

Privacy og biometri

Henning Mortensen

hem@di.dk

www.itek.di.dk

Teknologi tjener os



Kritik af teknologier er baseret på uhensigtsmæssige implementeringer - ikke på teknologiske fejl

Eksempler:

- Roadpricing
- Biometri
- Betaling

Enhver teknologi kan indrettes så den respekterer privacy

Biometriens velsignelser



Lethed

- hjemmet genkender dig
- bilen genkender dig
- din arbejdsplads genkender dig
- dit flyselskab genkender dig

Ekstra lag af sikkerhed

- hjemmet lukker af for andre
- bilen starter ikke
- din arbejdsplads ved hvem der er der
- du kommer hurtigere igennem tjeck in

Udfordringer

Der er en række udfordringer

- modenhed - bedre teknik og funktionalitet
- pris - på vej mod integreret commodity
- anvendelsesområder - mere let end sikker
- oversalg i branchen + fiktion - realisme
- særlig etiske overvejelser - kropslig integritet
- privacy - løst nogle gange, som anden teknologi

Privacyanalogi til RFID



Generelt er der behov for at arbejde med privacy i forbindelse med teknologier

- brugernes kontrol

privacy bør inlejres i arkitekturen
information til brugerne

brugeren skal kunne kontrollere teknologien og have samme muligheder uden teknologien

- personlig integritet

skiltning, krav til brugervenlighed, beskyttelse af personhenførbare oplysninger
"best practice" til anvendelse fra erhvervet

- interoperabilitet

teknologier bør kunne fungere sammen
åbenhed omkring internationale spilleregler

- brugervenlighed

intuitivt at håndtere
åbne standarder
forskning i brugervenlighed

- bæredygtige tags

håndtering af elektroniskrot
støtte til udvikling af miljøvenlige alternativer

Hvorfor DI og privacy?



- at stimulere en offentlig dansk debat
- at tydeliggøre nogle af de sammenhænge, hvor man skal vogte over sin privacy - og dermed beskytte borgere og virksomheder (brugere)
- at give en opfordring til teknologileverandørerne om at efterleve de skitserede principper og udvikle løsninger, som efterlever privacy
- at sætte fokus på mulighederne for en særlig dansk nicheindustri indenfor privacy

Aktører



En række organisationer og virksomheder er interesseret i emnet

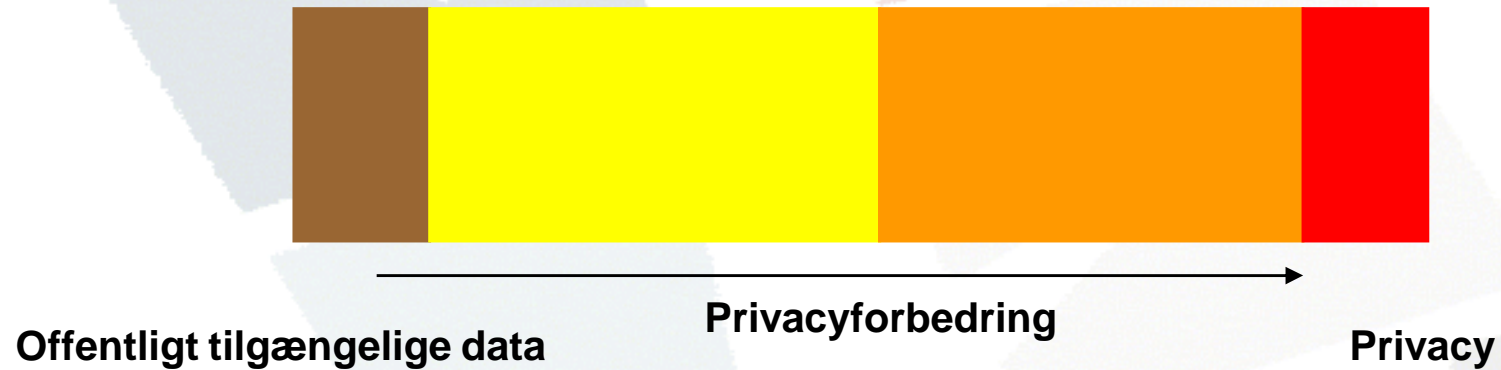
CSIS	Forbrugerrådet
GN	Institut for menneskerettigheder
IBM	Human Rights
Logisys	Finansrådet
Microsoft	VTU's IT-sikkerhedspanel
Nensome	IT- og Telestyrelsen
P&K sikkerhed	Forsvarets
RFIDsec	Forskningsstjeneste
Siemens	AIM Danmark
TDC	HK / FTF / Metal
Unispeed	ITEK / Dansk Industri
Zebranet	

