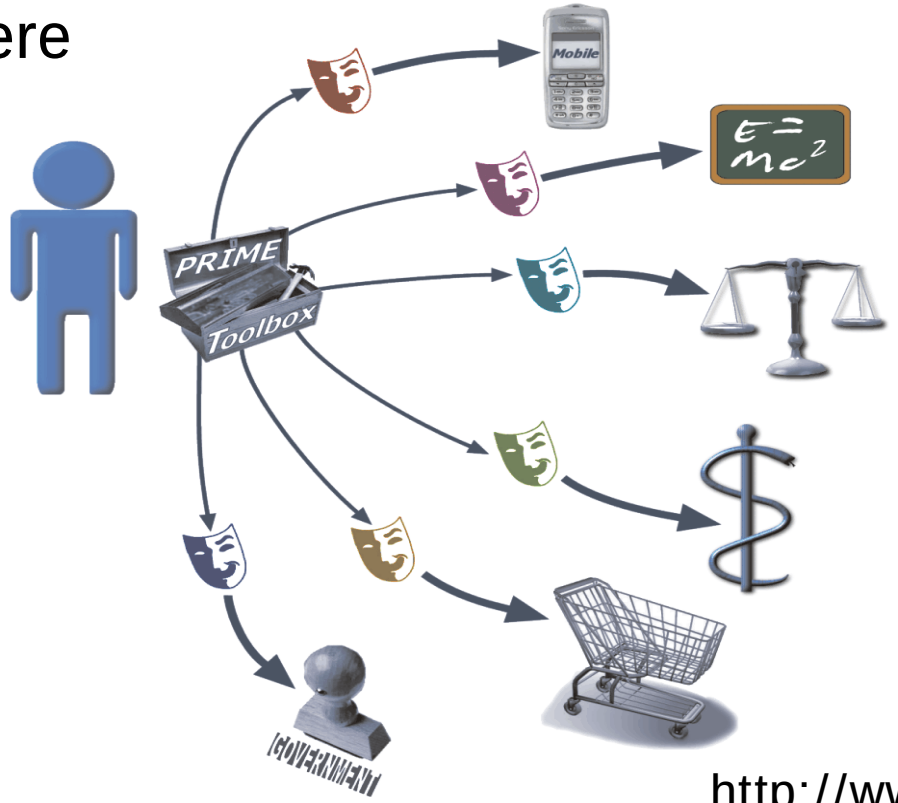
ORGANIZATIONAL ADOPTION OF PRIVACY ENHANCING TECHNOLOGIES (PET)

John Borking

Vision: Users can act securely and safely in the Information Society while keeping sovereignty of their private sphere



CENTRAL QUESTIONS

- WHEN STARTS AN ORGANIZATION BOTHERING ABOUT PRIVACY
- WHAT FACTORS AFFECT AN ORGANIZATION'S DECISION TO INTRODUCE PET
- IS THERE IS AN ORGANIZATIONAL ADOPTION PROBLEM FOR PET?
- DRIVERS AND INHIBITORS FOR ADOPTION BY ORGANIZATIONS OF PET

DEFINITI0N OF PET

PET IS A SYSTEM OF ICT MEASURES PROTECTING THE INFORMATIONAL PRIVACY BY:

1. **ELIMINATING OR**
2. **MINIMIZING PERSONAL DATA OR**
3. **PREVENTING UNNECESSARY OR UNWANTED PROCESSING OF PERSONAL DATA, WITHOUT LOSS OF FUNCTIONALITY**

HYPOTHESIS

For the implementation of PET, certain maturity of the organization is required. It is highly unlikely that immature organizations will implement PET, let alone that these organizations have any awareness of privacy protection. The level of maturity for IAM is a strong indication for the introduction of PET in an organization.

