Universitetet i Oslo
Institutt for informatikk

Masteroppgave

Veileder:
Steinar Kristoffersen

Kandidat:
Arnstein Rosvold Andreassen
(arnsteia)

Personvern med allestedsnærværende teknologier

13. desember 2004

TAKK til

- Steinar Kristoffersen IFI, for veiledning.
- Jørn Hanssen, prosjektleder for billettsystemer, Sporveien i Oslo, for viktig informasjon om forskningsbakgrunnen.
- Gunnel Helmers og Beate Dagslett ved Datatilsynet, for informasjon om personvernaspekter ved transportsystemer.
- Erik Andreassen, Silje Kivle Andreassen og Benedicte Tveter Kivle for korrekturlesing og innspill.

Innholdsfortegnelse

1 Innledning

1.1 Allestedsnærværende systemer

Pervasive computing, *ubiquitous computing*, allestedsnærværende datasystemer: Mange navn for systemer som etterhvert ser ut til å befinne seg - nettopp - alle steder. Vi kan se en økende utbredelse av enheter og systemer som er i stand til å kommunisere med andre enheter, med nettverkssystemer og med mennesker. Og vi ser stadig nye løsninger der livet gjøres enklere ved at informasjon automatisk samles inn.

Automatisk identifikasjon og datainnsamling (AIDC) er en vid beskrivelse på ulike teknologier som blir brukt for at maskiner automatisk skal kunne utføre identifisering. Det er mange teknologier som kan falle inn under en slik definisjon: Noen av dem er strek-koding og RFID-*tags*[1] for unik identifisering av produkter , magnet/smartkort for autentisering og betalingsløsninger, samt bilde- og stemmegjenkjenning. Mobiltelefoner og trådløst utstyr kan brukes til lokalisering og identifisering. Leverandører av mobiltelefoni må til enhver tid vite hvor i basenettet en mobiltelefon befinner seg, for å kunne rute innkommende samtaler til telefonen, samt tilby brukeren utgående tjenester. Teknologier for å lokalisere telefoner i tettbygde strøk til 1-3 meter eksisterer[2]. Det samme gjelder for trådløse enheter i WLAN soner.

1.2 Hva er nytt?

Men hva er egentlig nytt med denne nye teknologiutbredelsen? Radiomerking og sensorteknologi har eksistert minst siden 2.verdenskrig. Mobiltelefoni og nettverk har vi også begynt å venne oss til i løpet av de ti siste årene.

Det som først og fremst er nytt er den store *mengden* av innsamlet informasjon. Teknologier som kanskje i utgangspunktet er tenkt for å kunne holde orden på varer i en produktlinje kan også brukes for å tilby mennesker nyttige og verdiskapende tjenester, basert på informasjonen som samles inn via de elektroniske enhetene de bærer med seg og benytter seg av. I tillegg ser vi en økende integrasjon av systemer, med dertil økende integrasjon av informasjon som disse systemene samler inn.

Noen snakker også om at teknologiene konvergerer. Dette kan altså innebære at teknologi som tidligere var forskjellig nå smelter sammen og blir det samme og tilbyr overlappende tjenester, eller at den samme teknologiske enhet kan utfylle mange ulike funksjoner.

Vi ser også en økende utbredelse av kommunikasjonsenheter som mer eller mindre sømløst kan benytte seg av de trådløse nettverk som til en hver tid skulle være tilgjengelige, slik som WLAN, Bluetooth, GSM, GPRS, EDGE og UMTS. Dette gjør at vi kan ha konstant tilgang til Internett og andre nettverk. Vi kan også være konstant tilgjengelige.

1 *Radio frequency identification (RFID)* er en type automatisk identifikasjonsteknologi som bruker radiobølger for å identifisere fysiske objekter som er merket med elektroniske *tags*.
Se kap 4.1.3 og [1], [2] og [3] for mer informasjon om RFID teknologi.

2 Se for eksempel http://www.radionor.no/ (Sett des.2004)

1.3 Problemstilling

En side med denne økende innsamlingen av informasjon er at den ikke bare tilbyr tjenester til enkeltpersoner, den kan også brukes til sporing og overvåking av personer. Løsningene som gjør livet lettere for oss og som forbedrer produktlinjer kan altså også utgjøre en trussel for vår rett til personvern.

Retten til personvern er nedfelt i Menneskerettighetene, artikkel 12 :

Ingen må utsettes for vilkårlig innblanding i privatliv, familie, hjem og korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike angrep.

Systemer som kontinuerlig samler inn informasjon om vår identitet, lokasjon og aktivitet kan potensielt brukes til slik utidig innblanding. Det er mange parter som kan ha interesse av slik innblanding: Myndigheter kan ha behov for å lete etter for eksempel lovstridige aktiviteter, bedrifter vil gjerne kartlegge behov og interesser for å drive aktiv markedsføring, kriminelle vil kanskje finne ut hvor det finnes verdier eller om eieren av et hus er hjemme. Det kan også være snakk om å respektere ønsker om ikke å være tilgjengelig og sporbar, nettopp fordi dette er en menneskerettighet.

Det er dermed åpenbart et behov for å beskytte informasjonen som slike systemer muliggjør innsamling av. Min problemstilling som jeg vil utdype i denne sammenheng er:

Kan eksisterende konsepter og systemer for personvern fortsatt brukes når det ser ut som teknologien og innsamlingen blir allestedsnærværende?

1.3.1 Trusler mot personvern i allestedsnærværende systemer

Trusler mot personvern finnes også i de eksisterende systemer som er sagt å konvergere eller som integreres. For datanettverk har det vært mye fokus på utvikling av sikkerhet for å beskytte systemer og sensitiv bedrifts- og personlig informasjon. Spesielt har dette blitt viktig som følge av opplevde problemer og informasjon som kommer på avveie som følge av virusangrep og innbrudd gjennom datanettverk. Dette har ført til at mange med rette er bekymret for at noen skal kunne snappe opp informasjon som blir sendt over nettverk, eller at noen skal bryte seg inn på maskiner for å stjele informasjon.

Fokus har dermed vært på å bedre på disse forholdene, ved å tette sikkerhetshull i kommunikasjonssystemene, og å utvikle adgangskontrollsystemer og protokoller for mer eller mindre sikker lagring og kommunikasjon.

Görlach et al. har i [4] presentert flere mulige trusler mot portabelt elektronisk utstyr. De mener at hovedbekymringen er at det nye teknologibildet med automatisk datainnsamling gjør det mulig å også drive automatiske angrep på personvernet. Et slikt angrep er en suksess når en angriper har fått tak i informasjon som det ikke var meningen at han skulle ha tilgang til. Og det er ikke bare problemer med sikkerheten som gjør at informasjon kan komme på avveie.

Informasjon kan skaffes på fire ulike måter: *første og annenhånds kommunikasjon*, *observasjon* og ved *inferens*. *Inferens* er definert som å dra statistiske slutninger om identitet, lokasjon og

andre persondata på grunnlag av ellers uidentifiserbar informasjon.

1.3.1.1 Førstehånds kommunikasjon

Førstehånds kommunikasjonsangrep forekommer når et individ eller en enhet gir fra seg informasjon direkte til angriper, enten ved et uhell, ved en feil, eller ved å bli lurt til å tro at mottaker er en annen enn han virkelig er.

Mange kjente feil i elektroniske enheter kan utnyttes til å skaffe informasjon: Enhetene lærer ikke selv om samme angrep gjøres mange ganger. Silke angrep kan gjøres automatisk, og er blitt svært utbredt for eksempel i Internett, kjent som virus av ymse slag, eller som spion-programvare som eksplisitt er til stede for å stjele informasjon som er lagret på maskinen, eller fra brukerens aktivitet.

En viktig del av sikkerhetssystemene som er utviklet angriper denne problemstillingen ved å sperre kjente sikkerhetsproblemer, og innføre streng adgangskontroll med bruk av krypterte passordsystemer og sertifikater, for å unngå at informasjon blir utlevert til feil vedkommende.

1.3.1.2 Observasjon

Beslektet med førstehåndskommunikasjon er observasjon, altså å passivt lytte til eller se på handlinger som blir gjort eller kommunikasjoner som blir ført.

Mange protokoller er utviklet uten spesiell tanke på slike problemer, eller har *bugs* som lar seg utnytte. For eksempel er WLAN protokollen lagt opp slik at trådløse kommunikasjonskort periodisk kringkaster sin unike MAC-ID for å opprettholde kontakt til nærmeste aksesspunkt. Potensielt kan alle høre denne kringkastingen, og dermed spore maskinens identitet. All informasjon som blir sendt trådløst over nettverk kan også høres og kopieres av andre som eventuelt skulle lytte, ukryptert informasjonen kan forstås i klartekst, og kryptert informasjon kan dekrypteres, dersom krypteringen ikke er avansert nok.

Informasjonen som samles inn ved slik passiv lytting kan også brukes til å lokasjonsbestemme trådløse enheter, både mobiltelefoner og WLAN kort, ved hjelp av en metode kjent som triangulering: Ved å måle tidsforsinkelse på signaler som går til ulike basestasjoner eller aksesspunkt kan man beregne seg fram til mer eller mindre nøyaktig posisjon for den elektroniske terminalen, bare ved å vite fysiske egenskaper ved elektromagnetiske bølger.

Det finnes store miljø, spesielt innenfor militære forskningsgreiner, som bekymrer seg for hvordan man kan beskytte informasjon i nettverk. Det finnes systemer for hvordan man kan få kommunikasjon til å høres ut som støy, hvordan man kan fullstendig maskere hvem avsender og mottaker er, hvor disse befinner seg, og om de i det hele tatt sender og mottar data.

En ting er observasjon på datanettverk. Informasjon om hva som er fysisk hørt og sett kan også fanges opp. Telefonavlytting har lenge vært i bruk, men utbredelsen av små opptagere, gjerne integrert i mobiltelefoner og ikke minst mobiltelefoner utstyrt med kamera medfører observasjoner av alle slag som tidligere ikke var mulig. I noen land i Asia har

snikfotografering blitt et så stort problem at det har blitt et krav om at telefoner med kamera skal ha så høy lyd ved fotografering at det er lett å høre at et bilde blir tatt.[3]

En annen måte å samle inn visuelle observasjoner av et stort antall personer er overvåkingskameraer. Mange av disse er så og si usynlig plassert i bymiljø og butikker, og er som regel plassert for å hindre eller hjelpe til med oppklaring av kriminalitet. Likevel fanger de også inn alle andre, og med utvikling av systemer for ansiktgjenkjennelse kan slike observasjoner også automatisk samle inn informasjon om en persons bevegelser.

Observasjon er et stort tema, og det blir ikke mindre når teknologien blir allestedsnærværende.

1.3.1.3 Annenhånds kommunikasjon

Ved førstehånds kommunikasjon har sluttbrukeren potensielt mulighet til å bestemme hva slags informasjon han vil frigi, og forsøke å beskytte denne informasjonen fra å bli observert av tredjepart. Annenhånds kommunikasjon dreier seg om situasjoner der man mer eller mindre frivillig har kommunisert med for eksempel en bedrift, og der denne bedriften sprer eller selger informasjon vi har gitt fra oss til en tredjepart, som igjen kan spre den videre. Dette kan være kontaktinformasjon som navn og adresse, informasjon om kundeforhold og kjøp, eller kanskje helseinformasjon. Opplysninger som blir spredd på denne måten er ute av kontroll i forhold til den personen som informasjonen omhandler. Eksempelvis kan også informasjon vi gir fra oss, eller hvordan vi oppfører oss og navigerer på Internett fanges opp av de nettstedene vi besøker eller av spion-programvare. Denne informasjonen kan så selges videre som kunnskap om våre interesser og vaner. Dette er informasjon som kan brukes f.eks. i direkte markedsføring. Det er nærliggende å tenke seg at lokasjonssporing kunne brukes på samme måte.

1.3.1.4 Inferens - datamining og statistiske slutninger

Den totale informasjonen som samles inn kan kombineres. Informasjon som hver for seg er anonym eller *pseudoanonym* (delvis-anonym) kan identifiseres ved å bruke mer eller mindre intelligente dataminingteknikker og krysskobling av registrere og annen informasjon. I mange situasjoner er slik krysskobling ulovlig, men det er likevel mulig. På denne måten kan man danne seg en profil av mange personer, og derav dra slutninger om en person. Med nok data kan hele livet til en person være kartlagt. Dette kan i verste fall brukes til å dra slutninger som kan føre til diskriminering, for eksempel basert på helseforhold, legning, religion eller politiske synspunkter.

1.3.2 Teknologiske løsninger mot sosialt misbruk?

Det virker som det er vanskelig å gardere seg mot disse to siste truslene. Noen vi har

3 Elisabet Dalseg i Din Side 2.november 2004: http://www.dinside.no/php/art.php?id=111642 (Sett des.2004) "Høy lyd mot kikkere: .. I flere asiatiske land diskuteres nå en ny og bokstavelig talt høyere standard for lyd når man tar bilder med mobiltelefoner. Det skal ikke være lett å ta bilde av andre uten at de er klar over det. Diskusjonen oppstod i Japan da det ble oppdaget at en rekke menn gjorde sport i å ta bilder oppunder skjørtet på skolepiker mens de sto i fullstappede T-banevogner. Til egen eller andres glede. Nå er det påbudt med et visst lydnivå som indikerer når et bilde blir tatt med en kameramobil..".

kommunisert med deler informasjon med tredjepart. Noen bruker delvis informasjon de skulle ha til å beregne identifiserbar informasjon. Sosialt sett er dette som å fortelle hemmeligheter og grave i informasjon som ikke var ment for andre parter.

Det er mulig at disse truslene er mer et spørsmål om misbruk av tillit enn leting etter teknologi som kan verne oss.

1.3.3 Konvergens av systemer?

Noen mener at utbredelsen av elektroniske enheter med muligheter for kommunikasjon og lokasjonsbestemmelse er et resultat av en konvergens eller integrasjon av ulike systemer vi kjenner fra før.

En karakteristikk av *ubiquitous* systemer fra Bellotti og Sellen, 1993 [5] sier (oversatt):

"I økende grad ser vi at systemer har innebygde sensorer, slik som mikrofoner, kamera, og signalmottakere for trådløs kommunikasjon. Disse sensorene har potensiale til å sende og motta informasjon slik som tale, videobilder eller signaler fra andre portable enheter, fra *active badges*, elektroniske oppslagstavler og så videre. Disse enhetene kan settes sammen i nettverk slik at multimediainformasjon kan lagres, gis tilgang til, behandles og distribueres på mange måter. Disse tjenestene inkluderer levende kommunikasjon med lyd og bilde, søk og fremhenting av informasjon, dagbok og kalender system, dokumenthåndtering og så videre."

