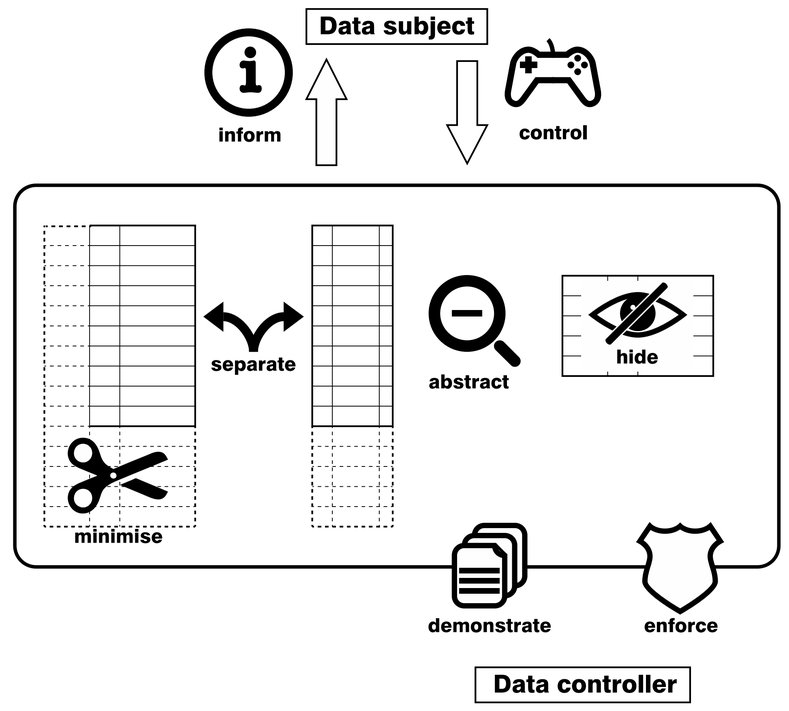
Privacy Design Strategies for the smart grid

Jaap-Henk Hoepman[1]
[1]TNO
Contact: jaap-henk.hoepman@tno.nl

Abstract

Smart grids process personal information. Therefore, they are covered by the upcoming General Data Protection Regulation (GDPR). The GDPR mandates privacy by design, without describing clearly what this means exactly, let alone giving concrete guidelines on how to go about implementing privacy by design when actually designing a system. To make privacy by design concrete, the soft legal norms need to be translated into more concrete design requirements that engineers understand. This is achieved using privacy design strategies. This poster summarizes the privacy design strategies and shows their relevance to designing a privacy friendly smart grid.

The Eight Privacy Design Strategies



References

SEGRID Deliverable D4.2 Preliminary specification of security and privacy solutions, September 2016.

M. Colesky, J.-H. Hoepman, and C. Hillen.
A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering – IWPE'16, pages 33-40, San Jose, CA, USA, May 26 2016.

Minimise

Definition: limit the processing of personal data.

Associated tactics:
- EXCLUDE: refrain from processing a data subject's personal data.
- SELECT: decide on a case by case basis on the processing of personal data.
- STRIP: remove parts of personal data that are no longer necessary.
- DESTROY: completely remove a data subject's personal data.

Smart grid examples:
- Pay before use
- Compute bill locally

Separate

Definition: separate the processing of personal data.

Associated tactics:
- DISTRIBUTE: partition personal data over separate physical locations.
- ISOLATE: (logically) process parts of personal data independently.

Smart grid examples:
- Isolate transactional data from network management data
- Collect and process personal data on the smart meter

Abstract

Definition: limit the amount of detail in which personal data is processed.

Associated tactics:
- SUMMARIZE: extract commonalities in personal data.
- GROUP: process personal data at a common category level, instead of a more detailed data subject or attribute level.
- PERTURB: add noise or approximate the real value of a data item.

Smart grid examples:
- Aggregate energy consumption for billing purposes over time
- Aggregate network data for management purposes over networks/housing blocks

Hide

Definition: prevent that personal data becomes public or known.

Associated tactics:
- RESTRICT: prevent unauthorized access to personal data.
- MIX: process personal data randomly within a large enough group to reduce correlation.
- ENCRYPT: encrypt data (in transit or at rest)
- OBFUSCATE: prevent understandability of personal data
- DISSOCIATE: remove the correlation between different pieces of personal data.

Smart grid examples:
- Access control

Inform

Definition: inform data subjects about the way their personal data is processed.

Associated tactics:
- SUPPLY: make extensive resources available on the processing of personal data.
- NOTIFY: alert data subjects to any new information about processing of their personal data.
- EXPLAIN: provide information on personal data processing in a concise and understandable form.

Smart grid examples:
- Ambient notifications whenever smart meter data is accessed remotely

Control

Definition: provide data subjects control over the processing of their personal data.

Associated tactics:
- CONSENT: only process personal data for which explicit, freely-given, and informed consent is received.
- CHOOSE: allow data subjects to select or exclude personal data for/from processing
- UPDATE: allow data subjects to keep their personal data accurate and up to date.
- RETRACT: honour the data subject's right to the complete removal of any personal data.

Smart grid examples:
- Privacy dashboard

Enforce

Definition: commit to the privacy friendly processing of personal information.

Associated tactics:
- CREATE: acknowledge the value of privacy and deciding upon policies which enable it, and processes which respect personal data.
- MAINTAIN: consider privacy when designing or modifying features, and updating policies and processes to better protect personal data.
- UPHOLD: ensure that policies are adhered to by treating personal data as an asset, and privacy as a goal to incentivize as a critical feature.

Smart grid examples:
- Grid/company wide privacy policies

Demonstrate

Definition: prove that personal information is processed in a privacy friendly way.

Associated tactics:
- LOG: track all processing of data, without revealing personal data, and review these logs.
- AUDIT: examine all day to day activities for any risks to personal data, and respond to any discrepancies seriously.
- REPORT: analyze collected information on tests, audits, and logs periodically to review improvements to the protection of personal data.

Smart grid examples:
- Logging of accesses by the smart meter.

SEGRID Security for smart Electricity GRIDs

www.segrid.eu info@segrid.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109