

STRATEGIES AND TACTICS

Strategies and Tactics, including definitions, adapted from M. Colesky, J.H. Hoepman, and C. Hillen. A Critical Analysis of Privacy Design Strategies. In 2016 International Workshop on Privacy Engineering IWPE'16

TECHNICAL STRATEGIES

ARCHITECT

MINIMIZE

- ▶ **Exclude**
Limit interactions only to that which is necessary to complete the task.
- ▶ **Select**
Limit interactions on a case by case basis.
- ▶ **Strip**
Remove unnecessary information prior to processing.
- ▶ **Destroy**
Remove information after interaction.

SEPARATE

- ▶ **Isolate**
Logically separate actors from individuals or their proxies (usually for different purposes).
- ▶ **Distribute**
Physically separate actors from individuals or their proxies.

SECURE

ABSTRACT

- ▶ **Group**
Limit interactions to groups of people, rather than individuals.
- ▶ **Summarize**
Generalizing detail about people to reduce particularity.
- ▶ **Perturb**
Add noise to interactions.

HIDE

- ▶ **Restrict**
Limit access to people or their proxies.
- ▶ **Mix**
Randomize people or their proxies to prevent correlations.
- ▶ **Obfuscate**
Reduce the understandability of information.
- ▶ **Dissociate**
Remove correlations between people or their proxies.

PROCESS STRATEGIES

SUPERVISE

ENFORCE

- ▶ **Create**
Decide on a policy that dictates interactions.
- ▶ **Maintain**
Continuously improve privacy values, policies and controls.
- ▶ **Uphold**
Identify core privacy values that drive organizational behavior.

DEMONSTRATE

- ▶ **Record**
Track interactions with people or their proxies. Document other activities meant to support privacy.
- ▶ **Audit**
Review activity regularly.
- ▶ **Report**
Analyze records and audits periodically and report to the people responsible.

BALANCE

INFORM

- ▶ **Supply**
Inform individuals about future interactions and risks.
- ▶ **Notify**
Alert individuals to past interactions or risks.
- ▶ **Explain**
Provide information about interactions and risks in a concise and easily understandable way.

CONTROL

- ▶ **Consent**
Interact with people or their proxies with their permission.
- ▶ **Choose**
Interact with people or their proxies within the scope and specifications they determine.
- ▶ **Update**
Give people the opportunity to make timely changes to information about them relevant to purpose.
- ▶ **Retract**
Cease interacting with people or their proxies after they withdraw permission.