Denne visjonen eksisterer i dag og heter mobiltelefoni, distribuerte nettverk og Internett.

Min tilnærming i denne oppgaven er å se på noen aspekter ved hvordan man tar vare på personvern i de systemer som finnes og som konvergerer, samt å se på noe av det arbeidet som allerede er gjort for allestedsnærværende systemer.

1.3.4 Oppsummering

Så langt har jeg sett på noen egenskaper ved de allestedsnærværende systemene som er i ferd med å omgi oss. Vi ser at disse skaper omfattende infrastrukturer for identifikasjon og lokasjonsbestemmelse, og jeg har spesielt pekt på noen av de potensielle og faktiske truslene vi kan se mot personvernet når dette skjer. **Ut fra en slik bakgrunn håper jeg å finne ut om de eksisterende konsepter og systemer for personvern fortsatt kan brukes når det ser ut som teknologiene konvergerer og blir allestedsnærværende.**

1.4 Tidligere arbeider

Det er mange miljøer som fokuserer på allestedsnærværende systemer. Det arbeides på alle nivåer som må fungere for at at systemene skal bli allestedsnærværende, fra sensorer, innebygde trådløse og trådbaserte nettverkssystemer, via såkalte "smarte " teknologier, bevissthetssystemer, arkitekturmodeller, til modeller for bruk og brukergrensesnitt.

Mange av disse miljøene fokuserer på sikkerhet, og noen av dem har også gjort arbeid omkring personvern. Et stort miljø jeg har konsentrert meg om er CSCW, eller *Computer Supported Colloborative Work*. Disse er spesielt opptatt av samarbeidssystemer, og har utviklet en del konsepter for hvordan slike systemer fungerer og hva som regulerer dem, også i

forhold til personvernhensyn. Jeg har brukt blant andre Palen og Dourish [6] og Eamonn O'Neill [7] som bakgrunn for reguleringsmekanismer, og Bellotti og Sellen [5] har gjort viktig arbeid omkring kontrollmekanismer for bruk i personverndesign. Jeg har også brukt Liechti [8] og Gutwin & Greenberg[9] for beskrivelser av mekanismer og konsepter for *awareness* systemer.

Personvern er jo i stor grad et ikke-teknisk tema, og jeg har sett på hvordan internasjonal og norsk lov og rett er med å regulere hvordan informasjon kan deles. Spesielt er dette *US Privacy Act* med *fair information practice* [10]og EU-lovgivning 95/46/EC: *The Directive* [11]. I Norge har vi Personopplysningsloven [12], og Datatilsynet[13] som overvåker at denne blir fulgt.

Et miljø ved Internett-organisasjonen *World Wide Web Consortium (*W3C) har jobbet med å utvikle standarder for utveksling av politikk for personvern, P3P[14] og APPEL[15]. Marc Langheinrich har gjort mye arbeid for å utvikle designprinsipper[16] bak disse standardene, og har foreslått en løsning for hvordan disse kan brukes i allestedsnærværende systemer[17].

Miljøer innen industrien har også forslått løsninger basert på W3C standardene , blant andre Cranor et.al [18] ved AT&T, og Karjoth [19] og Bohrer [20] ved IBM.

Innen sikkerhet er mye arbeid gjort innen matematiske miljøer for kryptering, og jeg refererer til Couloris [21], samt til miljø for *Information hiding.* Disse har konsentrert seg om usynliggjøring og dekobling av sendere, mottakere og informasjonen som går mellom dem. Jeg refererer til blant andre Hong et.al. [22], Gruteser et.al. [23], Chaum [24], Federrath[25]og [26]og Beresford [27].

Allestedsnærværende systemer inkluderer ofte trådløs teknologi, og jeg har sett på standarder og beskyttelse for RFID teknologi , blant andre fra AutoID senteret ved MIT [2], Juels et.al [28], og Sarma et.al. [29]. Jeg har også sett på sikkerhetsaspekter ved *Smardcard*, Sheifer et.al [30].

I tillegg finnes det store miljøer som konsentrerer seg om teknologi, sikkerhet og sosiale aspekter ved bruk av mobiltelefoni (*Mobicom*), og jeg har brukt Tisal [31], Palen et.al.[32], Ljungstrand et.al[33], Barnes [34] som kilder. I tillegg har jeg sett på Snekkenes [35] løsningsforslag for å verne om personvern basert på dagens mobilnettverk.

Hong og Landay [36] har presentert et løsningsforslag som de mener benytter seg av de beste innspillene fra mange av disse miljøene, og presenterer et system som de mener kan ta vare på personvernet i mange domener for allestedsnærværende systemer.

En annen som har presentert et *survey* over løsningsmodeller for allestedsnærværende systemer er Görlach et.al.[4].

Mitt bidrag i forhold til alle disse er å se på om modellene og løsningene som er presentert i disse miljøene kan fungere for systemer som driver automatisk datainnsamling, spesifikt testet på min forskningsbakgrunn med innføringen av et elektronisk billettsystem.

1.5 Metode

Mitt arbeid har vært fokusert på å sette meg inn i konsepter og teknologier omkring

personvern. Spesielt har jeg sett på de tilfeller der teorier og teknologi kan komme til anvendelse i situasjoner med utvidet automatisk datainnsamling, som beskrevet i min problemstilling. Første del av arbeidet gikk dermed på å beskrive teorier og lage et *survey* av noen eksisterende teknologier.

I samråd med veileder fant jeg så ut at jeg trengte et konkret eksempel å knytte opp til personvernutfordringene rundt allestedsnærværende systemer. Derfor tok jeg 29.oktober 2004 kontakt med Sporveien i Oslo for å forhøre meg litt om det elektroniske billettsystemet vi hadde hørt at de hadde under utvikling. Der ble jeg henvist til prosjektdirektør Magne Glomnes, som igjen henviste meg videre til prosjektlederen for billettsystemet , Jørn Hanssen, som ifølge Glomnes satt med de fleste detaljer om systemet. Ut fra teorien jeg hadde satt meg inn i stilte jeg en del spørsmål til Hanssen for å få vite litt om systemet som er under utvikling, spesielt med hensyn på databehandlingen i systemet. Resultatet av denne kommunikasjonen finnes i kapittel 2.2 som del av forskningsbakgrunnen.

Ut fra telefonsamtale med Hanssen fikk jeg vite at Datatilsynet også hadde vært konsultert for å vurdere personvernhensyn for billettsystemet. Hanssen mente at datatilsynet holdt på å utarbeide retningslinjer for slike transportrelaterte systemer, også med tanke på *Autopass* systemer med elektronisk registrering av biler i bomringsystemer[4]. Alle disse gir muligheter for innsamling av lokasjonsinformasjon over tid. Jeg tok kontakt med Datatilsynet via epost 1.november, og snakket 9.november 2004 med Gunnel Helmers og Beate Dagslett ved Datatilsynet. Jeg fikk vite at det konkrete prosjektet som omhandlet Sporveien var lagt på is sommeren 2004, og at så lenge Autopass systemene og kollektivselskapene tilbød sine kunder anonyme alternativer til billettering og passering var Datatilsynets krav oppfylt, og videre retningslinjer var for øyeblikket ikke under utarbeidelse.

Innspillet fra Sporveien ble etterhvert utgangspunktet for min videre fremstilling og diskusjon, og har påvirket hvordan vinklingen i denne oppgaven har blitt.

Jeg er klar over at dette bare er ett eksempel ut av mange eksempler i ulike domener som kunne vært brukt, og ulike løsninger finnes også for dette domenet, elektronisk billettering.

Selv om dette bare er ett eksempel vil jeg påstå at dette er tilstrekkelig likt andre eksempler av slike infrastrukturer som kommer og som finnes til at beskrivelsen er noenlunde generell. For transportsektoren har vi allerede muligheter for å reise billettløst med fly og flytog, der all reiseinformasjonen samt betaling av reiser skjer ved innsamling av informasjon fra kredittkort. Flytogreisen er ikke lenger anonym, ei heller parkeringen i parkeringshuset, betalt med kredittkort. Autopassbrikkene i biltrafikken fungerer som betalingsmiddel, og kjøretøyet til alle som bruker dette kan dermed knyttes til stedet. Systemer med elektroniske lånekort i biblioteker gir enkel og umiddelbar oversikt over en persons boklån, og kanskje hans interesser. For handel kan vi betale det meste av varer og tjenester elektronisk, og i tillegg benytter mange seg av bonusordninger for kjøpeutbytte, som gir forhandlerkjedene mengder av informasjon om kjøpevaner.

Ikke alle disse tjenestene er trådløse, slik Sporveiens system er tenkt, men det gjør egentlig liten forskjell i forhold til behandlingen av innsamlet informasjon.

4 Se http://www.autopass.no/ (Sett des.2004)

Jeg har ikke sett grundig på alle mulige case og domener der slike systemer er aktuelle, og videre forskning må naturligvis se nærmere på om resultatene faktisk er generelle. Jeg har brukt en *interpretativ* metode basert på kvalitative midler samlet inn for anledningen. I den forbindelse har jeg snakket med forholdsvis få mennesker, og det har vel heller ikke vært snakk om noen streng hypotesetesting. Personene jeg har snakket med og innhentet stoff fra har imidlertid vært sentralt plassert i utviklingsmiljøene jeg beskriver, og de burde dermed vite hva de snakker om. Jeg vil si at caset jeg har fungerer godt som et scenario og forskningsbakgrunn, men man må naturligvis innse at det er rom for utvidelser og forbedringer. Innenfor rammen av en kort masteroppgave og 30 studiepoeng har det imidlertid ikke vært rom for å gå dypere og mer metodisk til verks enn jeg har gjort, og dette må dermed overlates til videre forskning.

1.6 Resultater

Vi vil i denne oppgaven se at de fleste eksisterende teorier omkring sosial regulering av personvern baserer seg på at det finnes sosiale mekanismer som regulerer deling av informasjon mellom en bruker og andre personer, kjente eller ukjente. Ut fra disse teoriene og min forskningsbakgrunn med et elektronisk billettsystem, vil jeg analysere eksisterende domener, systemer, og løsningsforslag med hensyn på fire personvernkrav: Kontroll og tilbakemelding, avtaler, transaksjonskostnader, og forholdet til sikkerhet.

Jeg vil komme fram til at den sosiale prosessen, i form av gjensidig eller ensidig mulighet for å regulere hvordan man framstår, ikke er til stede i mange systemer. Spesielt gjelder dette systemer som automatisk samler inn informasjon uavhengig av brukerens sosiale inngripen og kontroll. Jeg vil også argumentere for at brukeren ikke *ønsker* en slik kontroll.

I stedet ønsker han et tillitsforhold til systemet. Jeg vil presentere en modell for hvordan tillit til en datainnsamler oppnås som følge av en viss autoritet kombinert med legitim datainnsamling i forhold til formålet. Modellen omfatter også hvordan en bruker er villig til å dele ytterligere informasjon dersom han får motytelser av ulike slag.

Teknologi kommer inn i bildet for å opprettholde tillitsforholdet. Dette kan skje gjennom å garantere sikkerhet og adgangskontroll, både innad i datainnsamlerens system, under datainnsamlingen, og ved senere forvaltning. Man kan også tilby anonymisering og begrense detaljert datainnsamling der dette ikke er nødvendig og derfor ikke legitim. Dessuten kan teknologi benyttes til å formidle og forvalte standardiserte personvernkontrakter, som ytterligere vil bygge opp tilliten til systemet.

Som et bi-resultat av de ulike sosiale sidene ved ystemene hevder jeg at vi også bare ser en integrering av funksjonalitet inn i de samme tekniske enheter, og ikke en faktisk konvergens i den sosiale bruk av systemene.

1.7 Teoretiske og praktiske anvendelser

Modellen jeg har presentert for hvordan brukere deler sine data kan kanskje brukes for nye infrastrukturer som blir innført, og kan gi en pekepinn på hva som skal til for at disse skal oppnå aksept og dermed bli brukt. I forhold til min konkrete forskningsbakgrunn har jeg gitt noen forslag til hvordan billettsystemet kan bygge tillit til sine kunder, blant annet ved å anonymisere informasjon som ikke trenger å være identifiserbar, holde informasjon lokalt, tilby personvernavtaler med ulike valg, samt å utvikle et system for internkontroll.

Disse prinsippene kan også komme til anvendelse i andre og lignende systemer.

1.8 Struktur av oppgaven

Oppgaven er strukturert som følger: I kapittel 2 vil jeg gi en oversikt over min forskningsbakgrunn, et elektronisk billettsystem. I kapittel 3 vil jeg gjennomgå ulike sosiale teorier for og designprinsipper for personvern. I kapittel 4 vil jeg se på hva som karakteriserer de ulike teknologier som sies å konvergere, samt at jeg ser på noen løsningsmodeller som er presentert for å ta vare på personvern i allestedsnærværende systemer. I kapittel 5 vil jeg diskutere mine resultater for de ulike domener og løsningsforslag opp mot hverandre, teori og personvernkravene. Deretter presenterer jeg en modell for hvordan deling av informasjon skjer, og oppsummerer hvilke konsekvenser mine funn har for min forskningsbakgrunn og for andre lignende systemer. I kapittel 6 avslutter jeg med en kort konklusjon.

2 Forskningsbakgrunn:
Et elektronisk billettsystem for kollektivtrafikk i Oslo.

For å konkretisere problemene rundt personvern ved automatisk datainnsamling har jeg tatt for meg et aktuelt eksempel, nemlig utviklingen av et system for automatisk innsamling av billettinformasjon for kollektivtrafikk i Oslo.

Fra NSB's Årsrapport fra 2003 [37] kan vi lese følgende:

Vedtak 19. september:
"Selskapene Stor-Oslo Lokaltrafikk AS, AS Oslo Sporveier og NSB AS beslutter å etablere et felles, elektronisk billettkort. Selskapene skal knytte sine billettsystemer sammen slik at de oppleves som et felles elektronisk billettsystem for Oslo og Akershus innen utgangen av 2005."

Jeg har i dette kapitlet undersøkt litt om hvilke planer og forutsetninger AS Oslo Sporveier legger til grunn for datainnsamling ved innføring av et slikt billettsystem. Først vil jeg se på noen overordnede retningslinjer som er lagt på slike systemer, før jeg vil se på noen detaljer ved Sporveiens planlagte system.

