethical foundations of Information Security.

In order to identify

- *morally defensible* ways of obtaining and securing personal data the following aspects should be *further* investigated:

(1)The type of data to be collected – what types of information are sensitive and why?

(2)The purpose of data collection and information security.

(3)The conditions for *substantial* informed consent (or consented information).

PRIVACY

- What is perceived of as privacy sensitive changes with time and between individuals. Hence, an updated understanding of individuals' *de facto* experiences /expectations of privacy is needed.
- Privacy protection legislation *should be informed by but* not only be based on actual perceptions - that could result in individuals claiming too much or too little protection.
- In addition, a normative analysis is needed.

The value of privacy

- Privacy is important and should be protected for the reason that the more fundamental value - personal autonomy - is safeguarded thereby (cf. Rössler, 2005).
- Not everything that individuals consider private should be framed and protected as privacy sensitive but such aspects that are related to self-government

Privacy - a collective interest

- Although central for personal autonomy, privacy is not only an individual interest.
- A more fruitful way of protecting privacy is to frame it as a collective good. ”People have a shared interest in privacy and privacy is socially valuable” (Regan, 1995:213). Also in German legislation.
- So understood, privacy is strengthened against competing values like security.

SECURITY

- Security is often framed as a collective good as opposed to the individual interest privacy and we are typically asked to accept the concrete and forseeable increment of individuals’ privacy for the *possibility* of increased security.
- Just like attempts have been made to operationalize privacy, the notion of security must be made operational.

Although no exhaustive answers

as to what security is can be given we must try to articultate:

(1)security regarding what and for whom, e.g. what threats we need protection from.

(2)What means that best serve these ends.

(3)When we have reached accpetable levels of security.

Otherwise, there is a risk that privacy will be sacrificed for an end that we cannot or wont know when we have achieved.

CONSENT

- The standard principle regarding data protection is that personal data cannot be disclosed without the consent of the data subject.
- The openness- and individual participation principles state that an individual must be notified of the fact that her data is stored and/or processed.

For consent to be meaningful however,

(1) the degree to which the data subject is aware of the implications of her acts and

(2) the number and quality of alternatives open to the moral agent must be considered. That is, consent must be contextualized (Palm, 2007).

Awareness

The level of awareness among individuals using ICT is of relevance for the degree to which they reasonably can be said to consent. It has been argued that Commonn Criteria (CC) are of little use for ordinary users who lack sufficient technical capabilities and legal knowledge to assess information systems in terms of information security and privacy. Therefore they need service of other competent parties to assess the quality of ICT systems.

Alternatives

- When assessing the moral acceptability of individuals' consent to omit personal data, the *value of utilizing/cost of refraining* from using the service for which data is needed must be taken into consideration such as the import of e-government and e-health services, e-etc etc.
- Since individuals often lack substantial alternatives their *de facto* use of certain services cannot simply be considered to imply a real acceptance.

Travelling by air for instance

typically requires of individuals to provide personal information as well as to undergo bodily and other privacy invasive procedures.

In order to avoid this form of travelling, they would have to choose much more time-consuming means of transport. In case of intercontinental travel there are often no reasonable alternative means of travel available.