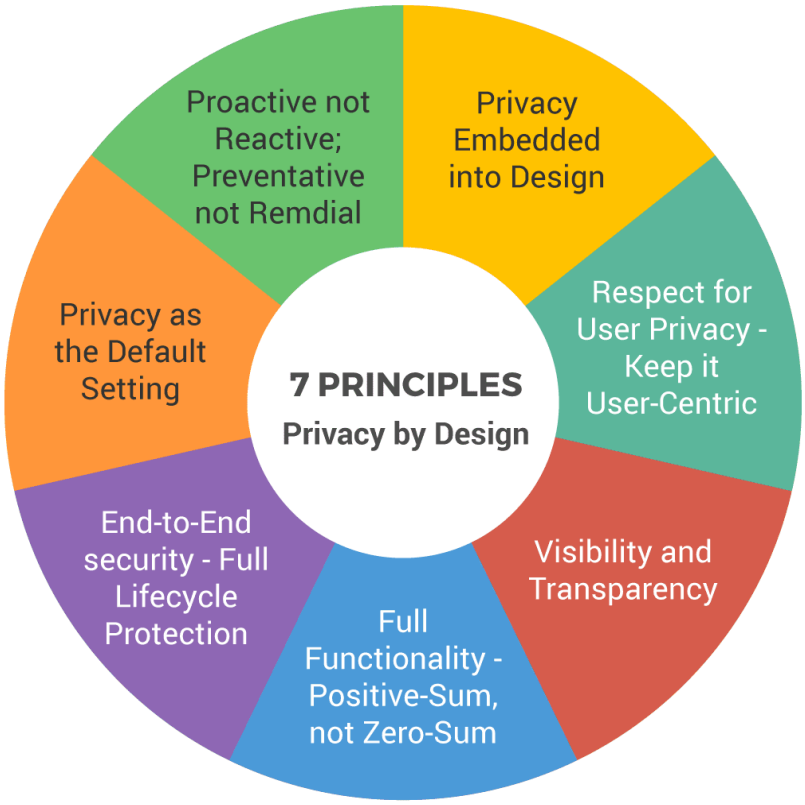
Practical Design Strategies for Implementing PbD

Oct 19th 2020

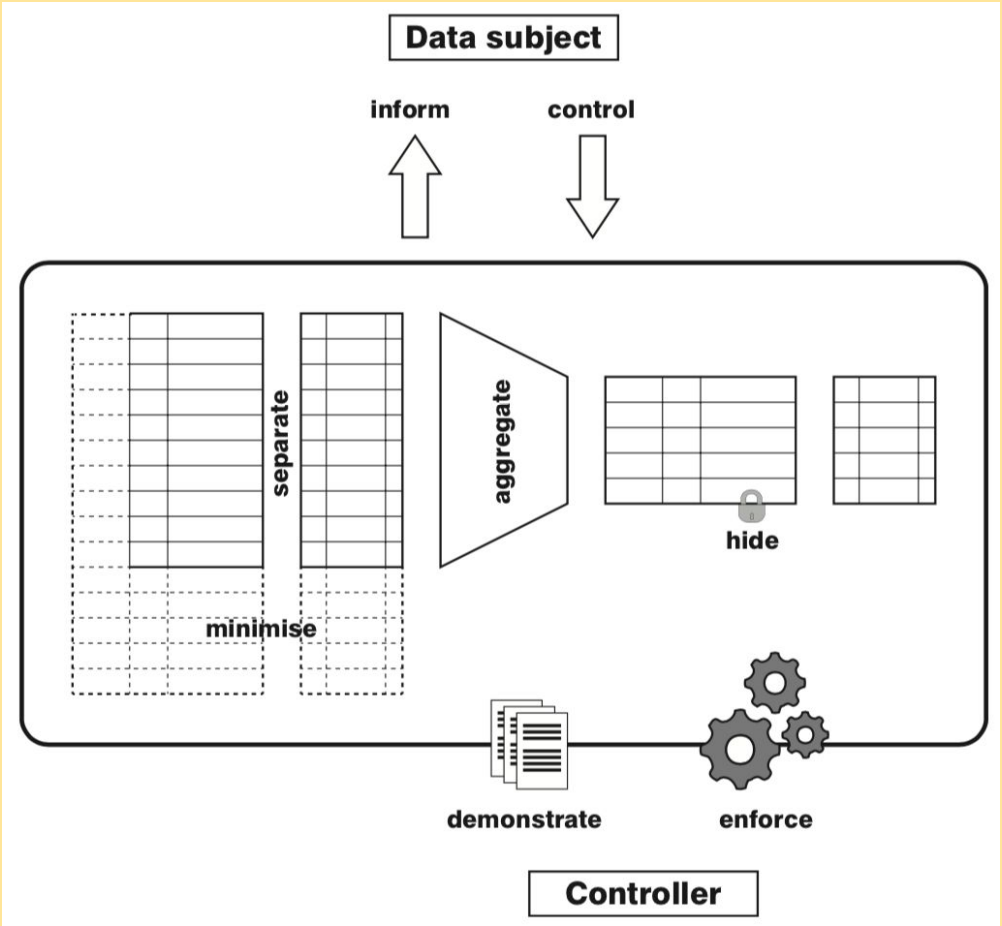
Privacy by Design (PbD) is an approach to systems engineering initially developed by Ann Cavoukian in 2009. It calls for proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices. The approach is based on seven "foundational principles" as depicted in the graphic below. The PbD principles have been criticized for being too vague and difficult to implement or enforce in practice.