2.1 Håndbok 206 Elektronisk Billettering

Det nye systemet for Oslos kollektivtrafikk bygger i stor grad på retningslinjer gitt fra Samferdselsdepartementet, Vegdirektoratet og Statens vegvesen i Håndbok 206 for Elektronisk Billettering[38].

I et elektronisk billettsystem vil det samles inn reiseinformasjon om hver eneste reise som gjennomføres. For at kunder skal ha tillit til slike systemer og for at nasjonale personvernkrav skal følges er det i [38] del 1, s 70ff satt som et fundamentalt krav at "den personlige integriteten" til kunden ikke krenkes. Personlig integritet er her definert som "den beskyttelsessonen et hvert individ ønsker å ha med hensyn til andres innsyn i ens eget privatliv og gjøremål"

Med "krenkelser" mener man elektronisk sporing av reisemønstre, registrering av navngitte kunders nærvær i systemer eller til opplysning for andre personer, samt kobling mot andre registre utenfor billettsystemet, for eksempel helseregistre, strafferegistre eller økonomiske registre.

Slike krenkelser vil kunne oppleves som tillitsbrudd fra kundens side, og som direkte lovbrudd i forhold til personvernlovgivning, og derfor settes det krav til at slike systemer skal sette strenge restriksjoner på slik bruk.

Det er imidlertid unntak fra restriksjonene. Dersom myndigheter, altså politiet, har mistanke om kriminelle forhold kan disse be om å få utlevert reiseinformasjon som kan brukes til krysskobling. Denne slags bruk må imidlertid følge strenge rutiner og det må foreligge en rettslig kjennelse om utlevering.

2.1.1 Bakgrunn for transaksjonslogger: Personvern vs. sikkerhet

Kollektivselskapene planlegger altså å samle inn en mengde reiseinformasjon for alle reiser, og det kan være nærliggende å spørre hvorfor dette er nødvendig.

Den viktigste årsaken er, ifølge Håndbok 206 for Elektronisk Billettering [38], at i et elektronisk billettssystem vil penger erstattes av elektroniske verdier. Slike verdier må beskyttes godt og være minst like vanskelig å forfalske som vanlige penger. En av hovedårsakene til at informasjon om alle transaksjoner må lagres i systemet er at det må være mulig å undersøke og lokalisere mulige eller faktiske feil og uregelmessigheter ved revisjon av disse data. På den måten vil det være mulig å plassere ansvaret for feilen hos enten kunden eller operatøren. Innsamlingen er altså ment å ta vare på sikkerheten og rettighetene til både kunde, operatør og eventuell økonomisk garantist.

Det foretas loggføring av transaksjoner, altså reiser og billettkjøp, på mange steder. Informasjonen lagres i kundens elektroniske billett, slik at han ved eventuell inspeksjon, ved overgang til et annet transportmiddel, eller ved uoverensstemmelser kan bevise at han har betalt. Denne loggen vil inneholde alle eller en viss mengde av transaksjonene som er gjort med billetten.

Transportmiddelet som kunden reiser med vil i mange tilfeller mellomlagre informasjonen lokalt, for senere å formidle denne til et sentralt system. Dersom man for eksempel etablerer systemer for etterskuddsvis betaling av reiser må kollektivselskapet også kunne dokumentere de kravene som blir sendt ut.

Dobbel logging vil også kunne begrense svindel og feil i systemet.

La oss si at en kunde forsøker å svindle kollektivselskapet. Han har kjøpt et anonymt klippekort hos en forhandler for et ganske høyt beløp, og brukt opp alle klippene. Kunden har en viss innsikt og ødelegger den elektroniske kretsen i kortet ved å sette spenning på noen av kontaktene. Deretter går han til en annen forhandler, sier han bare har brukt opp noen få klipp, og ber om å få refundert resten av verdien. Operatør har da muligheten til å ikke refundere noe selv om kortet ikke virker. Dette vil være urimelig overfor ærlige kunder, siden billettene jo skal erstatte penger, og defekte kort bør erstattes. Et alternativ kunne være å kreve legitimasjon og registrere identiteten til kunden før man refunderer verdien i kortet . Kunden vil kanskje føle seg mistenkeliggjort, men en uærlig person vil kanskje vegre seg for å oppgi sin identitet, i frykt for at det skal bli oppdaget at kortet er ødelagt med vilje. En mulighet er også at man ikke selger kort med høy pengeverdi uten av kunden oppretter en kundeavtale, altså oppgir sin identitet.

Et annet alternativ er altså å bruke dobbel logging, og registrere all bruk av alle typer kort både på kortet på de billetttyper der dette er mulig, og på en ”skyggekonto“ sentralt i systemet. Faktisk bruk kan da sjekkes opp mot hvor mye som er debitert på billettens sentrale konto, selv om kortet skulle være ødelagt.

I andre tilfeller kan det jo selvsagt hende at den sentrale konto er feil. En kunde kan eksempelvis få melding om at reisebeløpet eller antall klipp i kortet er brukt opp, mens han selv mener noe annet. Ved å holde transaksjonsloggen i kortet opp mot loggen i det sentrale systemet vil man kunne bestemme hvilken som er riktig.

For å beskytte både kundene og seg selv mot feil og svindel må altså operatørene og helst også kunden beholde en logg over transaksjoner, selv om billettene i utgangspunktet holdes anonyme.

Kravet om å beholde personlig integritet står altså i konflikt med kundens og operatørenes krav til sikkerhet.

2.2 Sporveiens billettsystem

For å få vite noen flere detaljer om systemet Sporveien i Oslo har under utvikling, kontaktet jeg 29.oktober 2004 prosjektlederen for billettsystemet i Oslo Sporveier, Jørn Hanssen, og spurte han noen spørsmål om det nye systemet. Spørsmålene jeg stilte er basert på anbefalte designspørsmål for å få vite hvilke personvernhensyn som er tatt i datasystemer, skissert av Bellotti og Sellen i [5]. Jeg vil komme nærmere tilbake til deres arbeid senere. I korte trekk går metoden ut på å spørre spørsmål og be om eller foreslå tiltak knyttet til fire problemområder ved datainnsamlingen: Informasjon om hvilke data som blir samlet inn, hva som skjer med data etter at de er samlet inn, hvem som har tilgang til og bruker informasjonen, og hva informasjonen brukes til.

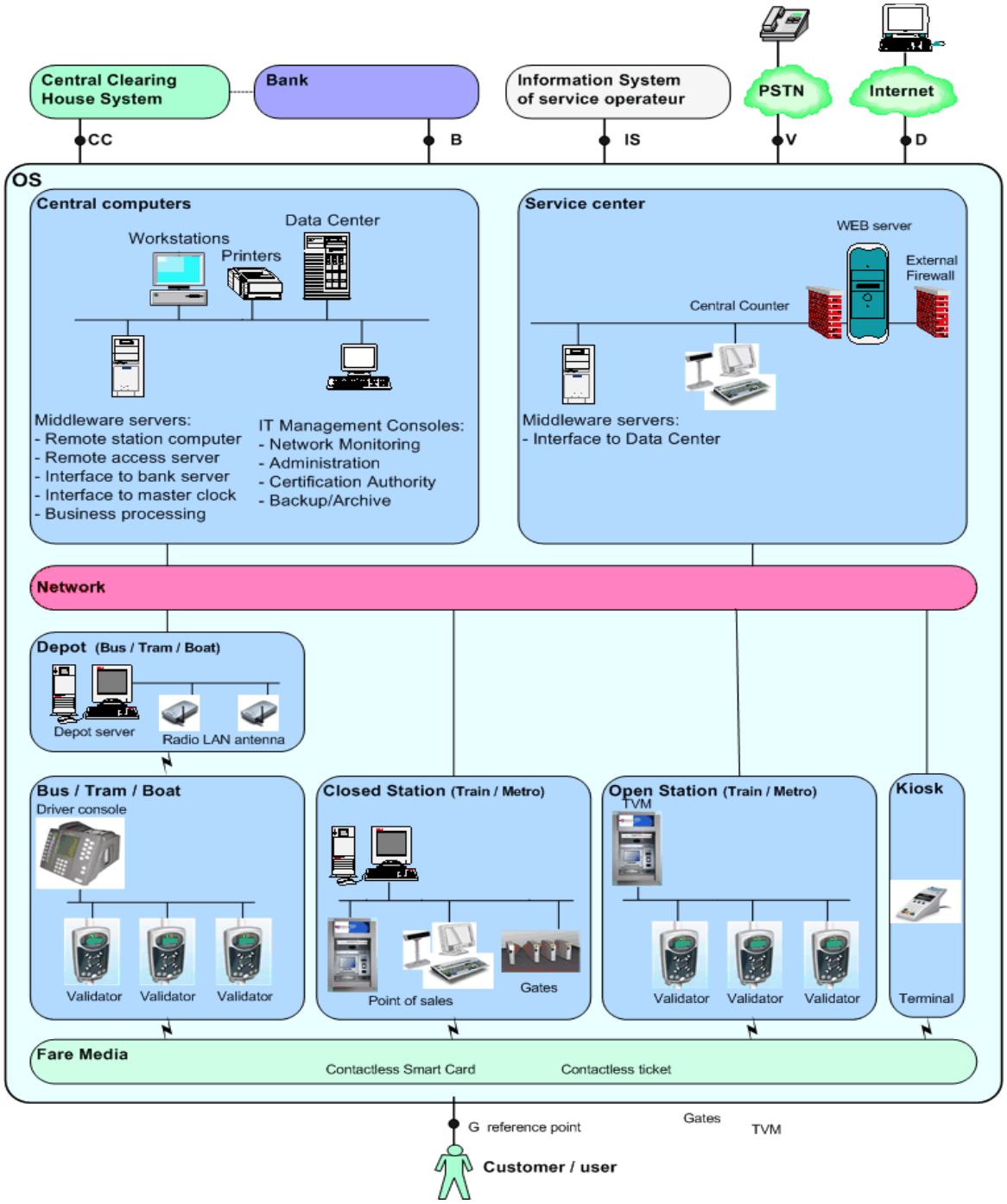
Jeg fikk svar fra Jørn Hanssen 15.11.2004, og de neste avsnittene er en beskrivelse av Sporveiens system ut fra den dokumentasjonen han sendte meg og de direkte svarene han gav på mine personvernrelaterte spørsmål.

2.3 Tekniske detaljer og sikkerhet ved billettsystemet

Først ville jeg gjerne ha en innføring i hvordan systemet er tenkt implementert i møte med kunden, og om hvilke roller sentrale systemer er tenkt å ha. Dessuten ville jeg gjerne vite hvordan informasjon vil bli kommunisert gjennom nettverket, mellom de enkelte transportenheter og sentralt. Som svar fikk jeg en overordnet systemoversikt med beskrivelser av systemet, delsystemer og dataflyt, som jeg har brukt i den følgende beskrivelsen.

2.3.1 Overordnet arkitektur

Et system for innsamling av billettinformasjon vil naturlig nok ha mange kontaktpunkter mot kundene. I tradisjonelle billettsystem kan billetter kjøpes på transportmiddelet, på holdeplasser eller stasjoner, og i kiosker og billettsentra over hele det geografiske området kollektivtrafikken spenner seg over. Et elektronisk billettsystem bør tilby de samme eller bedre kanaler for billettering, hvilket betyr at man må ha et distribuert system som kan foreta datautveksling over alle disse kanalene.



Illustrasjon 1: Overordnet arkitektur for Sporveiens billettsystem. Illustrasjon fra tilsendt dokumentasjon Jørn Hanssen.

Illustrasjon 1 viser et overordnet bilde av arkitekturen for hvordan Sporveiens nye billettsystem er tenkt implementert i møte med kunden, og hvordan de distribuerte enhetene er knyttet sammen med sentrale systemer. I de neste avsnittene vil jeg kort beskrive de enkelte bestanddelene som vises her.

2.3.2 Kontaktløse billetter

Sporveien ser for seg å bruke billetter av kategorier som ikke krever fysisk kontakt. Det betyr at billettene kan avleses trådløst på kort avstand, enten ved å holdes foran en leser, eller ved at leseren kan lese billetten uavhengig av hvor den er plassert på en person eller i hans bagasje. Disse billettene vil kunne ha minne og eventuelt også mikroprosessorer innebygd, noe som betyr ulike grader av funksjonalitet og sikkerhet i billetten.

To billetttyper er planlagt. For sporadiske kunder tilbys billetter med enkeltreise, periodereise eller klippekort. Disse billettene har reiserettigheter elektronisk lagret, med skrivebeskyttelse. For klippekort blir reiser registrert ved at en sikring blir kortsluttet, og elektronisk lagrede reiserettigheter "strykes ut". Samtidig lagres transaksjonsinformasjonen i kortet, som bevis for at reisen er registrert.

For faste kunder tilbys mer avanserte *smartkort*. Alle typer reiseavtaler kan lagres på slike kort. Disse kortene vil registrere den samme informasjonen som går inn i systemet, og vil kunne holde en lengre logg av transaksjoner, altså tidligere reiser, i kortet. Det vil også kunne holde personlige data om kunden og om produktene han eier. En mikroprosessorarkitektur muliggjør et høyere sikkerhetsnivå enn de enklere billettene, som bare har et begrenset minne.

2.3.3 Billettregistrering og kontroll

Inspektører kan overalt verifisere at billetter er betalt ved hjelp av portabelt utstyr. Betaling av reiser skjer ved at billetten passerer en billettleser. Billettleserne, også kalt *validatorer*, er enhetene som er utplassert for å gjennomføre transaksjoner der beløpet eller reiserettighetene som er lagret i kortet blir debitert, og reiseinformasjonen lagret i loggene.

Alle validatorer og billettsalgenheter som kunden møter er i prinsippet autonome. Det betyr at ingen kommunikasjon skjer direkte med det sentrale systemet i transaksjonsøyeblikket, med unntak av autorisasjonsforespørsler ved kortbetaling.

2.3.4 Kjøretøy

Kunder kan møte systemet via ulike kanaler. På kjøretøyer som buss, trikk og båt vil det være lokale nettverk der billetter kan selges eller valideres av fører eller av validatorer distribuert i kjøretøyet.

Sentralen i kjøretøy-systemene vil være førerens konsoll, som samler alle data mellom hver gang kjøretøyet daglig er inne til et depot. Der vil informasjonen kommuniseres trådløst til en depotserver, som igjen kommuniserer med det sentrale systemet.

