PR**I**WAY
Security in Context

Without PETs, democracy and markets won't work

Stephan J. Engberg
Priway
sje webmail at Priway.com

Agenda

- Examples of PET economic value in live cases
- Provide operational definitions for economic analysis
- Document with behavioral economics that
    - PETs are a pre-requisite for markets (like property or agreement)
    - That cartel standards & externalities block markets from working
    - Present Governments action damage markets & democracy
- Suggesting the road ahead is National Id 2.0 ensuring
    - Structured pseudonyms negotiated to context
    - Citizens empowered to regain critical control of context
    - Restore markets ability to self-adjust & recover from failures

PET do not protect data - PET eliminate the need to protect data as a pre-requisite to facilitate market-driven progress

Without PETs, markets wont work

2003 EU PET Workshop

Terms definition

Examples (my list)

Privacy Enhancing technologies (PET)

Anonymity plus some kinds of pseudonymity or partial

Anonymity (workshop definition)

Operational understanding :

> **"Enabling without transfer of data control"**

Digital Cash, Broadcast, Zero-knowledge protocols (e.g. RFIDsec), **Biometrics system-on-card**, Blinded Certificates

Privacy Friendly Technologies

Internal Risk reduction or DP compliance

P3P, internal separation of data and identity, Conditional Identification, sticky policies

Privacy Invasive Technologies (PIT)

Deliberate identification & preventing PETs from protecting privacy

Most Biometrics, server-side identity control, surveillance, thin clients/**cloud desktops**

OBS: An application can be designed as a PIT even with PET details

Without PETs, markets wont work

Successful PET systems
Enabling without creating threats

Characerics of good PETs:

    NO NEED for Data Protection.

    No "trusted party" with secrets.

    No transfer of control.

- Democratic Election
- Cash Money
- Broadcast radio/tv/pager
- Car GPS Navigation

No room for security naivity – failures needs to be considered.

CAR GPS can be stolen and leak history. Cash money store DNA.

Without PETs, markets wont work

Key definitions

Privacy:

**Security
from the viewpoint of ONE stakeholder**

Control of personal data:

**Individual control of
referability of data to physical entities
and transfer of data between contexts**

In interdependent systems, Security by Design must include Privacy by Design

Without PETs, wont work

Economics framework
Behavioural Economics

EVEN the strongest pro-market framework requires PETs
for markets to work(*)

**Market innovation is driven by individual free choice
according to a complex set of preferences**

1. Consumers (citizens) must have superior knowledge of personal preferences

2. Cartels cannot be maintained

3. No negative (and positive) externalities

In the internet age, these require PET to hold !!

(*) My interpretation of Ludwig Von Mises – Human Action, "The Prerequisites of Human Action"
http://mises.org/humanaction/chap1sec2.asp

Without PETs, markets wont work

1. Consumers preferences
PETs required to maintain Consumer power

Practical:
See movies
"Groundhog Day"
"Minority Report

Our modern world is build on the quality of citizens free choice & causality learning to choose the better solution and rate it relative to other solutions through how much he is willing to pay.

BUT - Customers lose superior knowledge of personal preferences

- Data Profiling across context undermine free choice
- Systemic & invisible testing of stimuli automate profiling & use
- "Security or service" is not a choice or informed consent
- Consumers have no way to put a specific value to the invisible collection of data & hidden abuse of visible data
- Political profiling undermine democracy as such

Citizens loose power in negotiations due to profiling and testing. This is a primary threat to markets ability to create prosperity. It damage the critical demand-driven innovation !

PETs EMPOWER THE DEMAND to maintain CONTROL

Without PETs, markets wont work

2. Cartels
"Code is law" lead to cartels

According to Behavioral economic theory price cartels cannot be upheld unless enforced by government regulation

Digitalisation have changed that - "CODE IS LAW"(*).

Commercial sector uses "Cartel"-standards to enforce cartel interests (gatekeepers, access to data) within a small group. Interoperability within a standard do not create innovation if the standard block competition – forced identification is by far the main problem.