Privacy

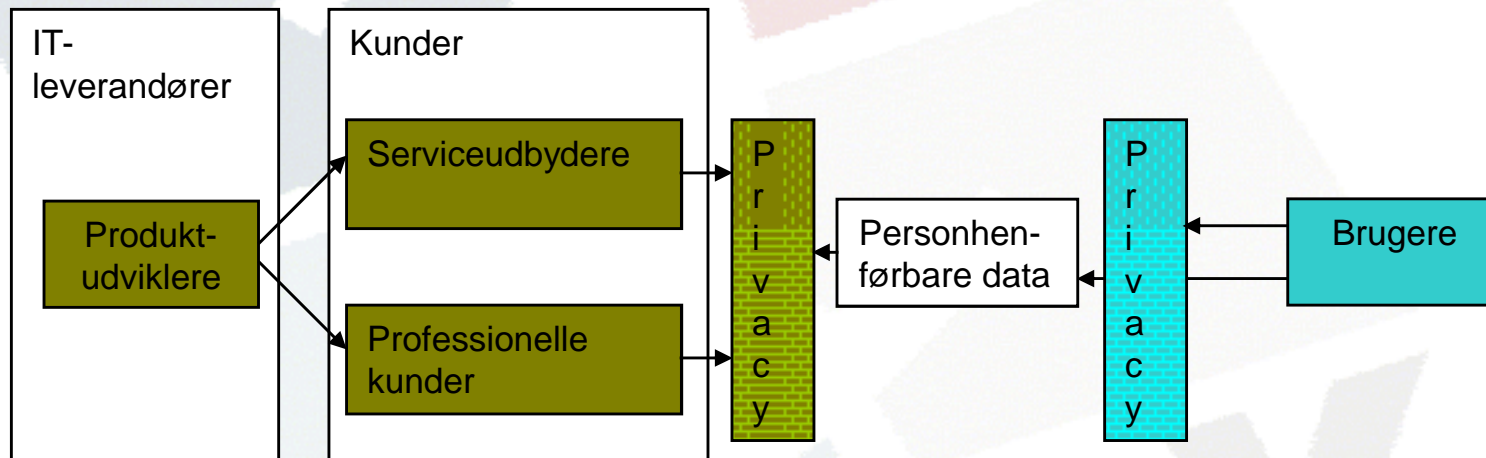
Forskellige definitioner af privacy

- Retten til at være alene – Louis Brandeis
- Fysisk frirum, uden forstyrrelser, indtrængning, blive sat i forlegenhed eller blive holdt ansvarlig for vores handlinger – Robert Ellis Smith
- Retten til at indsamle, vedligeholde, anvende, videregive/transmittere og behandle personlig information - EPIC
- Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance - EU

Model for privacy



Roller



Kilder

De "vigtigste" kilder er gennemgået, men det er ikke et litteraturstudie. I hovedtræk er der tale om følgende kilder:

- OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Europarådet: Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention
- EU: Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Danmark: Lov om behandling af personoplysninger

Principper for privacy



Brugerne skal kunne styre anvendelsen af data (3)	Dataindsamlingen skal være fair	Dataindsamlingen skal være lovlig	Dataindsamling skal ske med viden fra brugeren	Dataindsamling skal ske med accept fra brugeren
	Dataindsamling kan være krævet af en kontrakt, loven, hensyn til brugeren og offentlig myndighedsudøvelse (3)	Dataindsamling kræver konkret afgrænset formål	Databehandling må kun finde sted til det formål de er indsamlet	Ved ændret formål skal data destrueres eller anonymiseres
Databehandlerens eventuelle videregivelse af data kræver at brugeren oplyses herom (og giver accept)	Data skal have god kvalitet i betydningen præcise, komplette og opdaterede	Brugeren har altid ret til at få adgang til egne data	Brugeren har altid ret at få indsigt i om en enhed har registreret data og i givet fald hvilke, deres anvendelse, formålet med at have dem og hvor de lagres	Databehandleren skal give indsigt til brugeren på en forståelig måde, indenfor en rimelig tid og til en rimelig pris
Databehandler skal udvise åbenhed overfor brugerens indsigt	Databehandler kan anvende betingelser for brugerens indsigt og i givet fald skal disse begrundes	Brugeren har ret til retslig prøvelse af sammenhæng mellem data og formål, datas kvalitet og eventuel manglende efterlevelse af privacypolitikker (1)	Brugeren har kun ret til indsigt med begrænset frekvens (1)	

Principper for privacy



Databehandler har ansvar for data og disses sikkerhed	Dataflow over grænser er betinget til international handel, anvendelse af elektroniske services og dataflow internt i virksomheder. Dette bør reguleres gennem kontrakter	Databehandler skal sikre at privacyforanstaltninger implementeres under hensyn til det tekniske niveau (2)	Databehandler skal sikre at privacyforanstaltninger implementeres under hensyn til omkostninger (2)	Databehandler skal sikre at der findes en opdateret politik for privacy
Databehandler skal sikre at brugeren med rimelighed er bekendt med politikken og har accepteret den	Databehandler skal anmelde behandling af data til tilsynsmyndighed	De nævnte principper gælder ikke hvis der er særlige nationale interesser, der varetages bedre ved en undtagelse (3)	De nævnte principper gælder ikke hvis der er tale om behandling af kriminelle forhold (3)	
De nævnte principper gælder ikke hvis det vurderes at være i brugerens interesse at undtage dem eller hvis det gælder andre personers frihed (3)	De nævnte principper gælder ikke hvis for særlige faggrupper – herunder anvendelse til historisk, journalistisk, videnskabeligt eller statistisk bearbejdelse (3)	De nævnte principper gælder ikke hvis behandling af data sker ved arbejdsmarkedsforhold, foreninger, allerede offentliggjorte data, sygdomme og særlig lovgivning (3)	Databehandlers videre beskyttelse end de angivne principper er altid mulig	De angivne principper er overordnede og der kan der ske en gradbøjning af dataanvendelse (3)
	De angivne principper er overordnede og der kan der ske en gradbøjning af foranstaltninger (3)	De angivne principper er overordnede og der kan der ske en gradbøjning af risici, som data kan udsættes for (3)		