2.3.5 Stasjoner

T-bane og togstasjoner vil eksistere som åpne og lukkede stasjoner. De mest sentrale stasjonene vil være lukkede stasjoner. Her vil det være en fysisk sperre mellom områder der man må ha løst billett og utenfor der man eventuelt kan kjøpe dette. Lokale nettverk knytter salgsterminaler og billettvalidatorer sammen med en stasjonssentral som aggregerer data, som igjen blir kommunisert til det sentrale systemet i periodiske intervaller.

Geografisk perifere stasjoner vil fungere som åpne stasjoner, altså uten fysiske sperrer til områder som krever billett. Kunder løser billett på selvbetjeningsstasjoner og validerer billetten på stasjonens billettlesere. Alle disse enhetene er ubetjente. Alle enheter på en åpen stasjon opererer i nettverk, og en av salgsautomatene opererer som konsentrator av innsamlet billettinformasjon og kontaktpunkt med det sentrale systemet. Kommunikasjonen skjer periodisk gjennom en kommunikasjonslink, som kan være via modem eller direkte tilknyting. Innbruddsforsøk på en automat kan også føre til at det må opprettes kommunikasjon med sentralen.

2.3.6 Salgssteder

Andre salgssteder, som kiosker og trafikk-knutepunkt, vil opptre som forhandlere av enkle billetter og for fornyelse av kort. Disse kan være direkte knyttet mot systemet eller bruke modem.

2.3.7 Sentrale systemer

Informasjon og kundetjenester som formidles bl.a. via Internett skal gi kunder muligheten til å kjøpe billettrelaterte produkter. Det kan være klippekort, periodeabonnement, eller opprettelse av autogiroavtaler. Billettene kan formidles til kunden per post eller ved oppmøte og "oppladning" ved et salgssted.

Systeminformasjon om drift og annen informasjon skal også gjøres tilgjengelig via Internett for autorisert personale.

All informasjonen som blir samlet inn i alle stasjoner og kjøretøy blir etterhvert samlet opp og prosessert i transaksjons- kunde- og systemdatabaser i et sentralt datasenter. Datasenteret har grensesnitt mot Internett-tjenester, kundesenter og eksterne systemer.

Sentralsystemet vil dessuten administrere nettverksinfrastrukturen og sikkerheten ved systemet, som generering av sikkerhetsnøkler, adgangskontroll, administrasjon av brannmurer og backuptjenester.

2.3.8 Dataflyt mellom transportenheter og sentralsystem

To datastrømmer går mellom de distribuerte enheter og sentralsystemet: Nedlasting av konfigurasjonsdata og opplasting av transaksjonsdata. Transaksjonsdata som blir lastet opp til systemet vil komme i store mengder, konsentrert i transaksjonsfiler.

Konfigurasjonsdata som lastes ned til enhetene inneholder parametere som billettpriser, svartelister over ugyldige/falske billetter, nøkler for digital signering av transaksjoner og enhetsdrivere. For å få konsistente transaksjonsdata må nettverket operere med globale tidsreferanser. Disse blir satt sentralt, og delt ut sammen med konfigurasjonsdata til de distribuerte terminaler.

Det er viktig å å forsikre seg om at ikke hvem som helst kan forsyne enheter med konfigurasjonsdata. På samme måte må man forsikre seg om at alle transaksjonsfiler som lastes opp i systemet kommer fra tillatte kilder.

For å få til dette vil det foretas en autentisering ved både opp-og nedlasting mellom de ulike

enheter. Dette foregår ved en kryptert *handshake* ved bruk av masternøkler som ble lagt inn ved initialisering av kommunikasjonsenhetene.

Man vil også opprettholde kopier av opplastede transaksjonsfiler for en tid i de lokale stasjoner og depot, i tilfelle det er behov for å replikere data på nytt.

2.4 Databehandling i systemet

2.4.1 Hvilken informasjon blir samlet inn?

De neste spørsmålene handlet om sensitiviteten av innsamlet informasjon, og ble direkte besvart av Jørn Hanssen.

Når blir informasjon samlet inn, og hvilken informasjon blir samlet inn av systemet?

I forhold til kommersiell bruk er det informasjon om den reisendes bruk av kortet som blir samlet inn. Dette innebærer at det blir samlet inn informasjon i det billetter blir kjøpt og i det de blir brukt til reiser. Ingen sensitiv personopplysninger blir i utgangspunktet registrert. Majoriteten av kort og billetter kan kjøpes og brukes anonymt. Den avanserte typen billetter som er basert på smartkort vil imidlertid kunne inneholde "personlige produkter". I disse tilfellene vil man sentralt holde en kundedatabase som inneholder tilstrekkelig med opplysninger til at avtaleforholdet kan opprettholdes, for eksempel ved bruk av autogiro. Disse opplysningene kan dermed omfatte navn, adresse og betalingsinformasjon.

For kjøp samles det inn informasjon om tidspunkt, kjøpssted, hva slags billett eller produkt som er kjøpt, betalingstype(kontant, kort, etc.), og utstyrsidentitet, altså identiteten til både billetten og salgsutstyret.

For reiser samles det inn opplysninger om tid og sted, hvilken type billett som er i bruk, samt transportoperatør.

For alle typer transaksjoner følger dessuten billettens/smartkortets unike serienummer med, sammen med sekvensnumre som genereres på bakgrunn av transaksjonsdata.

2.4.2 Hvilken hensikt har innsamlingen av informasjon?

De siste spørsmålene handlet om hensikten for datainnsamlingen. Hvor lenge blir informasjonen lagret? Hva skjer videre med informasjonen når den har kommet inn i systemet? Hvilke personer/roller og programvare har tilgang til informasjonen og hva slags informasjon kan disse få?

Hensikten med datainnsamlingen er å spore all bruk av kort og billetter. Dette benyttes til regnskapsformål, statistikk, trafikkplanlegging, samt for å bevare sikkerheten til systemeier, forvaltere og kunder/passasjerer, som omtalt i håndbok 206 for Elektroniske Billettering[38]

Sporveiens system vil være integrert mot tilsvarende systemer i SL og NSB, og for å få til en riktig fordeling av trafikkinntekter mellom selskapene vil det skje periodiske dataoverføringer mellom disse systemene. Dette vil gjøres ved at en tredjepart som alle selskapene blir enige om samler inn og distribuerer informasjon mellom de tilknyttede operatørene.

Tilstrekkelig og relevant informasjon må lagres for å oppfylle lovkrav til regnskapsføring. Det er videre to krav til lagringstid: For det første må informasjonen lagres fram til avregning mellom selskapene er fullført. For det andre lagres data for å kunne foreta sporing av økonomiske transaksjoner, som en a*udit trail*, for å kunne undersøke og rette opp i uregelmessigheter og feil. Potensielt kan derfor lagringstiden for data være lang, uten at dette er nærmere spesifisert.

For at informasjonen om *audit trail* skal være pålitelig stilles det krav til dataintegriteten i hver eneste transaksjon. Med dette menes at man skal kunne stole på at den innsamlede informasjonen er riktig. Denne opprettholdes ved de nevnte sekvensnumre genereres ut fra unike sikkerhetsnøkler som blir lagt inn i kortene og alle andre enheter ved initialisering, og disse kombineres med transaksjonsinformasjonen i en enveisalgoritme[5]. Denne informasjonen utgjør sammen en digital signatur.

Detaljer om den videre bruken av informasjonen i systemet, altså om hvordan informasjonen videre skal behandles, hvilke roller og programvare som skal ha tilgang til informasjonen var ikke avklart, så dette fikk jeg ikke noe svar på.

2.5 Personvernproblemer i Sporveiens system

2.5.1 Sosiale forventninger til kollektivtransport

Kollektivtransport er av natur en handling i det offentlige rom. I en offentlig situasjon som å reise med kollektivtransport forventer vi å bli oppfattet som en hvilken som helst reisende. De eneste som skal kjenne oss igjen er personer vi eventuelt kjenner på bussen/trikken/toget.

Ved bruk av tradisjonelle papirbilletter er det mulig å reise så godt som anonymt. Kjøp av billetter blir selvfølgelig registrert for regnskap og trafikkplanlegging, slik som det også er tenkt med elektroniske kort. Ved papirbilletter er det i beste fall aggregert informasjon om antall reisende som blir samlet inn i det reisen faktisk foregår. Et stempel på en billett registreres som regel ikke noe sentralt sted. Billetten er identitetsløs, og det er bare billetten som holder informasjon om at reisen er betalt, og ved inspeksjon må denne forevises . Det er heller ikke noen kobling mellom flere reiser på samme billett/stempling. For korttyper av større verdi har kunden gjerne en opsjon om å registrere seg for å eventuelt få erstattet kort ved tyveri. Ellers er reiser foretatt med slike kort også anonyme, og stempel foretas bare for første reise over en potensielt lang periode, fra en enkeltreise på maks en time, til dagskort og månedkort.

2.5.2 Registrering på offentlig transportmiddel

Innføring av elektroniske billetter innfører et nytt regime av registrering i kollektivtrafikken. Fra i beste fall innsamling av aggregerte trafikkdata samles det nå inn detaljert reiseinformasjon om hver eneste billett.

Ved gjentatte reiser vil billettens unike serienummer følge med. Dermed vil man for en gitt

5 En enveisalgoritme er en regneoperasjon som det ikke finnes en invers operasjon til. Det innebærer at man ikke kan regne seg tilbake til sikkerhetsnøkkelen ved hjelp av transaksjonsinformasjonen og sekvensnummeret. Dette er en ofte brukt metode for kryptering, f.eks ved hjelp av primtallsoperasjoner.

billett kunne hente ut en komplett reiserute for personen som innehar denne billetten.

Informasjonen jeg har fått fra Sporveien indikerer at Sporveien ikke har noen intensjoner om å drive elektronisk sporing av kunder, altså ved å knytte identitet til billetter for å gjenskape reisemønsteret til spesifikke personer.

Kunder har tilgang til anonyme alternativer ved å kjøpe billetter uten å identifisere seg. I utgangspunktet kan denne reiseinformasjonen derfor ikke brukes til å lokalisere navngitte personer.

De fleste av validatorenhetene i transportmidlene er autonome, og sender bare periodisk informasjon til det sentrale systemet. Dermed vil det sentrale systemet ikke være i stand til å gi informasjon i sanntid om hvor personen med en gitt billett-ID befinner seg på et gitt tidspunkt. Unntaket er reiser som er påbegynt og registrert akkurat i det en periodisk oppdatering begynner.

2.5.2.1 Kobling av informasjon er likevel mulig

Det er mange måter transaksjonsinformasjonen likevel potensielt kan kobles.

Selv om billetter kan være anonyme vil det kunne presenteres mange fordeler ved å opprette en såkalt reiseavtale med Sporveien, der man avgir sin identitet mot å få tilgang til gunstige tjenester, som for eksempel spesielle rabatter, etterbetaling, abonnement o.a.

Håndbok 206 Elektronisk Billettering[38] omtaler mulithet for innføring av en reiseavtale med individualiserte billetter, som kan brukes på tvers av transportmidler over hele landet.

For Sporveiens tilfelle har man tenkt seg noen billetttyper av typen smartkort som inneholder personlig informasjon om kunden og hans produkter. Denne informasjonen kan potensielt avleses sammen med transaksjondata. Slik lesing kan foregå i et forsøk på misbruk, eller som del av en verdiøkende tjeneste som kollektivselskapet tilbyr sine kunder.

Betalingsinformasjon som kunden avgir i kjøpsøyeblikket, dersom han betaler elektronisk, kan lagres og kobles sammen med serienummer på billetten. Ikke nødvendigvis ved at serienummeret på billetten kobles til kjøpet eller omvendt, men også ved sammenfall av tidspunkt og sted for kjøp og utstedelse av billetten kontra det elektroniske kjøpet.

I disse og andre tilfeller vil det i teorien være enkelt å koble en billett mot en persons identitet, og dermed alle hans reisetransaksjoner.

2.5.2.2 Verdiøkende tjenester

Som en fremtidsvisjon kan det hende at selskapene som samarbeider om elektroniske billettsystemer enkeltvis eller i fellesskap vil bruke data de har samlet inn på en måte som oppleves verdiøkende, for selskapene og/eller for kunden. For eksempel kan man tenke seg at kollektivselskapene kan gi hjelp til ruteplanlegging: La oss si at en person har reist fra et sted til et annet på en måte som indikerer at dette er et sted kunden regelmessig besøker. Ruten er imidlertid tungvint, og med en individualisert tjeneste kan selskapene gi kunden tips om en raskere eller mer behagelig reise. Kundene vil kanskje oppleve dette som en god service, som øker tilliten til selskapet.

Et annet scenario kunne være at den elektroniske billettinformasjonen kunne bygges inn en persons mobiltelefon, for eksempel som en RFID brikke i SIM kortet, som jo allerede er et slags smartkort. Reiseinformasjon og forslag til ruteforbedringer kunne da formidles som meldinger til mobiltelefonen. En annen tjeneste kunne være direkte markedsføring til mobiltelefonen i det personen går av transportmiddelet. Dersom personen har sagt seg interessert i slike tjenester, enten av ren interesse eller som motytelse for andre tjenester, som rabattert billettpris for transporten, vil dette være verdiøkende for begge parter.

Disse eksemplene viser at tjenestene kan brukes konstruktivt ved å tilby tjenester som gir kundene fordeler og potensielt raskere og billigere transport. For mange kunder vil dette være viktigere enn tanken på at reisemønsteret deres kan bli sporet. Holdningen til mange mennesker er at de har "ingenting å skjule". På den andre side vil noen kunder oppleve datainnsamlingen som invaderende og krenkende, og dette er det motsatte av den tilliten kollektivselskapet helst vil ha av sine kunder. Et viktig spørsmål blir derfor: Hvordan kan man beholde kundenes tillit selv om man samler inn potensielt sensitiv informasjon?

2.6 Tillit til kollektivtransport

Tillit til et kollektivselskap er begrunnet i flere faktorer, blant annet disse:

- At kollektivselskapet utfører tjenesten de skal, nemlig å frakte oss via en gitt rute til ønsket sted.
- At selskapet tar en riktig pris i forhold til pristabeller og rabatter, at man ikke blir belastet for tjenester man ikke mottar, og at dette gjelder for alle kunder.
- At reisen er anonym og at man blir behandlet som en hvilken som helst reisende i på et offentlig transportmiddel.

Med innføring av elektroniske billettsystemer endres forutsetningene for de to siste punktene. Sedler og mynter blir erstattet av elektroniske verdier i form av en sum som debiteres eller klipp/reiserettigheter. Kunden må derfor få fornyet tillit til at selskapet tar seg riktig betalt ut fra verdiene som er lagret i billetten, og at kundene så godt som mulig er vernet mot svindel.

