Foretræde
Udvalget for Digitalisering og IT

INPUT TIL DIGITALISERINGSSTRATEGI

med eksempler fra
ZafeLoc, Priway Trustworthy Cyberdefence og CitizenKey

Catharina og Stephan Engberg

Priway Trustworthy CyberDefence

- Coordinate or fail
- If they can see you, they can kill you
- Adapt or die

Vi skal sikre vores børn og unge i fredstid med de samme midler som vi bruger til at sikre vores soldater i krigstid

Trustworthy Identitet og datadeling er nøglen til al digitalisering

ZafeLoc – Sikring af unge

Anonyme Lokations-baserede services

Deler færden op i en serie anonyme sessioner
Som udgangspunkt ”i nærheden af x”

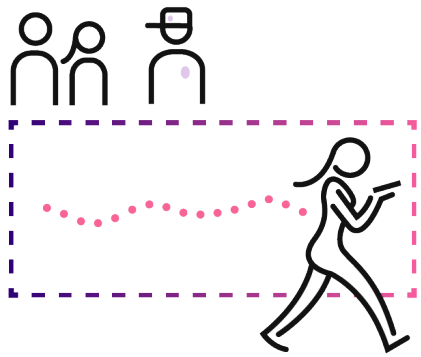
Tryghed uden overvågning – Private Guardian

Samvær uden indblanding – Private Groups

Handel uden dataindsamling – Private Marketing

Private Guardian

- Brugeren kan efterlade brødkrummer – dobbelt-krypteret lokation
- Deres guardians kan frigive til politiet, så politiet kan åbne
- Ingen kan overvåge, men hjælpen kan komme hurtigt i en nødsituation



Trustworthy digitalisering – Billigere og bedre på samme tid

ZafeLoc finansieres af anonyme data

- Anonyme lokationsbaserede markedsundersøgelser
- Anonyme tilbud / event services
- Anonyme abonnementer til lokale medier

Borgeren kan sammenstille anonymt

- Anonyme rejsemønstre til analysebrug. Borgeren kan sammenstille flere anonyme sessioner til anonyme rejser med den nødvendige blurring

SmallData
Reelt anonyme data
sammenstillet anonymt
på tværs af kilder
af borgeren

Bedre end BigData !

Trustworthy Identitet skaber værdi

Basic
Anonym app med samtykke og alderscredential

Anonyme services – Safety, convenience, marked
Alders-credentials
Mål: at rulle ud til alle børn og unge hurtigt

Trustworthy PKI (lokal)
Basic supporteret med hardware

Ansvarlighed / Lovlig logning
Trustworthy Unilogin
Forsvaret

Qualified Trustworthy PKI
eIDAS certificeret digital signatur / identitet

Trustworthy MitID
Trustworthy AI
Marked, demokrati og offentlige services

Logning

Man diskuterer:

Ansvar uden Frihed vs Frihed uden Ansvar

Man burde diskutere:

Frihed under Ansvar

Trustworthy logning på transaktionen – ikke på personen
Betinget identifikation, dvs. dommeren har data minimeret adgang til at ”de-anonymisere”.

Vi kan redde ofre bedre og hurtigere uden overvågning

Offer:

- Borgere kan selv sikre egen safety UDEN overvågning
  - Private Guardian sikrer sporbarhed til sidste sekund → hurtig hjælp v. ulykker etc.

Vidner / gerningsmænd:

- Tilvalg af Lovlig Logning → Ingen mastelogning
  - Logning på Transaktionen – IKKE på personen (Retshåndhævelsesdirektivet art 20)
    - Politiet kan indsamle alle trustworthy sessioner ”i nærheden” (stoppe uret/sikre beviser).
    - Dommeren kan lukke op for deres præcise lokation (behov valideret af gerningen)
    - Derefter kan dommeren de-anonymisere de relevante (uden overvågning af ikke-involverede)
- Trustworthy specifikke behov
  - F.eks. Trustworthy Roadpricing kan gennemføres trustworthy anonymt med ansvar for anti-crime
  - Manglende trustworthy validering kan så aktivere f.eks. CCTV

Trustworthy digitalisering *Oftest bedre og billigere løsninger på samme tid*

- Eksamener med online adgang uden overvågning af individet
- Trustworthy AI uden persondata
- Skole IT – anonym adgang til nettet delt med egen lærer
- Bopælsbeviser
- Anonym sundhedsforskning
- Anonym adgang til selv sensitive data, f.eks. Babysam / graviditet
- Trafik / roadpricing inkl. samkørsel
- Allibier
- Rejsefradrag