Examples: EMV-payment cards, Mobile Phones, SAML

Governments enforce legacy-"standards" making public services less innovative while making them vulnurable and ineffective.

Examples: eID, IDABC and ICAO

Infrastructure cartels block competetion, innovation & PET

(*) Lawrence Lessig – "Code is Law"

Without PETs, markets wont work

3. Negative externalities
Externalities undermine markets

Markets are very bad at dealing with externalities

Examples:

Photo expose others

Online email expose counterparts without knowledge or consent

Surveillance (identification) can always be turned into attack

Biometric Identification create risk (identity theft & prevent PETs)

National Id without PETs prevent society from adopting PETs

Infrastructure gatekeepers prevent markets from adopting PETs

Government give public employes access to abusable data

When security fails, system AND external stakeholders get hurt.

Without PETs, markets wont work

Data is a "currency" Society value is negative !

The direct value of PET-protected pseudonymous personal data depends on the application in context !

The additional value to service providers of making data identifiable is equal to the secondary abuse value

- Always smaller than the negotional loss to citizen !!

- Negative externalities to innovation & scaling risks

Convenience & marketing value of identification is zero as PETs make citizens able to define & control context, i.e. citizens can extend or create new context & transfer profile data between contexts.

Problem – stakeholders assess different values of identification
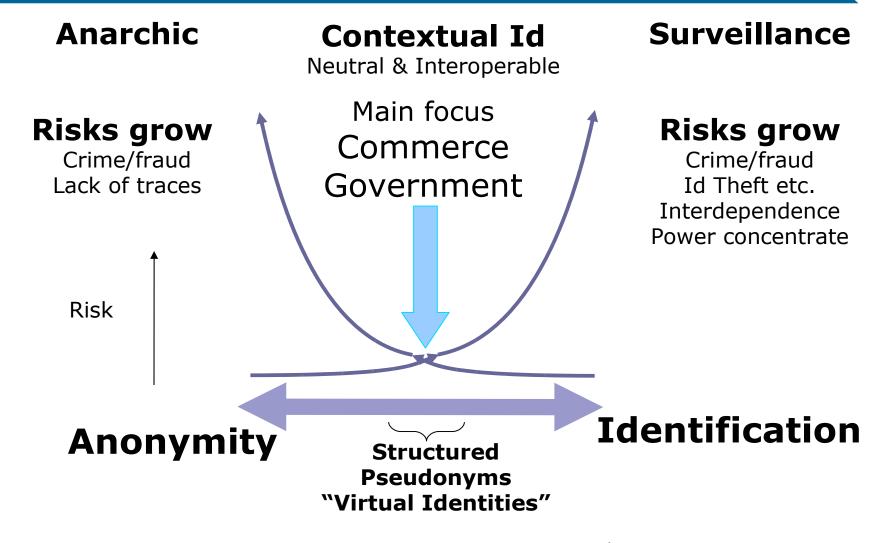
Service Provider assess identification value positive (but dropping)

Society value is increasingly negative (risks & innovation loss)

Markets cannot solve a government/infrastructure problem

Without PETs, markets wont work

Anarchic

Contextual Id
Neutral & Interoperable

Surveillance

Risks grow
Crime/fraud
Lack of traces

Main focus
Commerce
Government

Risks grow
Crime/fraud
Id Theft etc.
Interdependence
Power concentrate

Risk

Anonymity

Structured
Pseudonyms
"Virtual Identities"

Identification

k

11

Towards structured multi-id National Id 2.0 is citizen-centered

Single National Id & Biometric Id
outdated pre-internet thinking

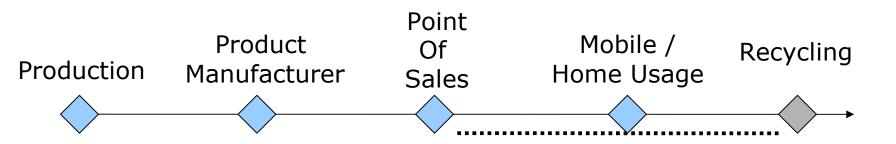|	Single-Id	Multi-Id
Structured	Scandinavian Countries	Strong Root Id with PET ID overlay
Unstructured	Biometri Id	US, UK, Germany etc.