Kunden vil fremdeles forvente at kravet om anonymitet er oppfylt. Slik systemene er designet har vi sett at datainnsamling gir muligheter for kobling, selv om dette ikke er intensjonen. Dersom kunden søker eller blir gitt kunnskap om hvilken registrering som blir foretatt må man også kunne garantere at selskapet ikke misbruker eventuell sensitiv informasjon om enkeltindivider. Det blir viktig at kunden oppfatter dette.

I Håndbok 206 for Elektronisk Billettering[38] har man anerkjent kundens behov for personlig integritet, og innsett at reiseinformasjonen som samles inn inneholder potensielt sensitiv informasjon.

For forhindre misbruk er det derfor satt en del krav til elektroniske billettsystemer:

- Alle enheter inkludert billettmedia må implementere et strengt sikkerhetssystem for adgangskontroll.
- Sentralt skal registre som inneholder identifiserbar informasjon holdes logisk og helst

fysisk adskilt fra reiseinformasjon, og eventuell kobling må ha bakgrunn i rutiner og adgangskontroll, og eventuelt i rettslige kjennelser.

- Personopplysninger skal ikke være tilgjengelige for enheter utenfor billettssystemet.
- Sensitiv informasjon skal ikke utleveres til andre enn kunden informasjonen omhandler, og kun etter at kunden har legitimert seg.

Vi skal etterhvert se at disse kravene er vanlige personvernkrav også i andre miljøer og systemer der det har vært fokus på personlig integritet.

2.7 Oppsummering av personvernkrav

I den følgende presentasjonen i denne oppgaven vil jeg ordne min framstilling med basis i utfordringene kollektivtransportørene i Oslo møter med innføringen av sitt billettsystem.

2.7.1 Feedback og kontroll

Sporveiens system tilbyr anonyme billetttjenester for sine kunder. På den andre side kan kunder velge billetttyper som kan forenkle og kanskje også forbedre deres forhold til kollektivtjenestene de er mer eller mindre avhengige av i sin hverdag. Kunden kan altså selv velge om han vil ha fordelene ved å reise anonymt, eller ha fordelene av å reise som en registrert kunde, og dermed velge ulike grader av identifisering. Sporveien planlegger å gi kundene innsyn og tilgang til informasjon som selskapet har lagret om dem og eventuelle billettmedia de måtte eie, mot autentisering. Tjenester knyttet til kunden skal tilbys over kanaler som Internett, og dermed kanskje også via medier som mobiltelefon. Ved innføring av tjenester som etterbetaling av reiser, potensielt over et landsdekkende system vil dette kreve at kollektivselskapene dokumenterer hvilke reiser kunden har foretatt.

Informasjon blir samlet inn ved hver eneste reise, og informasjonen blir lagret på billetten og sentralt i kollektivselskapets system. Tilbakemelding om registreringen kan gis ved validatorene, og ved inspeksjon kan det bekreftes at billetter betalt, nettopp ved å kontrollere at informasjonen er registrert, på billetten, på det lokale transportmiddelet/stasjonen, eller sentralt.

Disse egenskapene ved systemet vil jeg videre diskutere som et krav til at kunden trenger en viss grad av tilbakemelding/*feedback* og kontroll på informasjonen som omhandler han.

2.7.2 Avtaler

Selskapene er opptatt av at de vil beskytte kundenes integritet. Som reisende ved et offentlig transportmiddel har vi forventninger om hvordan vi skal behandles, som et sett av uskrevne regler eller en avtale for hvordan offentlig transport skal foregå.

Vi er vant til skrevne og uskrevne regler og avtaler i mange situasjoner.

En vanlig måte å sikre at to parter gjør det som er forventet av dem er å opprette en form for avtale eller kontrakt. Ved avtalebrudd eller uoverenstemmelser har man da noe man kan vise til som kan være grunnlag for sanksjoner mot datainnsamler. At partene er villige til å inngå avtaler kan også være tillitsskapende.

Det er viktig at kundene beholder tilliten til kollektivselskapene også når de så radikalt endrer på mengden av innsamlet informasjon. Det er viktig å formidle hvilken informasjon som samles inn og hvordan denne blir brukt, slik at kunder som ønsker slik informasjon kan få det. Selskapene må selvsagt følge dette opp ved å ha gode systemer og rutiner for intern lagring og bruk.

En viktig del av diskusjonen blir derfor omkring personvernavtaler.

2.7.3 Transaksjonskostnader

Det må være enkelt å ta kollektivtrafikk. Kunder ønsker sannsynligvis ikke å bli presentert for mange valg når de kjøper billetter, om noen i det hele tatt i det de skal gjøre sine daglige reiser. Dette kan stå i motsetning til ønsket om å formidle eventuell tilleggsinformasjon om datainnsamlingen.

Fra Oslo Sporveiers årsrapport for 2003[39] finner vi under nøkkeltall at Sporveien i 2003 gjennomførte omtrent 158,5 millioner personreiser for i Osloområdet. Dette er anslaget for antall reiser med tradisjonelle papirbilletter. Dette er mange reiser, men med elektronisk registrering av alle reiser inkludert alle overganger er det grunn til å tro at dette tallet vil bli mye større. All denne transaksjonsinformasjonen skal samles inn distribuert, og mellomlagres lokalt, før data replikeres sentralt. Datainnsamlingen må gå fort nok til at denne ikke virker som ekstra forsinkelse. Et viktig mål med innføring av elektroniske billetter er å få opp effektiviteten og påliteligheten, og forsinkende elementer er sannsynligvis uønsket.

Kollektivselskapene må altså ha et system som lar seg skalere. Både med hensyn på hvor mye data som samles inn, og hvor mye prosessering og kommunisering hver transaksjon krever. Dette gjelder både i transaksjonsøyeblikket, ved sentral prosessering, og når data eventuelt skal presenteres i andre kanaler.

Dersom personvernsystemer medfører vesentlig forringelse av skaleringsdyktigheten er de ubrukelige i slike systemer. Hvor store kostnader det er ved å innføre personvernsystemer er altså et hensyn vi må ta i med i diskusjonen videre.

2.7.4 Sikkerhet

Som ofte ellers i databehandling er sikkerhet et viktig tema i Sporveiens system. I Håndbok 206 for Elektronisk Billettering [38] er det gjort en egen sikkerhetsanalyse av trusler mot slike systemer, og man legger opp til diverse mottiltak mot disse truslene. Det er skissert at man ønsker kryptering, autentisering og autorisering ved overføring av opplysninger mellom systemenheter, fra elektroniske billetter til sentrale systemer, og med hensyn på hvem som har tilgang til system-, person- og transaksjonsdata. I og med at billettene vil fungere som elektroniske penger er det designet å foreta digital signering av samtlige transaksjoner for å opprettholde transaksjonsintegritet, altså uomtvistelig å kunne bevise at reiser har funnet sted.

Det distribuerte systemet som er skissert vil inneholde enheter med ulik kommunikasjons og prosesseringskapasitet: trådløst og trådbasert, potensielt ulike tekniske plattformer, ulike grader av minne og regnekraft, og dermed varierende sikkerhet. Dette må selvsagt veies opp

mot mengden og sensitiviteten av informasjonen som kommuniseres, økonomiske hensyn, skalering, og tilgjengelige teknologier.

Sikkerhetssystemer er åpenbart viktig for å hindre at informasjon kommer i gale hender via førstehåndsinformasjon eller observasjon. Jeg vil i den videre diskusjonen se på hvordan sikkerhet behandles i forhold til andre personvernhensyn.

3 Teorier for regulering og design for personvern

Det er mange miljøer som har jobbet med personvernrelaterte spørsmål. I dette kapitlet vil jeg se på hvordan personvern er forsøkt lovregulert, for å kunne dra linjer for hva som er lovlig behandling av data. Andre miljøer har jobbet med det faktum at mennesker uansett har behov for å dele individ -informasjon, for eksempel i arbeidsmiljøer. Disse miljøene har forsøkt å utvikle teorier og retningslinjer for design for hvordan informasjonsdeling foregår.

Jeg vil forsøke å strukturere slike teorier opp mot mine fire identifiserte behov for Sporveiens system: *feedback* og kontroll, avtaler, transaksjonskostnader og sikkerhet.

Først vil jeg fokusere på lovgivning og internasjonal praksis for innsamling av personopplysninger.

3.1 Personvernlovgivning? Historisk viktige direktiver

Kollektivselskaper som Sporveien må som alle andre forholde seg til lover og regler som gjelder for innsamling av informasjon, spesielt når det er snakk om personopplysninger.

Utvikling av lovverk for personvern og datasikkerhet er problematisk. Utviklingen av ny teknologi går svært mye fortere enn utviklingen av lovverket, dermed er det ofte at det oppstår gråsoner der det ikke er klart hva som er lov.

Jeg har allerede nevnt menneskerettighetene, paragraf 12, som definerer personvern som en grunnleggende rettighet for alle mennesker. Innføringen av to andre lover har hatt spesielt mye å si for utviklingen av modeller for datasikkerhet og personvern.

3.1.1 US Privacy Act 1974 : Fair information practices

Komiteen som utarbeidet denne rapporten for amerikanske myndigheter lagde begrepet *fair information practices*, eller *god informasjonspraksis*. Disse kjøreregelene har senere blitt brukt som utgangspunkt i de fleste datasikkerhetslover overalt i verden.

Disse reglene baserer seg på de følgende prinsipper:

1. ***Åpenhet og transparens:*** *Hemmelige arkiver bør ikke forekomme. All kunnskap om eksistens av data såvel som kunnskap om innholdet skal være offentlig for den registrerte.*
2. ***Individuell tilgang og deltagelse:***

   Den som informasjonen omhandler skal kunne ha tilgang til å se og eventuelt korrigere innholdet om seg selv.
3. ***Begrenset innsamling.*** *Datamengden som samles inn må være proporsjonal med den tiltenkte bruken av disse data.*
4. ***Datakvalitet.*** *Data må være relevante i forhold til formålet de er innsamlet for, og de må være oppdaterte.*
5. ***Begrenset bruk.*** *Bruken av data må begrenses til det formålet de var tiltenkt ved innsamlingen, og bare brukes av personer og/eller systemer som er autoriserte til databehandlingen.*
6. ***Fornuftig sikkerhetsnivå.*** *Avhengig av hvor sensitive data er må det legges opp til et fornuftig*

sikkerhetsnivå for å forhindre uvedkommende å få tilgang til disse data.

7. ***Ansvarlighet**. Den som oppretter og holder et arkiv må holdes ansvarlig for at prinsippene over følges.*

3.1.2 95/46/EC: "The Directive"

I 1995 innførte EU et direktiv 95/46/EC , effektuert oktober 1998, som tok for seg "beskyttelse av individer med hensyn til bruk og utveksling av personlige data" (Oversatt fra Langheinrich [16]). Dette direktivet har blitt så viktig at det bare omtales som *The Directive.*

Dette direktivet har to viktige sider . For det første krever artikkel 24/1 at dataoverføring til land utenfor EU bare kan gjøres med organisasjoner som holder et "tilstrekkelig" nivå på sin behandling av private data. Hva som er et tilstrekkelig nivå defineres så i direktivet. Dette betyr i praksis at alle organisasjoner som vil ha tilgang til europeisk dataflyt og dermed handel må tilpasse sin lovgivning til å oppfylle kravene som stilles i direktivet.

For det andre utvides reglene for *god informasjonspraksis*. I tillegg til eksisterende regler stilles det krav til at ingen data om personer kan samles inn eller brukes uten **eksplisitt** samtykke fra den som er registrert. Det innebærer altså at all datainnsamling som ikke er lovpålagt er ulovlig, og krever et helt klart samtykke fra den datainnsamlingen omhandler i hvert tilfelle. Dette medfører også at personvernet er så sterkt forankret i loven at de ikke kan ignoreres.

Denne loven setter også krav til land utenfor Europa som gjerne vil fortsette å handle med land i Europa. US og EU har inngått en avtale kalt *Safe Harbour*. Avtalen sies å være en øvelse i "selv-regulering", ved at selskaper som vil fortsette å handle med Europa må tilpasse seg et sett eller sub-sett av frivillige retningslinjer som er utarbeidet i forbindelse med *The Directive.* Selskapene "sertifiserer" seg selv, og sender årlig en offentlig bekreftelse på dette til det amerikanske handelsdepartementet. Denne avtalen gir amerikanske selskaper muligheten til å få stempelet "Tilbyr adekvat personvernbeskyttelse" av EU kommisjonen, slik at de kan handle med europeiske selskaper. For amerikanske selskaper er det frivillig å bli med på avtalen, og utbredelsen har gått sakte.

3.1.3 Personopplysingsloven

I Norge har vi et organ, Datatilsynet, som overvåker innsamling og bruk av persondata i Norge. De bygger sin virksomhet på et mandat fra Stortinget om å følge opp lover og regler som EU (gjennom EØS) og den norske stat innfører omkring personvern og registrering. Deriblant finner vi direktiv 95/46/EC som nevnt over, samt den norske personopplysningsloven, personregisterloven, Schengenavtalen og diverse helseregisterlover. Disse norske lovene er i stor grad laget i samme ånd som reglene til *God informasjonspraksis.* Personopplysningsloven Kap.II, § 8. setter for eksempel som vilkår for å behandle personopplysninger at "Personopplysninger bare kan behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller at behandlingen er nødvendig for a) å oppfylle en avtale med den registerte, eller for å utføre gjøremål etter den registrertes ønske før en slik avtale inngås, b) at den behandlingsansvarlige skal kunne oppfylle en rettslig forpliktelse, c) å vareta den registrertes vitale interesser, d) å utføre en oppgave av allmenn interesse, e) å utøve offentlig myndighet, eller f) at den

behandlingsansvarlige eller tredjepersoner som opplysningene utleveres til kan vareta en berettiget interesse, og hensynet til den registrertes personvern ikke overstiger denne interessen".

Loven er altså i utgangspunktet streng på at den registrerte skal samtykke, men man har også avveininger mot samfunnsmessige og lovmessige behov. Loven inneholder i tillegg mange spesifikke regler og forskrifter om tilfeller der loven kommer til anvendelse.

3.1.4 Myndigheters tilgang til personopplysninger

Lovgivningen for personvern er streng i Europa og EU, i motsetning til USA, der en miks av lovgivning og selvregulering er det som gjelder. I Europa prøver politiske og lovgivende instanser å ligge i forkant av teknologien ved å innføre lover som ligger på et mer overordnet nivå enn de mulighetene teknologien enhver tid skulle gi.