In the context of developing IT systems, PbD requires eliciting and analyzing privacy requirements; developing designs that fulfill those requirements; implementing the design; and testing that in the implementation the functional and privacy requirements are fulfilled. In his 2013 paper Jaap-Henk Hoepman introduces the concept of privacy design strategies and presents the concept of design strategies,

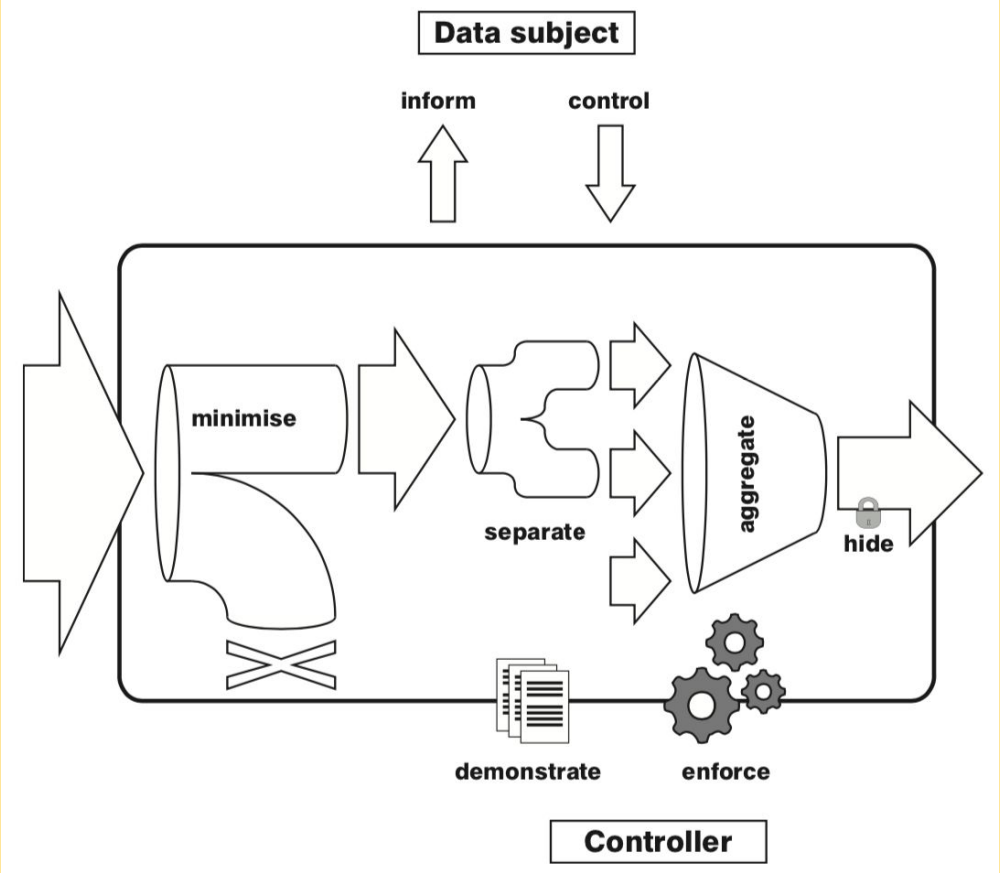
design patterns and concrete technologies as distinct approaches to supporting the decisions to be made in each phase of systems development. Strategies support the concept development and analysis phases, patterns are applicable during the design phase, and Privacy Enhancing Technologies (PETs) are useful during the implementation phase. Key takeaways from the article -

- The distinction between a design strategy, a design pattern and a PET are in some way similar to the classification of strategic, tactical and operational levels of decision making.
- We can view an IT system either as an information storage system (i.e., database system) or an information flow system. In practice a system is often a hybrid, with some information flow components and some information storage components.
- Current data protection legislation is pretty much written with a database model in mind. In a database, information about individuals is stored in one or more tables. Applying the legal framework point-of-view, we distinguish the following eight privacy design strategies: **MINIMISE, SEPARATE, AGGREGATE, HIDE, INFORM, CONTROL, ENFORCE and DEMONSTRATE**.



The eight privacy design strategies derived from the DB metaphor

- The eight privacy design strategies also naturally apply to an information flow system.



The eight privacy design strategies derived from the flow metaphor

---

Sources : Wikipedia, Jaap-Henk Hoepman Article