Purpose of National Id 2.0 :

**Ensure citizen can establish and maintain
a new pseudonymous context
and negotiate & adapt to the specific application
independently of previous or future transactions**

Without PETs, markets wont work

PRIWAY
Security in Context

Linkability define context

Production — Global Id 1

Product Manufacturer — Global Id 2

Point Of Sales

Mobile / Home Usage — Silent / Deactivated

Recycling — Group Id

Zeroleak® interactions without leak of persistent Identifier

RFIDsec

Σ sigma

Without PETs, markets wont work
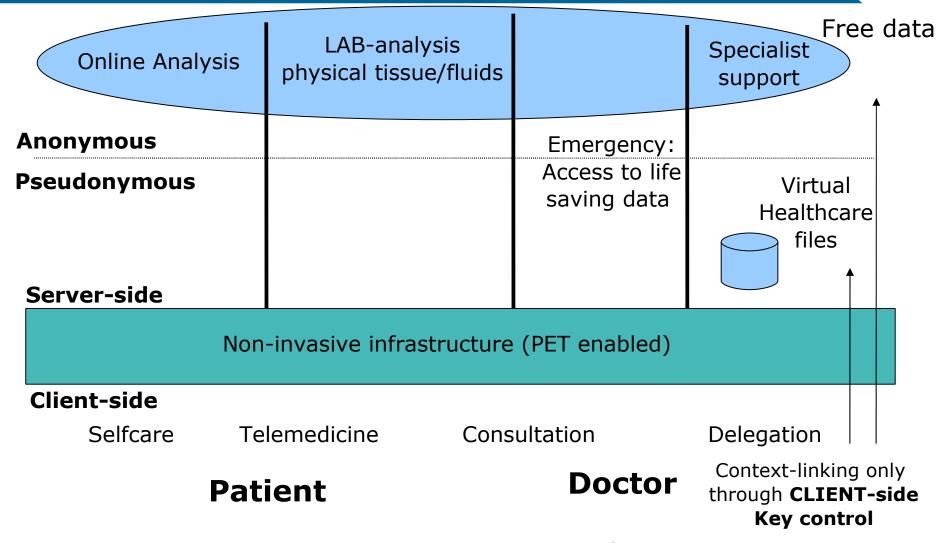
Healthcare security overview
Case: Enabling healthcare with PETs
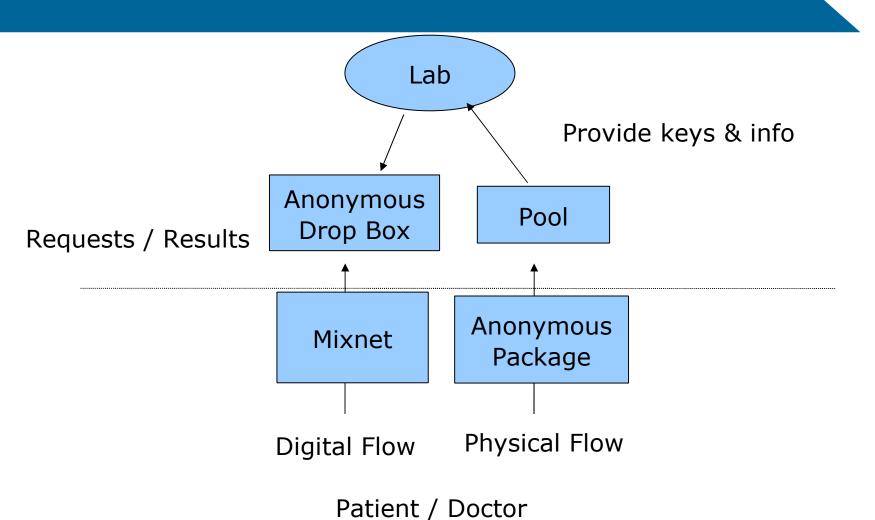
Free data