Risiko for misbruk av data er åpenbart tilstede, og av den grunn er loven er streng. Mange unntak er imidlertid gjort for lovens lange arm og for at myndighetene skal ha muligheter til innsyn.

3.1.5 Lovgivning og Sporveien

Sporveien forholder seg til lovgivningen jeg har nevnt her på flere måter. For det første samler de i utgangspunktet ikke inn personopplysninger, men reiseopplysninger. Disse er i utgangspunktet anonyme, og det foreligger dermed ikke restriksjoner på innsamlingen. Dersom Sporveien skal holde personspesifikk kundeinformasjon er dette knyttet til en kundeavtale/reiseavtale. Denne vil antagelig vil fungere som samtykke for datainnsamlingen, og bare tilstrekkelig informasjon til å opprettholde kundeforholdet skal samles inn. De legger opp til ulike grader av adgangskontroll og sikkerhet i systemet, og skisserer prosedyrer for utlevering av informasjon til myndigheter, slik personopplysningsloven krever.

Lovgivning har med implisitte **avtaler** å gjøre, og gir mulighet til å straffe forhold som er i strid med loven. Dette vil regulere hvilke plikter en datainnsamler har, og hvilke rettigheter en registrert har. Lovgivning sier imidlertid ikke alltid like mye om hvordan denne reguleringen skal foregå, og da må vi hente innspill fra andre miljøer.

3.2 Sosial regulering av personvern

Er det alltid like viktig å verne om personlige opplysninger? Er risikoen for misbruk alltid like stor? I det sosiale liv er det ofte slik at vi må gi oss til kjenne for å være med på aktiviteter, og for å differensiere oss fra andre personer. Og i det daglige er det sannsynligvis sjelden vi går rundt med en frykt for at opplysninger om oss skal bli misbrukt, muligens sjeldnere enn det burde. Hvilke mekanismer det er som gjør at vi vurderer forholdene på denne måten?

3.2.1 Computer Supported Colloborative Work - CSCW

En forskningsretning innenfor informatikk og menneskers bruk av teknologi er CSCW. Innenfor dette miljøet har det i lengre tid blitt utviklet og testet systemer for

bevissthet/*awareness*, det vil si systemer som kan gi informasjon om en persons identitet, lokasjon eller aktiviteter, og tilby kanaler for kontakt og samarbeid, spesielt i arbeidsmiljø, som det engelske navnet antyder.

Omkring disse applikasjonene har det blitt gjort undersøkelser av hvordan de som har brukt dem forholder seg til ny teknologi og hvordan de ble påvirket av disse.

Leysia Palen og Paul Dourish skisserer i [6] et system og et vokabular for å kunne forstå hvilke mekanismer og spenninger som er knyttet til personvern, spesielt i forhold til teknologi. Deres tilnærming er at vi ofte er i stand til å se at nye teknologier som blir innført og blir en del av dagliglivet kan ha problemer knyttet til personvern. Det finnes imidlertid få verktøy for å finne ut akkurat hvilke hensyn det er snakk om i de forskjellige situasjoner. Palen og Dourish forsøker å presentere en modell for å kunne "pakke ut" hvilke personvernaspekter som må adresseres i ulike situasjoner, isteden for å samle alle personvernproblemer i en "pakke".

Palen og Dourish bygger på personvernteorier utviklet av psykologen Irwin Altman. Hans arbeid på syttitallet bygde hovedsaklig på relasjoner mellom mennesker, mens Palen og Dourish utvider dette til også å gjelde når teknologi kommer inn i bildet.

3.2.2 Personvern – en dialektisk og dynamisk prosess

Personvern er bygget på at alle personer har rett til å holde noen ting privat. Det finnes mange definisjoner fra ulike fagmiljøer som har forsøkt å definere hva *privacy,* retten til personvern innebære. Tradisjonelt er det sett på som en tilstand der man trekker seg tilbake fra samfunnet.

Palen refererer til Altman, som mener at personvern i stedet kan ses på som en "selektiv kontroll av tilgang til selvet" (Fra psykologien, selvet, ego, *the self*), som reguleres gjennom en "dialektisk og dynamisk grenseregulerings prosess"

Med "dialektisk" mener han at vår holdning til private hensyn er regulert av våre egne forventninger og erfaringer til hva vi trenger av personvern, holdt opp mot de samme forhold hos den vi konverserer med. Disse forhold kan være i konflikt.

På den andre side er prosessen "dynamisk" fordi grensene mellom privatliv og publisitet er under kontinuerlig forhandling alt etter omstendighetene. Håndtering av personvern er en prosess der man må gi og ta mellom tekniske og sosiale entiteter, der man også har behov for publisitet.

Mennesker regulerer tilgang til seg selv på en skala fra full åpenhet til å være totalt utilgjengelig, fra trengsel til isolasjon. Mennesker kan være omgitt av tusener av andre men samtidig føle seg ensomme. Personvern blir dermed relativt til hva som er ønsket og hva som er oppnådd.

Reguleringen pågår gjennom et nettverk av oppførselmekanismer, som består av verbal og ikkeverbal kommunikasjon, fysisk avgrensing og kulturelle normer. Mange ulike kombinasjoner av virkemidler kan brukes for å oppnå ønskede personhensyn, og de kulturelle ulikhetene for hva som er akseptabelt kan være store.

Personvern handler altså etter Altmans mening ikke om å sette regler og håndheve disse, men om en kontinuerlig balansegang der grensene endres alt etter som omstendighetene endrer seg.

3.2.3 Øyeblikket blir bevart

Spørsmålet er så hva som forandrer seg når informasjonsteknologi kommer inn i bildet.

I det tradisjonelle bildet av verden har fysiske egenskaper stor betydning: Man kan ikke se gjennom dører, man kan ikke høre samtaler på avstand: Man må være til stede, altså innenfor begrenset fysisk avstand for å kunne få med seg detaljer. I menneske-til-menneske relasjoner har vi skrevne og uskrevne regler om hva som er akseptabelt å høre, si og gjøre, det kan handle om kropps- eller øye-kontakt, høflighet o.a. Omgangsformer er også kulturelt bestemt. Og det som blir sagt eller gjort kan ikke reproduseres annet enn gjennom gjenfortelling.

Med innføring at informasjonsteknologi kan vi ikke lenger bare forholde oss til disse fysiske og sosiale mekanismene for hvordan informasjon blir spredd, altså hvem som er publikum. I tillegg har det kommet inn et nytt aspekt: Informasjon kan lagres. Det innebærer at informasjon som har et publikum nå eller tidligere, også kan komme til å ha det i fremtiden. Dermed blir den informasjonen som eksisterer om oss utvidet til å omfatte både informasjon vi eksplisitt og implisitt har kommet med, med eller uten vår kontroll, viten og vilje.

Teknologien er altså i stand til å destabilisere grensesettingen som vi kontinuerlig utfører for å beskytte og/eller eksponere oss selv.

Dette er ikke noe nytt. Informasjon har blitt gjenfortalt og lagret i skriftlig form gjennom bøker og dokumenter i tusenvis av år. Tilgjengeligheten og mengden av informasjon som blir lagret om enkeltmennesker har imidlertid vokst dramatisk de siste 50 år. Og med disse endringene endres reglene.

3.2.4 Spenninger ved grensene

Det er behov for å identifisere hvilke personverngrenser det er snakk om.

Palen og Dourish identifiserer tre ulike grenser på bakgrunn av Altmans teorier:

Avsløring (disclosure), identifikasjon, og tid.

- Spenningen ved å avsløre informasjon står mellom hva man vil holde privat og hva man vil publisere, under hvilke omstendigheter og med hvilken kontroll?
- Spenningen ved identifikasjon står mellom individet (selvet), eller individets tilknytning til en institusjon, og publikum på den andre siden.
- Tidsaspektet kommer inn fordi informasjon som blir offentliggjort vil ha en fortid, nåtid og en fremtid.

Når man gir fra seg informasjon tenker man gjerne på hvordan informasjonen kan komme til å bli brukt i framtiden, både i forhold til et eventuelt nytt publikum og i å være en publisert del av ens fortid. Det er ikke sikkert at informasjonen vil være representativ resten av livet? Dermed blir hva man gir fra seg av informasjon også påvirket av hvordan man vil presentere

eller identifisere seg selv.

3.2.5 Avsløring av informasjon (disclosure)

Deltagelse i det sosiale liv krever at vi frivillig frigjør informasjon om oss selv. En del av vår identitet er knyttet til at vi differensierer oss fra andre, og for å få til dette må vi fortelle om hva vi mener om ting, hvilke aktiviteter vi interesserer oss for, med andre ord hvem vi er. Både i personlige sosiale situasjoner og i arbeidslivet er det viktig å bli lagt merke til. I en del situasjoner er vi avhengige av å eksistere i det offentlige rom, samtidig som vi vil beskyttes mot at det samme offentlige rom trenger inn i våre private områder.

I nettverksverdenen, for eksempel gjennom Internett eller mobiltelefonbruk, må vi også gi fra oss noe informasjon for å få delta. Ved innføring av mange nettbaserte tjenester, for eksempel nettbutikker, gir vi fra oss vital identifikasjon og transaksjonsinformasjon fordi det er behagelig for oss å kunne handle og betale på denne måten. Vi påfører oss selv en risiko for identitetstyveri, men begrenser kanskje denne ved bare å handle i butikker vi stoler på. Garantien vi har for at informasjonen ikke blir misbrukt ligger i forhandlerens løfte om riktig behandling av data, lovverkets sanksjoner dersom de ikke skulle gjøre det, samt at vi stoler på at kommunikasjonsforbindelsen vi har til forhandleren er trygg.

Problemene oppstår når det som er offentliggjort har kommet ut av vår kontroll, eller informasjon har blitt frigjort uten at det vår viten eller vilje. Det kan handle om tidligere publisert materiale som kanskje representerte noe man ville formidle på et tidspunkt – f.eks diskusjonsgrupper på Internett. Det kan gjelde offentlige register som plutselig har blitt lett tilgjengelige via Internett. Det kan gjelde bilder fra sammenhenger man har vært med i som blir publisert uten at man vet om det. Vi ser igjen at identitet er knyttet sammen med tidsaspektet og med hva som blir offentliggjort. Å publisere informasjon som man vil skal komme ut, f.eks via Internett (hjemmeside?), kan noen ganger være nødvendig for å balansere informasjon som kommer fra andre kilder. Mye informasjon kan for eksempel komme fra et enkelt søk på et personnavn med en søkemotor på Internett.

3.2.6 Identitet: Selvet og de andre

Ofte snakker vi om personvern som at personer alltid opptrer som uavhengige individer. Dette er ikke alltid tilfelle. Ofte uttaler man seg som profesjonell, som representant for en bedrift eller en organisasjon. Det blir da satt krav til at man formidler det som institusjonen vil at man skal formidle. Mange bedrifter har egne regler for hva som kan spres av informasjon, for eksempel hvordan man forholder seg til klientinformasjon. Hvordan man behandler sensitiv informasjon kan ha innvirkning på sosial og profesjonell status, både som bedrift og enkeltperson.

Men det er ikke bare "selvet" som kan forandre seg alt etter hvilke omstendigheter vi står oppi. Som regel tilpasser vi også informasjonen vi gir til den kjente mottakeren. "De andre" endrer seg også. Vi vil behandle familien annerledes enn arbeidskolleger og igjen annerledes enn mennesker på bussen. Det innebærer at selv om man opptrer offentlig for et visst publikum betyr ikke det at man er villig til å opptre offentlig for alle slags publikum.

Når så informasjonsteknologi kommer inn i bildet kan dette forpurre evnen vi har til å tolke

vårt publikum og bestemme hvilken informasjon vi vil frigi og hvilken vi vil holde tilbake. Teknologien virker som et mellomledd mellom oss og publikum. Det innebærer at vi ofte ikke har mulighet til å tilpasse informasjonen til publikum i det hele tatt. Dette kan gå på bekostning av hvordan vi ønsker å framstå. Det blir nemlig fullstendig opp til mottaker å tolke informasjonen, uten at vi har mulighet til å korrigere. Det at informasjonen er persistent muliggjør også at andre kan sette informasjon vi har lagt/gitt fra oss i system på en måte som ikke var intensjonen. Informasjonsgiver har da ikke lenger kontroll på denne informasjonen.

3.2.7 Fortid, nåtid og fremtid

Informasjon som vi gir om oss selv er ikke isolert som selvstendig informasjon. Det vil så godt som alltid eksistere en rekke tidligere handlinger i vårt liv som nåværende handling kan sees i perspektiv av. Omtrent like sikkert er det at handlingen vi gjør nå vil være den første i en rekke av kommende handlinger, der denne handlingen vil være bakgrunn for kommende. Det innebærer også at dersom vi har gjort eller sagt noe tidligere i en gitt situasjon, vil en ny respons på samme situasjon være avhengig av erfaringen fra den første, uten at vi av den grunn trenger å handle på samme måte.

Informasjon som alt er frigjort eller som vil bli frigjort i fremtiden er i prinsippet ute av vår kontroll i øyeblikket. Det som frigis nå kan imidlertid være ment for å påvirke hvordan tidligere eller eventuelt kommende informasjon kan oppfattes. Politikere er konstant i denne situasjonen. De blir sitert eller gjengitt i media, men kanskje bare delvis, og ofte tatt ut av sin sammenheng. Da kan det være nødvendig å komme med nye uttalelser for å prøve å rette på feilaktige inntrykk.

Teknologien innfører persistens for informasjon som tidligere kunne være ment for og oppfattet bare i øyeblikket. Teknologien har potensiale til å fjerne publikum fra selvet, og kontroll med hva som blir frigitt kan komme ut av kontroll. Teknologien kan i så måte fungere som en representasjon for individet og det som det vil fremstå som eller formidle. Dette utfordrer regler og konvensjoner vi har omkring personvern, men etter Altmans teorier vil også dette aspektet komme inn som en del av den kontinuerlige dialogen og forhandlingsprosessen vi er inne i. Når vi vet om disse spenningene som teknologien kompliserer, kan vi begynne å snakke om tiltak for å beholde integriteten i informasjonen, mener de.

3.2.8 Ulike sjangere

Vi sett at vi har krav hos individet som er i konflikt med hverandre. Man vil være synlig samtidig som man er vernet mot unødig inntrengning og i verste fall sporing og identitetstyveri. I skjæringspunktet mellom alle de tre spenningene som er skissert må det finnes en løsning for hvordan vi formidler det vi ønsker til en hver tid.

