Hvilke muligheter gir teknologien for at den enkelte skal kunne velge et personvern som samsvarer med individuelle ønsker?

Ragni Ryvold Arnesen

Seniorforsker, Norsk Regnesentral

Ragni.Ryvold.Arnesen@nr.no

Hva vil folk ha?

- Folk er generelt opptatt av personvern
- Vil ikke oppgi personopplysninger på Internett
- Men mange oppgir personopplysninger likevel for å få en vare eller tjeneste de er interessert i

=>Vil ha god beskyttelse av personlig informasjon, men muligheten til å velge annerledes i spesielle tilfeller

Dagens situasjon

- Som regel bare to valg:
  - Oppgi personlig informasjon, eller la være å gjøre det
- P3P: http://www.w3.org/P3P/
- Individuelle valg i form av samtykke eller reservasjon er lite utbredt
- Generell praksis må gjelde alle, og dermed være strengere enn mange ønsker
  - Mange nyttige, personaliserte tjenester er umulig å tilby

Hva må teknologien tilby?

- Minimere mengden innsamlet informasjon
  - Anonymisering, pseudonymisering, la være å samle inn
- Individuelle valg: Støtte for, og sammenheng mellom, alle steg i prosessen fra ønske til oppfyllelse:
  - Definering av personlig personvernpolicy
  - Overføring av policy til de som skal etterleve den
  - Håndheving av personvernregler og -policy
  - Deteksjon og reparasjon av brudd på personvern

Personvern policy

- Personvern policy ≈ Aksesskontroll policy
- *Formålet* med databehandlingen er viktig
- Må defineres i stringent, maskin-tolkbart språk
  - F. eks. EPAL laget av IBM
  - ”Hvem kan gjøre hva med hvilken type informasjon, med hvilket formål, under hvilke betingelser og med hvilke påfølgende forpliktelser”
- Trenger verktøy for å kunne gjøre det gjennomførbart for folk flest
- Behov for raske oppdateringer av policy, avhengig av situasjonen

Overføring av policy

- Personlig policy må gjøres tilgjengelig for de som skal etterleve den
  - Dvs. bedrifter, organisasjoner, etater osv., som eier og bruker databaser med personinformasjon
- Standardisering er nødvendig
  - Overføringsmetoder
  - Vokabular

Håndheving av personvern

- Automatisering
  - Trenger systemer som kan lese en policy og avgjøre forespørsler om tilgang til data
- Hvordan avgjøre hvilket formål datatilgangen har?
- Utvidet adgang til data krever gode sikkerhetstiltak
  - Autentisering
  - Konfidensialitet
  - Integritet

Deteksjon av brudd på personvern

- Innsyn i data, hvor de kommer fra, hva de blir brukt til
  - Mest mulig automatisert
- Automatisk deteksjon av unormal oppførsel i systemet
  - Anomalideteksjon med statistiske metoder som ”lærer” hva som er normal oppførsel
  - Sammenholde ulike datakilder: aksesshistorie, policyer, logger

Advarsel til slutt

- En personvern policy kan i seg selv være meget sensitiv
  - Sier mye om personens liv, ønsker og behov
- Muligheten til å gjøre individuelle valg kan også lede til ”valgpress”
  - Gruppepress blant ungdom
  - Sjalu ektefeller
  - Aggressiv markedsføring