Input til Digitaliseringsstrategi

- Retten til egenkontrol over egne data
  - Flag i CPR-registeret – ”Forbud mod samkøring / borger bidrager trustworthy”
  - Ret til adgang til egne data ved kilden (GDPR art 20 / Data Portabilitet)

- Håndhæv trustworthy digitalisering (GDPR art 25 – Data minimering)
  - Opgrader MitID og Unilogin med eIDAS pseudonyme / anonyme signaturer
  - Hvis borgeren kan, så SKAL it-systemer kunne håndtere ikke-CPR-henførbare processer
  - Lav D-Dag – Demokrati-Digitaliseringsdag, hvor it-systemer SKAL understøtte

- Ryd op i den megen lovsjusk og dårlige digitalisering i Danmark
  - Start med de to lovforslag i regi af Udvalget

.

Digitaliseringsmyter

- at overvågning skaber sikkerhed, heller ikke for nationen eller ofre.
- at sammenkøring er nødvendig for kontroller mod social svindel
- at overvågning og sammenkøring er nødvendig for forskning.
- at statens opsamling af CPR-data effektiviserer den offentlige sektor.
- at MitID øger sikkerheden

Hvis du støder på nogle af disse misinformerende påstande, så bed vedkommende dokumentere hvorfor det sekundære behov ikke kan dækkes bedre trustworthy ! ← Retskrav (GDPR art 35)

CPR-data er ikke Danmark styrke – det har længe været vores voksende svaghed.

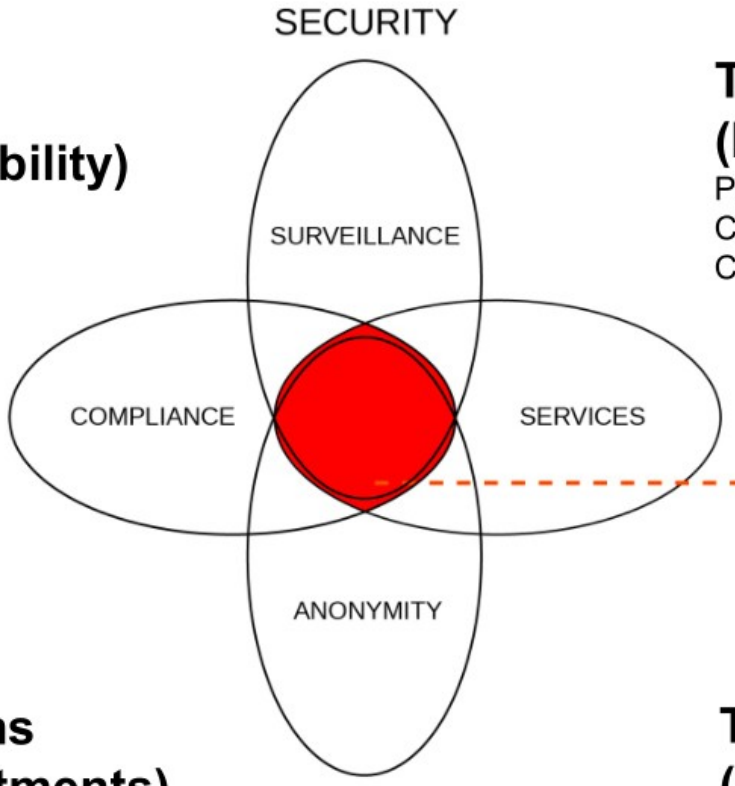
Hensigten helliger IKKE midlet

Primary	Secondary
Citizen Security	Law Enforcement
Citizen Choice	Learning & Research
Citizen Rights	Taxation
Market ability to work / competition	Innovation/effectiveness
Democracy	Social cohesion / Environment

Systemejere og særinteresser tenderer til at vælge it-design, der prioriterer de sekundære interesser, men samtidig skader alle de primære hensyn – demokrati, marked, rettigheder kan ikke fungere uden reel sikkerhed og selvbestemmelse mod BigTech og BigGov

Gældende lovgivning siger, at det må man IKKE, medmindre det er STRENGT nødvendigt for lovgivne legitime interesser. Med trustworthy digitalisering er det sjældent nødvendigt !

ALLMOST ALL SOCIETY WORK BETTER TRUSTWORTHY



Trustworthy Secure
(Trustworthy Accountability)
Freedom with Accountability

Trustworthy Hybrid
(Intimate sharing with proof)
Patient send datalink to doctor
Citizens share with social group
Citizens share with self / guardian

Trustworthy Restrictions
(Inddirect proof/commitments)
Schengen
Finance KYC/AML
Taxation

Trustworthy Anonymous
(Consentual anonymity)
Elections
Data research/AI training
Searches / access content

Gradvis omlægning starter med retskravet om egenkontrol i design