Disse løsningene vil utvikle seg sammen med utvikling av ny teknologi og endringer i sosiale mønstre som følger av ny teknologi. Små endringer i teknologien kan gi store endringer i hva som er mulig.

I verste fall må man ta høyde for hva teknologien muliggjør, ikke bare hva som skjer i praksis i de fleste tilfeller.

Det finnes ulike sjangere av situasjoner som kan inneholde personvernproblemer. Publisering av informasjon på Internett, f.eks på personlige hjemmesider er en sjanger. En annen kan være overvåkning med bilde og lyd og forventning til hvordan dette foregår på offentlige steder. En tredje kan være hvordan trådløse enheter som vi bærer brukes til å identifisere og spore oss.

Det at vi tenker at det finnes personvernproblemer med disse situasjonene må innebære at vi har en forestilling og forventning om hva som er uakseptabel bruk av slike data. Med andre ord må det med de ulike sjangere følge en forventning til respons og til hvordan informasjon samles inn og eventuelt benyttes senere. Hver sjanger inneholder på en måte et "løfte" regulert av lover og regler,men også sosiale normer på hva som er akseptabel bruk. Når disse løftene brytes, er det brudd på personvernet.

Poenget er altså at disse grensene er i konstant endring. De er er ikke faste for mennesker av ulike kulturer, ei heller for mennesker av samme kultur.

3.2.9 Grensespenninger i Sporveiens elektroniske billettsystem

Palen og Dourish sin bruk av Altmanns personverngrenser tar sikte på å kunne plassere alle situasjoner der mennesker har behov for å dele eller verne informasjon ett eller annet sted i disse tre dimensjonene; avsløring, identitet, tid.

Hva som blir "avslørt" av informasjon er jo nettopp avsløring av identitet, lokasjon, og eventuelt mengden av disse over tid. En forflytning på identitetsskalaen, for eksempel fra anonym reise med en enkel elektronisk billett til en kundeavtale, vil automatisk føre til en forflytning på avsløringsskalaen. Det samme gjelder for gjentatte frigjøringer av hvilken som helst informasjon over tid. Kanskje er "avsløring" ikke er en egen dimensjon, men heller en funksjon av de to andre, tid og identitet? Identitet kan da omfatte all informasjon som kan knyttes til en person, for eksempel lokasjon på et tidspunkt.

3.2.9.1 Dimensjoner i billettsystemer

For papirbilletter i tradisjonelle kollektivsystemer er Altmanns dimensjoner lite aktuelle: Man reiser anonymt, reisemønstre spores ikke over tid, og man befinner seg omtrent ute av dimensjonene. Med elektronisk billettering har dimensjonene fått mer mening. Hva slags informasjon er det som blir avslørt? Jo, at personen med en gitt billett var på et gitt sted (ved eller på et transportmiddel eller en stasjon) på et gitt tidspunkt. Ved kjøp av billett kan salgsstedet og betalingsmiddel spores. Og dersom vi har inngått kundeavtaler knyttes også potensielt denne personens identitet seg til stedet billetten befinner seg på, så lenge personen ikke har lånt bort sin billett. I kollektivtrafikk har vi som oftest ingen ønsker om å differensiere oss fra andre passasjerer, eller "publikum" i Palen og Dourish sin artikkel. Selvet er ett med publikum (i alle fall så lenge vi ikke har betalt for bedre service). Med anonym billett kan en reisende ikke skilles fra "publikum", eller "de andre", og vi befinner oss altså motsatt ende enn *self* i identitetsskalaen. Men med kundeavtaler er vi identifiserbare, selv om det ikke var verken vår eller Sporveiens intensjon at vi skulle være det.

Reiseinformasjon om en reise kan også settes i sammenheng med andre reiser på andre tidspunkt med den samme billetten. Dimensjonen med fortid, nåtid og framtid blir viktig,

fordi man, basert på en historie av registrerte reisedata, kan avdekke et totalt reisemønster, som igjen kan være med å fortelle noe om en persons liv. Tidaksen i billettsystemet er problematisk i forhold til trusselen om inferens-trusselen presentert av Görlach et. al. [4]. Det er den samme informasjonen om reisen som frigjøres hver gang. Informasjonen som frigis kan altså ikke reguleres for hver innsamling på bakgrunn av en analyse av hvordan informasjonen vil oppfattes i nåtid og muligens i fremtid, som Palen og Dourish skisserer, selv om bekymringen for *datamining* er den samme.

3.2.9.2 En prosess? Kontroll og tilbakemelding

Altmanns dimensjoner, referert av Palen og Dourish forutsetter at personen som "dynamisk og dialektisk" regulerer sitt personvern er *opplyst* om den situasjonen med eventuelle personvernkonflikter han står ovenfor. Tradisjonelt er personvernkonfliktene ved kollektivreiser små, man er anonym så lenge man ikke blir tatt for å snike i en kontroll, lite blir registrert. Dermed har personen ingen forventninger og erfaringer av at han trenger å tenke på av personvern. For at det skal være en "dialektisk og dynamisk" prosess må han, etter Palens syn, være klar over disse forhold. Uten omfattende og kontinuerlig tilbakemelding/*feedback* fra kollektivselskapets side vil han sannsynligvis ikke være særlig oppmerksom på at situasjonen har endret seg i det hele tatt. Han vil i beste fall ha en liten mulighet til å kontrollere noe av den identifiserbare informasjonen som frigis ved *ikke* å opprette en kundeavtale. All annen informasjon som Sporveien ønsker å samle inn vil uansett bli samlet inn dersom han ønsker å benytte kollektivtilbudet.

I en slik situasjon vil jeg altså si at man ikke befinner seg i en aktiv "dialektisk og dynamisk" prosess, man må bare godta systemet som det er.

3.2.9.3 Informasjonssjangere og avtaler

Palen og Dourish introduserer begrepet informasjonssjangere; implisitte eller eksplisitte avtaler til hvordan informasjon skal behandles i de ulike domener. De definerer dette negativt, ved at man har en følelse av når personvernet er brutt, altså må det gå en grense et sted for hva som er greit. For Sporveiens billettsystem vil dette kanskje være en forventning om en anonym reise uten registrering av start og stopp. Sjangeren brytes altså ved å innføre automatisk innsamling av slik informasjon. I beste fall må en ny sjanger formidles på et vis, kanskje i form av en ny slags avtale, altså en ny sjanger.

Palen og Dourish snakker forøvrig ikke om fastsatte avtaleforhold i forhold til delt informasjon. Deres vinkling er heller at slike avtaler, eller sjangere, er i konstant endring som følge av "den dialektiske og dynamiske prosessen", under påvirkning av ulike sosiale forhold.

3.3 Offentlig og privat informasjon

Andre som har forsøkt å systematisere hvordan informasjon formidles i det sosiale liv er Eamonn O'Neill et.al [7]. Identifikasjon handler etter Irwin Altmanns teorier om forholdet mellom "selvet og de andre", der begge parter kan ha varierende egenskaper. Man velger å formidle informasjon som er tilpasset den som skal ta imot informasjon. O'Neills sosiale

dimensjoner bygger på arbeidet Palen og Dourish har gjort, og handler om hvordan vi konstant er i stand til skifte oppmerksomhet mellom private, offentlige, og alle sosiale situasjoner og tema i mellom, og tilpasse informasjonen vi formidler deretter.

O'Neills modeller dreier seg i første rekke om formidling i offentlige rom, og deres forskningsfelt er offentlige informasjonssystemer innenfor fagområdet menneske-datamaskin interaksjon. De har studert mulighetene for å kombinere offentlig og privat informasjon gjennom teknologiske hjelpemidler som skjermer og høyttalere på offentlige steder, spesifikt hos legevakten (*Emergency Room*).

3.3.1 Brukeren som informasjonsborger

Deres utgangspunkt er at konseptet "borger" eller *citizen* kan være mer meningsfylt og favne videre enn begrepet "bruker". Hans beskrivelse av en informasjonsborger er en person som mottar offentlig informasjon på et offentlig sted. Vi kan ikke vite svært mye om denne personen, nettopp fordi han kan være hvem som helst. Personen er likevel ikke *nobody* eller *anybody*, men en borger, med endel rettigheter og plikter som man kan vite noe om, også i forhold til informasjonspraksis. Det kan være rettigheter borgere har, hvordan de ser på og bruker andre offentlige systemer, som TV og offentlig transport, og hva slags type tilgang borgere vanligvis foretrekker eller krever. Dette går også på tilgjengelighet for grupper i samfunnet som har nedsatt funksjonsevne, eksempelvis eldre eller funksjonshemmede. Poenget er at offentlige systemer bør tilstrebe å være inkluderende, og ikke ekskluderende på spesielle grupper.

Potensielt er borgeren en person som kan identifiseres. Likevel er "borger" et såpass vidt begrep at det kommer omtrent nederst på identifikasjonsstigen, og det meste som kan sies om vedkommende er statistiske antagelser.

3.3.2 Informasjonssfærer

Informasjon som formidles kan kategoriseres som offentlig, sosial eller privat. Offentlig og privat representerer ytterpunktene i denne skalaen, der offentlig tradisjonelt er rommet der informasjon av allmenn interesse blir publisert og der meninger blir konstruert og diskutert. Generelt har alle tilgang til det offentlige rom. Den private sfære omfatter naturligvis private emner og tjenester som man må holde streng kontroll på hvem som har tilgang til. Den sosiale sfære er alt i mellom disse to ytterpunktene. Informasjon som eksisterer her er bare interessant for en begrenset gruppe mennesker. I den sosiale sfære eksisterer det skrevne og uskrevne regler som forhindrer informasjon i å bli offentlig.

Grensene her er bevegelige. Å snakke med en venn i mobiltelefonen på venterommet vil føre oss inn i formidling av informasjon som tilhører den sosiale eller private sfære selv om informasjonen som kommer ut vil tilhøre den offentlige sfære. De som hører informasjonen vil kanskje oppfatte at dette likevel ikke er offentlig informasjon, men noe som bare vedkommer denne personen.

3.3.3 Informasjonsrom

Et geografisk rom eller sted inneholder forståelse og regler for hva som er akseptabel adferd.

I tillegg vil det ha betydning om det befinner seg andre personer på stedet. Disse forhold påvirker og regulerer hvordan vi oppfører oss på stedet vi befinner oss.

På samme måte som informasjonsfærer kan vi dele opp alle mulige geografiske steder i offentlige, sosiale og private rom. Ved å bruke disse kategoriene tar vi også med oss karakteristikker og forståelser som vi assosierer de respektive rom: Det offentlige rom er typisk fysisk åpne for alle: Offentlige transportmiddel, parker, og gater og torg. Private rom kan være soverom og andre steder der folk forventer å være alene. Sosiale rom kan være rom som verken er private eller offentlige, som hjem, biler, behandlingsrom på sykehus. I noen tilfeller vil disse rom være private, ofte når ingen eller bare spesielle andre er tilstede, i andre tilfeller vil de oppfattes mer offentlige. En park kan også være et sosialt rom, når f.eks en gruppe er samlet i parken. På et sykehus er venterommet offentlig, mens resepsjon og behandlingsrom kan være sosiale rom der folk har mer eller mindre behov for å begrense offentligheten. Kanskje vil legen eller pasienten be familie eller pleiere å forlate rommet, nettopp for å endre dets karakter. Grensene er bevegelige.

3.3.4 Interaksjonsrom

Med fysiske lokasjoner kategorisert i informasjonsrom og informasjon kategorisert i informasjonsfærer kan beskrive hvordan prosessen med å formidle og utveksle informasjon foregår. I det fysiske liv tilpasser lager vi oss slike interaksjonsrom ved vår kroppsholding, f.eks ved å vende oss mot den vi vil snakke med, med øyekontakt, ved stemmeleie. På den måten kan vi forsøke å sette fokus på den eller det vi vil.

Tekniske hjelpemidler fungerer også som interaksjonsrom. Informasjonstavler med rutetider på en jernbanestasjon fungerer som et offentlig interaksjonsrom. En borger som bruker et skjermbasert billettbestillingssystem på den samme jernbanestasjonen har er privat interaksjonsrom med denne, der han kanskje gir fra seg betalingsopplysninger (og dermed oppgir sin identitet). En person som bruker et samarbeidsverktøy i sitt arbeid deltar i et sosialt interaksjonsrom.

Generelt kan man si at informasjon som blir annonsert gjennom høyttalere og på tv-skjermer oppfattes offentlig. Informasjon på pc-skjermer, mobiltelefoner og fra hodetelefoner oppfattes privat.

Situasjonen er imidlertid ikke alltid så opplagt. En mobiltelefonbruker kan befinne seg fysisk i et offentlig rom, mens han psykologisk befinner seg i en privat eller sosial informasjonsfære i samtalen som foregår på telefonen. Det samme kan være tilfelle for den han snakker med i telefonen.

En person som befinner seg i et privat informasjonsrom har som regel ikke problemer med å bruke et offentlig interaksjonsrom, for eksempel å sette på høytaleren på telefonen, selv om informasjonen tilhører den private informasjonsfære. På den andre siden vil han ty til et privat interaksjonsrom dersom han befinner seg i en offentlig informasjonsrom, ved kanskje å gå litt unna og snakke lavt i telefonen. Interaksjoner tilpasses altså situasjonen.

3.3.5 Elektroniske billettsystemer, borgere, og de ulike rom

3.3.5.1 Bruker eller borger?

O'Neills omtale av brukere av offentlige systemer som borgere gir mening i noen typer offentlige systemer, spesielt når det gjelder å ha fokus på inkluderende systemer, for eksempel tilpasninger for syns- eller funksjonshemmede. På den andre side må vi vel kunne anta at en bruker eller *anybody* også vil ha normale borgerettigheter i et land, og slik sett gir ikke begrepet borger noe spesiell innsikt. For de ulike domener vil etter mitt syn en kategorisering som bruker av akkurat det systemet gi oss mer informasjon om brukerens forventninger og behov enn en kategorisering som "borger". En bruker av et køsystem hos legevakten vil kanskje være interessert i ventetider, hvor han selv befinner seg i køen, samt eventuelle koder som kan tolkes som direkte meldinger til den enkelte. For en reisende vil det på samme måte kunne sies mer konkret om hans sannsynlige forventninger til hvilken informasjon han trenger som en bruker av transportmidler enn som en "borger". En borger virker på meg som generalisering mer enn en informativ spesifisering når vi begynner å snakke om faktiske informasjonsdomener, som for eksempel transportsystemer i mitt eksempel.