PRIVACY MATURITY MODEL

- ***"a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached."***

- **Existing models: CMMi (SE Carnegie Mellon), Nolan Norton, INK (EFQM)….**

IAM topology with organization class segments for maturity

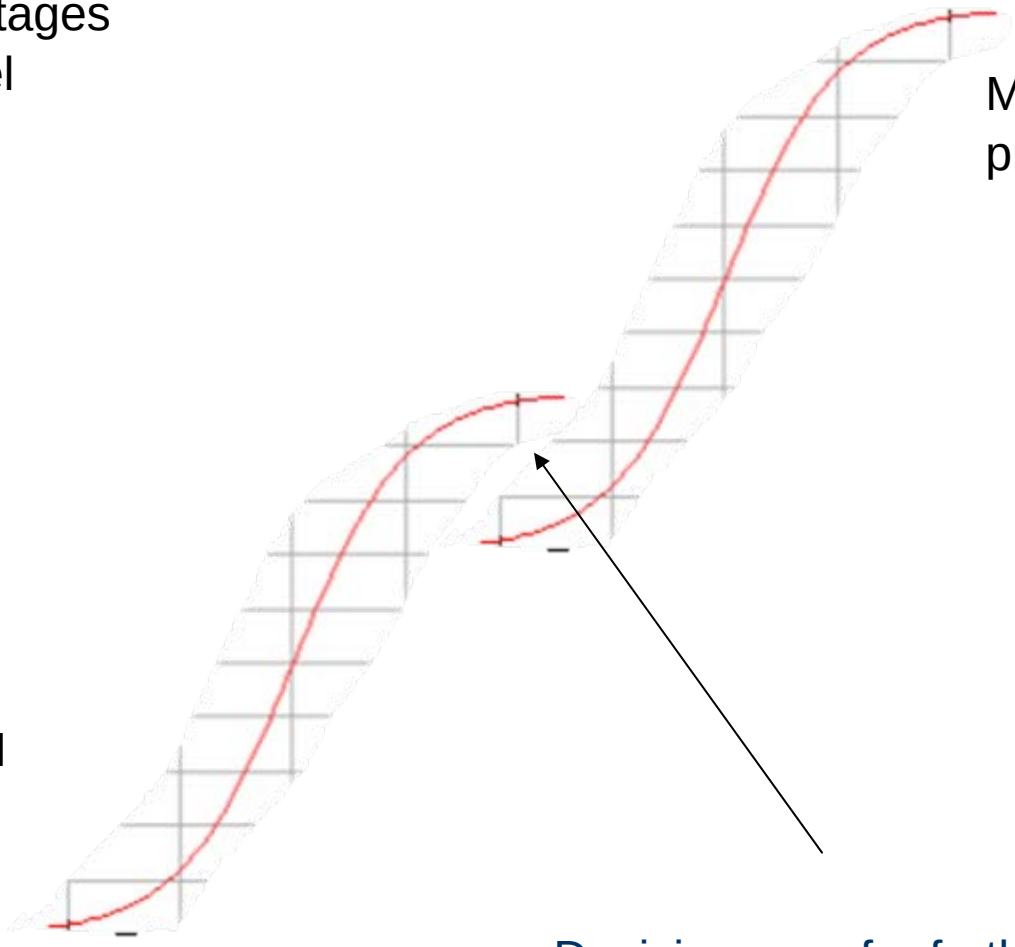
Top Class	Authentication requirements based on continuous risk analysis and are continuously adjusted	Central real-time controlled authorizatino sources, automated procedures	Role Based Access Control for all applications and continuous updated authorizations	Automated and reliable for multiple sources	Full responsibility to AO/IC with periodic reporting
Pro-Active	Authentication Requirements based on continuous risk analysis	Central registration, controlled authorization processes, manual procedures	Role Based Access Control used for critical applications	Limited Automated and reliable for multiple sources	Full responsibilty to AO/IC
Active	Authentication Requirements based on a one time survey	Central registration, Limited user group, manual procedures	Authorization matrixes are updated periodically	Limited Automated but reliable processes locally	Partial delegation of responsibility to AO/IC
Starting-up	Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)	Entries can be double but they are consistent	Authorization matrixes defined but are not updated	Limited Automated unreliable processes locally	Sporadically delegated responsibility of AO/IC
Immature	No authentication means	Double and inconsistent entries because of chaotic and ad hoc processes	No authorization matrixes, authorization is defined ad hoc	Manual process locally	No responsibilty delegated into a AO/IC organization
	Authentication Managment	**User Managment**	**Authorisation Managment**	**Provisioning**	**Monitoring(Audit)**
	Organization				