Online Analysis | LAB-analysis physical tissue/fluids | Specialist support

Anonymous

Pseudonymous

Emergency: Access to life saving data

Virtual Healthcare files

Server-side

Non-invasive infrastructure (PET enabled)

Client-side

Selfcare   Telemedicine   Consultation   Delegation

Patient

Doctor

Context-linking only through **CLIENT-side Key control**

k

Lab

Provide keys & info

Anonymous Drop Box

Pool

Requests / Results

Mixnet

Anonymous Package

Digital Flow

Physical Flow

Patient / Doctor
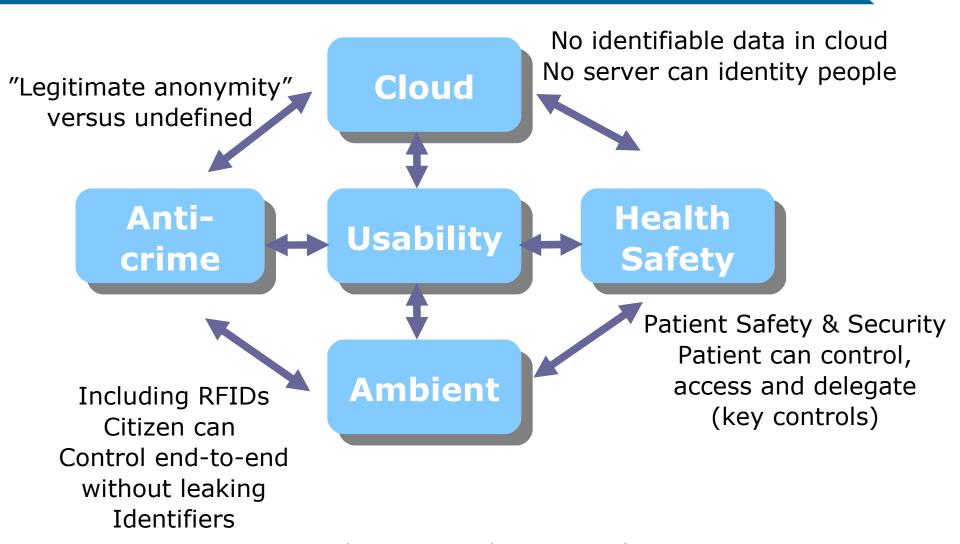
Without PETs, markets wont work

Complex Challenges

"Legitimate anonymity"
versus undefined

No identifiable data in cloud
No server can identity people

Cloud

Anti-crime

Usability

Health Safety

Ambient

Including RFIDs
Citizen can
Control end-to-end
without leaking
Identifiers

Patient Safety & Security
Patient can control,
access and delegate
(key controls)

Without PETs, wont work

16

PET Society Business Case

PETs are critical for trust through maintaining consumer control
- Consumers choice to share depend on risk assessment
- With PETs consumers can "punish" and revoke data use

Demand Empowerment is driving efficiency & innovation
- Enable needs-driven free use of data (non-identifiable)
- Enable markets to self-adjust & recover from minor failures

PET part of Security by Design – no security without privacy
- Cheap & effective security through infrastructure
- Service provider CANNOT secure his service alone !!!

Market principles, rights and law enforced by design
- Prevent concentration of market dominating powers
- Prevent profiling – both commercial, public and political

Without PETs, markets wont work

Conclusions
We can (must) empower Demand

- Markets cannot overcome negative externalities of eID
- Profiling is eroding markets, democracy & efficiency
- "Cartel" standards block competition & innovation

- PETs are future oriented, stabilising & driving innovation
    – make it possible to "drop past profiling and leakage"
    – enable transactions while minimising secondary risks
    – force markets to focus on actual preference & adjust

- Political – invest in society interests - PET National ID 2.0
    – Prevent instead of trying to control & protect
    – Focus first on commerce and public services
    – Help SMEs innovate - open gatekeeper cartels
    – Public administration holds the largest potentials

Without PETs, markets wont work