Eksempel på et princip



Dataindsamlingen skal være fair

En fair indsamling af data betyder at de øvrige principper i denne "best practise" skal overholdes ved indsamlingen af data.

Brugeren må ikke kunne snydes til at afgive data og der må ikke afgives flere data end nødvendigt for formålet.

Processen skal således være fair og gennemskelig overfor brugeren.

Leverandør	Kunde/databehandler
<p>Er formålet med dataindsamlingen tydeligt specificeret?</p> <p>Er løsningen designet så brugeren kun afgiver de nødvendige oplysninger eller indsamles unødvendige oplysninger i den pågældende løsning?</p> <p>Er der gennemført brugervenlighedsanalyser, som sikrer, at systemet virker gennemskeligt for brugeren, så brugeren ikke føler sin privacy krænket?</p>	<p>Er formålet med dataindsamlingen tydeligt specificeret?</p> <p>Kan systemet siges kun at indsamle de oplysninger, der er brug for?</p> <p>Er der dokumentation for at de oplysninger der indsamles er relevante?</p> <p>Kan brugeren føle sig snydt til at afgive informationer eller til at få bestemte services - f.eks. elektroniske nyhedsbreve?</p>

Privacy og biometri



Særligt trusselsbillede

- Man kan ikke ændre sine biometriske data let (modsat f.eks. et password)
- Når først biometriske data er blevet stjålet hænger man på den (i forhold til visse teknologier)
- Der er stadig en "film"-effekt i forhold til denne teknologi: afskåret finger eller udskåret øje
- Hvilke biometriske data er det rimeligt at give fra sig hvornår? Om nogen overhovedet?

Alle principper holder fortsat som lovgivningsmæssigt grundlag!

- Brugere skal i videst muligt omfang kunne styre deres egne data
- Der skal indtænkes teknologier svarende til det aktuelle stade
- Der skal være regler for data-indsamling og behandling
- Brugere skal fortsat have sine rettigheder
- Databehandleren har fortsat en række forpligtelser i forhold til disse data
- Staten kræver fortsat undtagelser - f.eks. ifht nationens sikkerhed

På grund af det særlige trusselsbillede er principperne måske ikke nok

- Som udgangspunkt skal data helst slet ikke indsamles
- Hvis data indsamles skal sikkerhedsmodeller være på plads på forhånd
 - Disse kunne inkludere at originale karakteritika ikke kan genskabes
 - Princippet om relevant formål og tidsbegrænsning
 - Adgang til data
- Der skal være sikkerhed for at de data der indsamles

Politisk perspektiv



Privacyarbejdet under VTU

Rapport om privacy i 2003

Anbefalinger fra VTU's IT-sikkerhedspanel

Møderække om privacy

Fire arbejdsgrupper under møderækken

- Forskning og innovation (institut for grundforskning, udrede holdninger til privacy, innovation - også ifht virksomheder, formidle viden, internationalt udsyn)
- Regulering og arkitektur (tværoffentlig arkitekturgruppe, borgerne bør have kontrol med egne data og identiteter, skabelon for PIA, offentlig tilgængelig privacy politik)
- Internationalt (Dialogforum: nye problemstillinger, erfa-udveksling, særlige danske synspunkter)
- Awareness (casesamling, brugervejledning med bl.a. TOR, materiale til indlæring af privacy, privacypris, privacykonference, awareness om privacy blandt beslutningstagere - f.eks. offentlige og private IT-indkøbere)

Målsætning:

Lave et katalog over mulige privacy initiativer

Få lavet en skabelon for privacy, som bruges af det offentlige ved nye indkøb og som kan spredes til resten af verden.

Privacy i forhold til Finansministeriet

Ændring af digital strategi

Nedsættelse af tværoffentlig arbejdsgruppe til at komme med arkitekturanbefalinger samt evt. PIA

Relevant i forhold til alle politiske områder

F.eks. sundhed (L50B, pas, borgerkort og transport)

Opsummering

- Biometri er en fremragende teknologi, der kan give rigtig mange fordele
- Der er dog en række forhold, der kan gøres bedre i design, og en række krav vi må stille ved implementering
- Principper for privacy bør efterleves
- Brugere bør være i kontrol med teknologien
- Det skal overvejes om der er behov for særlige PET ved implementering i en konkret situation