GENERIC PRIVACY MATURITY LEVELS

Initial	Activities are ad hoc, with: • No defined policies, rules, or procedures. • Eventually lower-level activities, not coordinated. • Redundancies and lack of teamwork and commitment.
Repeatable	The privacy policy is defined, with: • Some senior management commitment. • General awareness and commitment. • Specific plans in high-risk areas.
Defined	The privacy policy and organization are in place, with: • Risk assessments performed. • Priorities established and resources allocated accordingly. • Activities to coordinate and deploy effective privacy controls.
Managed	A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with: • Early consideration of privacy in systems and process development. • Privacy integrated in functions and performance objectives. • Monitoring on an organizational and functional level. • Periodic risk-based reviews.
Optimizing	Continual improvement of privacy policies, practices, and controls, with: • Changes systematically scrutinized for privacy impact. • Dedicated resources allocated to achieve privacy objectives. • A high level of cross-functional integration and teamwork to meet privacy objectives.
	— *Source: Hargraves et al 2003*

S- CURVES MATURITY IAM & PRIVACY

Nolan Norton stages
of growth model

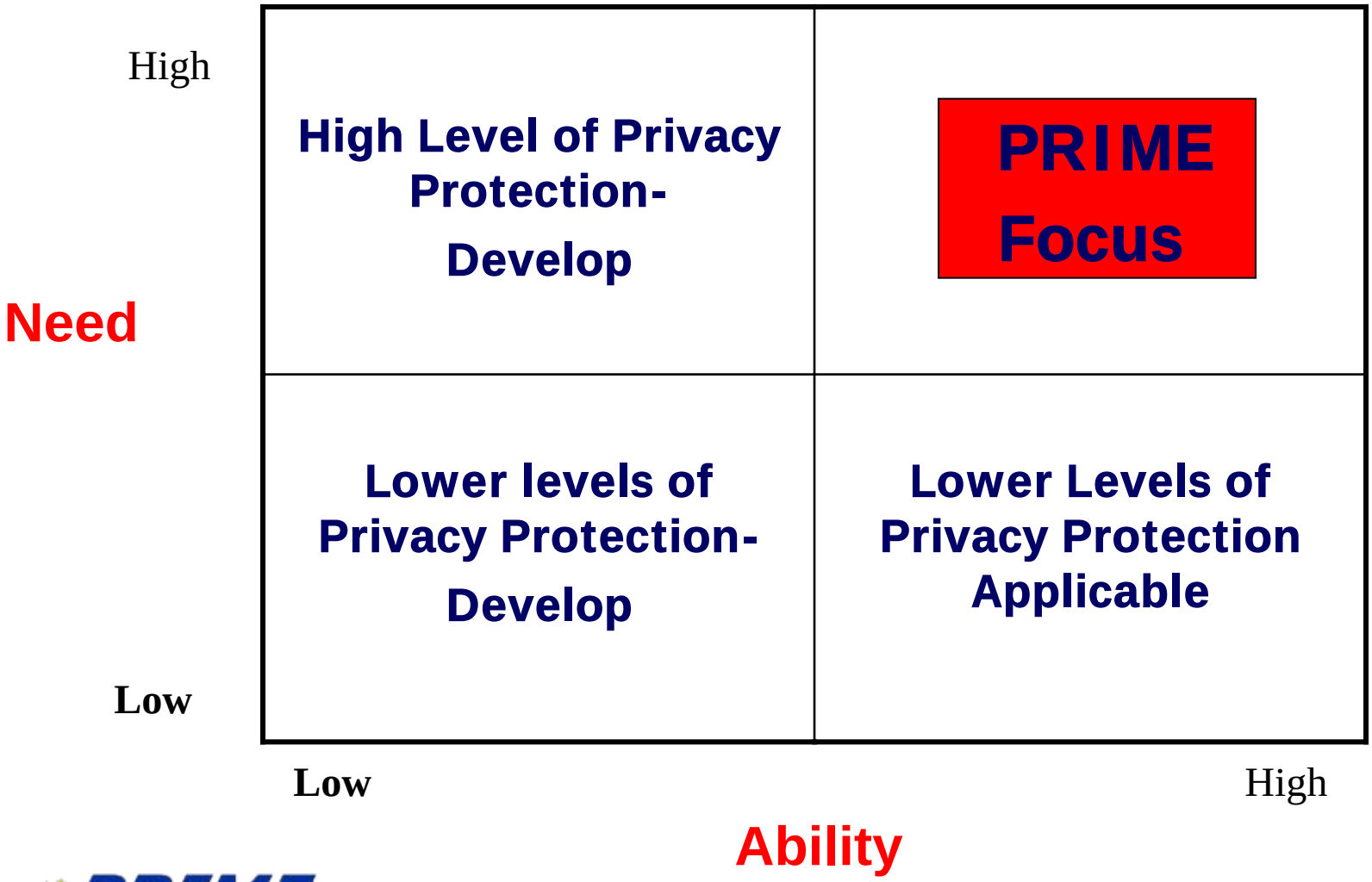


Maturity Privacy
protection

Maturity IAM
Processes

Decision area for further growth

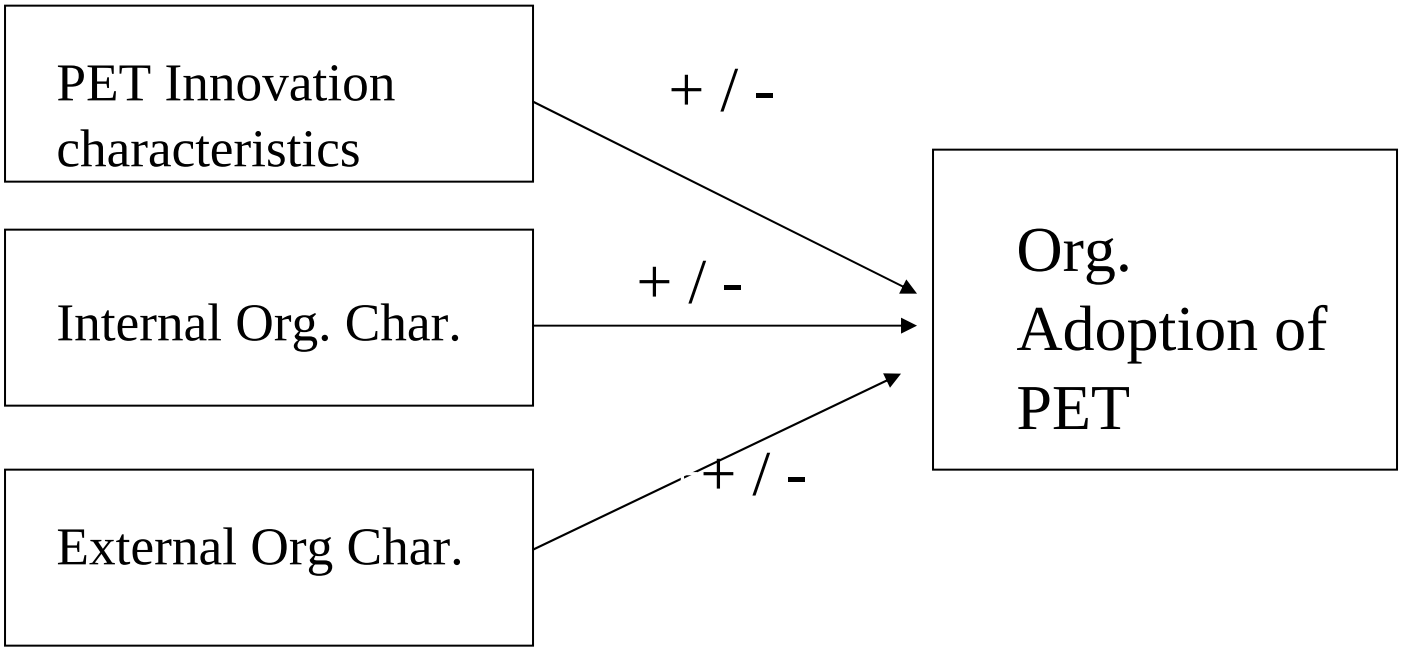
Towards a Typology: Which Organizations?



Organizational Adoption of PET

Literature Review

Studies by a.o. Rogers (2003) and Fichman (2000): Clusters of factors impacting adoption of IT based innovations.



Results of Interviews and Case Analysis by category

Factor I: Characteristics of PET

Positive:

- + Relative Benefit
- + Role of advisory institutions

Negative:

- – Costs
- – Compatibility
- – Complexity
- – PET woven into business processes

Results of Interviews and Case Analysis by category

Factor II: Internal Organizational Characteristics

Positive

+ Perception and level of awareness of privacy regulation

+ Type of Data processed (e.c. risks incurred)

+ Individual Ties with advisory institutes

+ Presence of Key persons

Negative

- Complexity of organizational processes

- Structure and size of the organization

- Diversity in Information Systems

Results of Interviews and Case Analysis by category

Factor III: External Organizational Characteristics

Positive

+ Pressure by privacy legislation
+ Existing offer of PET measures

Negative

- Complexity of privacy law
- Private versus Public organizations

QUESTIONS?

- **Thank you**