3.3.5.2 Kontroll, tilbakemelding og avtaler

Transportmidler er, som O'Neill sier, et offentlig informasjonsrom. Å formidle informasjon i høyttalere og på skjermer, eller å snakke høyt i et slikt rom vil kunne medføre at noen får dette med seg. I de fleste tilfeller vil mennesker søke den informasjonen de er interessert i, og folk som snakker høyt vil sannsynligvis oftest bli oppfattet som støy. Likevel, O'Neills ulike rom handler om hvordan vi er i stand til å regulere informasjon *som vi har kontroll over.* Eksempelvis handler det om hvordan vi bruker mobiltelefon, pc-er, betalingsterminaler og hvordan vi styrer samtaler med mennesker på ulike måter avhengig av hvordan vi oppfatter situasjonen omkring oss. Vi tilpasser oss ulike forventninger til implisitte "avtaler" relativt til våre erfaringer om de situasjonene eller sjangerne vi kommer opp i, slik som Palen og Dourish også pekte på.

Automatisk datainnsamling av typen elektroniske billettsystemer vil være et interaksjonsrom i et offentlig informasjonsrom som kollektivtransport er. Interaksjonsrommet kan kanskje ses på som "privat", fordi de andre passasjerene på transportmiddelet ikke vil ha noen direkte tilgang til denne informasjonen. Innsamlingen er begrunnet i en implisitt avtale mellom kollektivtransportør og kunden om at man må stemple/*validere* billetten for å kunne reise kollektivt. Hvem som faktisk er mottaker og bruker av informasjonen er uklart, selv om Sporveien forsikrer at informasjonen ikke er offentlig. Informasjonen havner i et informasjonsrom (fysisk og virtuelt) utenfor innsamlingsstedet. Kunden har liten kontroll eller tilbakemelding på hvilken informasjon som samles inn og hvor og hvordan denne brukes senere, og dermed få muligheter til å velge andre slags "rom".

Informasjonen som blir utvekslet vil i noen tilfeller bare være knyttet til billetten, og dermed til dels anonym, i andre tilfeller i tillegg knyttet til en kundeavtale som identifiserer den reisende. Dette fører til en flytende informasjonssfære, men om man ser på lokasjon som privat, vil identifiserbar lokasjon innebære en privat informasjonssfære, og det med en noe

diffus samtalepartner.

Som begreper er det mulig å forholde seg til O'Neills ulike rom i de tilfeller der vi har mulighet til å regulere spredning av førstehånds informasjon, slik som når vi snakker med mennesker eller i mobiltelefon, som O'Neill har som eksempel. Med automatisk datainnsamling virker det som disse dimensjonene mister sin betydning, fysiske rom får uklar betydning i forhold til virtuelle rom, og informasjon i private informasjonssfærer havner på steder som er ute av datasubjektets kontroll.

3.4 Personverndesign

Så langt har jeg sett på hvordan lovverk og teorier for sosial regulering av personvern har relatert seg til mitt eksempel på allestedsnærværende systemer, nemlig elektroniske billettsystemer. Det kan se ut som dimensjonene til både Palen/Dourish og O'Neill ikke fungerer helt, hovedsaklig fordi den kontrollen og sosiale *prosessen* som de begge forutsetter ikke er særlig fremtredende i eksempelet med billettsystemer.

I det følgende vil jeg se på noen designprinsipper for informasjonsdeling og personvern, utviklet blant annet innenfor CSCW miljøet, for å se om andre mekanismer kan regulere hvordan informasjon deles. Prinsippene er basert på erfaringer fra utvikling og bruk av faktiske systemer.

3.4.1 Awareness

"Åpenhet", "bevissthet", eller *awareness,* er begreper som er velbrukt i CSCW miljøet. Disse begrepene brukes i første rekke om samarbeidsystemer som tilbyr ulike grader av opplysning om status i et miljø, begrenset i tid og rom. Et miljø innbefatter informasjon om de samarbeidende parters aktiviteter, samt hva de deler og har delt av informasjon. Olivier Liechti har i [8] oppsummert fire kategorier av *awareness,* til bruk som introduksjonsartikkel for konferansen CSCW'2000. Liechti fokuserer på hvordan systemer for *awareness* bruker Internett med to ulike vinklinger: som en plattform utviklere kan bruke til å bygge *awareness* systemer, og som et aktivitetsrom der arbeidere kan samarbeide og utveksle erfaringer.

Vi vil se at egenskapene i de fire kategoriene tildels overlapper, og ved utvikling av applikasjoner er det ofte naturlig å tilby kombinert funksjonalitet fra kategoriene.

3.4.1.1 Gruppebevissthet -group awareness

I kategorien *gruppebevissthet* faller systemer som har til formål å gi ulike grader av presis informasjon om andre personers tilstedeværelse og gjøremål, spesifikt innad i et team som befinner seg på geografisk forskjellige steder. Informasjonen trenger ikke å være spesielt presis, spørsmål som systemet kan besvare kan være av typen: Er personen tilstede? Er det passende å kontakte personen eller vil det være forstyrrende? Denne gruppen verktøy fokuserer på å støtte koordinasjon og samarbeid mellom arbeidsgrupper eller personer, formelt eller uformelt. Et av de første systemene i denne kategorien var *Portholes [40]*, som ble brukt som kanal mellom samarbeidende team i Xerox PARC i California og Xerox EuroPARC i England. Dette systemet var begrenset til å kunne se på stillbilder av personer i sitt arbeid, oppdatert med jevne mellomrom. Systemet inneholdt en epost-lenke for å kunne ta kontakt,

samt mulighet for å høre på lyd som personen hadde spilt inn på forhånd.

3.4.1.2 Bevissthet i arbeidsmiljø – workspace awareness

Etter at den initielle kontakten er opprettet, kanskje ved hjelp av gruppebevissthetverktøy, kan det være behov for miljø der man kan samarbeide om oppgaver, enten i sanntid eller i lengre utstrekning. For synkrone arbeidsprosesser (altså i sanntid) kan dette dreie seg om delte arbeidsflater, *whiteboards*, delte editorer og nettlesere og andre løsninger, gjerne i kombinasjon med video og lyd. Her vil det være en balansegang mellom å tilby brukeren kontroll over hva som blir delt, og å tilby funksjonalitet for gruppen som samarbeider.

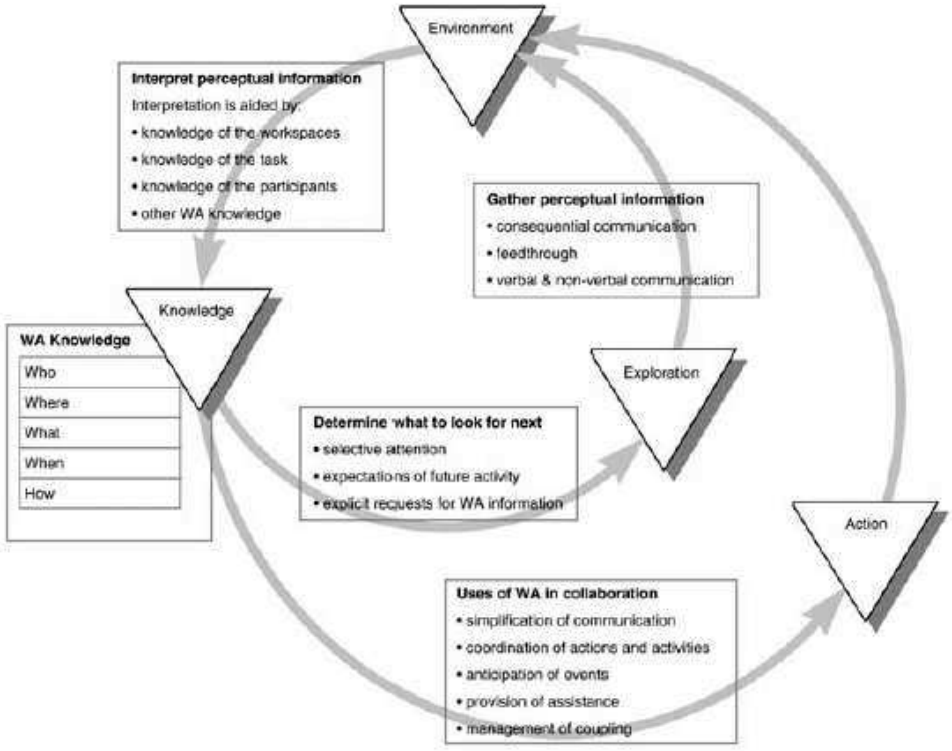
For arbeidsprosesser som spenner seg over et lengre tidsrom vil det være behov for å ha tilgang til persistent informasjon om resultater som har kommet ut av tidligere samarbeid. Dette vil altså omfatte diskusjonsgrupper, elektroniske oppslagstavler og dokumenthåndtering.

Mange systemer forsøker å tilnærme seg prosesser og fysiske miljøer som vi kjenner fra det fysiske liv. Nettbutikker bruker begreper som de også bruker i sine fysiske utsalg, nettopp for at vi skal kunne kjenne oss igjen: Som å gå til kassen, en handlevogn, osv. Også for arbeidsprosesser ordner vi oss likedan, ved for eksempel å opprette virtuelle grupperom der spesielle emner diskuteres, som ikke ville diskuteres i et mer offentlig rom.

Mange løsninger har støtte for både synkron og asynkron kommunikasjon, samtidig som de har støtte for gruppebevissthet ved å vise hvem som er tilstede i det virtuelle rommet brukeren er en del av.

Gutwin og Greenberg har i [9] beskrevet et omfattende rammeverk de har kommet fram til for *workspace awareness*. De har definert dette som en "fram-til-nå forståelse av en annen persons interaksjon med en delt arbeidsflate"(s.412). Problemer omkring å tilby *awareness er* systematisk gjennomgått knyttet til hvilken informasjon som bør samles inn, hvordan denne skal presenteres til gruppen, og når informasjonen vil være mest nyttig. De presenterer dette som et rammeverk for hvordan kommunikasjonshandlinger i et arbeidsmiljø kan genereres og forenkles ut fra kunnskap om miljøet, som igjen fører til utforsking av miljøet, som igjen vil påvirke miljøet. Se også illustrasjon 2.

Deres rammeverk omfatter innsamling av informasjon om hvem som er tilstede, hva de gjør og hvorfor de gjør det, hvor de befinner seg, og hva de ser og har tilgang til i sitt miljø. Denne informasjonen samles inn i sanntid, og kan hentes fram senere for å kunne finne ut hvordan en handling har foregått, hvem som har deltatt i handlingen, hvor, og når. De presenterer også hvordan deres deres rammeverk kan brukes i design av brukergrensesnitt for samarbeidsapplikasjoner.



Illustrasjon 2: Greenberg og Gutwins rammeverk for workspace awareness. Illustrasjon fra [9].

3.4.1.3 Kontekstbevissthet – context awareness

En annen kategori av awareness er ifølge Liechit[8] kontekstbevissthet, altså det å tilpasse oppførselen til systemet til konteksten brukeren eller systemet befinner seg i. Det kan være at delte arbeidsmiljø tilpasses i forhold til hvilken informasjon brukere skal gjøres oppmerksom på, og hvordan eventuell varsling skjer. Varslingen vil være avgjørende for om meldingen vil virke forstyrrende eller være nyttig. Dette er spesielt aktuelt dersom det er store delte miljøer med svært mange hendelser, og brukeren bare er interessert i et fåtall av disse. Kanskje må det gjøres prioriteringer av meldinger.

Noen systemer fokuserer også på å være fasilitator for uplanlagte interaksjoner, av typen som oppstår ved kaffemaskinen – korte og ofte, men viktige for sosiale og profesjonelle relasjoner, og for å holde seg orientert.

3.4.1.4 Perifer bevissthet -perpiheral awareness

Perifer bevissthet dreier seg om hva som er passende fokus for systemet for et *awareness* system. En del systemer kan befinne seg i periferien av det som en bruker er fokuserer på, men likevel være informativ nok til å fortelle om noe foregår i et virtuelt rom. Dette er også beskrevet som rolige (*calm*) teknologier, som lett beveger seg fra periferien av fokus, til senter, og tilbake til periferien.

3.4.2 Kontroll og Feedback

Bellotti og Sellen deler i [5] erfaringer de har gjort fra en installasjon av et gruppebevisshetssystem med videostrømmer og konferansemuligheter i et arbeidsmiljø,

nærmere bestemt RAVE systemet ved EUROParc. Dette er et tidlig system fra 1993, men har vært toneangivende for det som finnes av personverntenkning i miljøet.

3.4.2.1 Sosial praksis i endring?

Bellotti og Sellen ser en tendens til at det som er akseptabel bruk at innsamlede data er i endring. Sosial praksis og organisatoriske regler for bruk er i endring, og folk ser ut til å akseptere risiko for potensielt person-invaderende teknologi dersom fordelene med teknologiene er store nok. De peker på at vi ikke kan stole på at sosiale og organisatoriske strukturer skal regulere hva teknologier får lov til å gjøre, ei heller kan vi vente på at fordelene med teknologien blir så store at vi finner oss i at våre privatliv blir offentliggjort.

Teknologien er ikke nøytral når det gjelder personvern, den kan øke eller minske kontrollen folk har over personlige data.

Den viktigste effekten av *awareness*-systemer er at personer blir tilgjengelige – aktivt ved at man kan kommunisere med dem, eller passivt ved at man kan se/høre/spore dem. Dette reduserer altså muligheten personer har til å være utilgjengelige, noe som noen kan føle som invaderende. Selv om man kan se eller høre motparten er det også mulig at det vil virke ekstra invaderende dersom man skulle starte en samtale i en situasjon det absolutt ikke passer. Med bakgrunn i disse bekymringene frykter forfatterne sammenbrudd i sosiale normer for kommunikasjon og oppførsel.

3.4.2.2 Designprinsipper

I sitt system har de lagt to designprinsipper til grunn som kan bøte på disse problemene: Kontroll og Feedback(Tilbakemelding).

- ***Kontroll*** *innebærer at personer kan få vite og regulere hva slags informasjon som publiseres og hvem som kan se denne i systemet.*
- ***Feedback*** *innebærer at personer blir orientert om det når informasjon blir innhentet og hvem som gjør dette.*

Disse to prinsippene blir benyttet på fire ulike klasser av problemområder knyttet til datainnsamling:

- Innsamling: Hva slags informasjon blir innsamlet? Stemmer, video, bilder (nær eller fjern?), personlig identitet, lokasjon, arbeidsaktivitet, tastaturaktivitet, progamvare som brukes, filer i bruk, meldinger, dokumenter?
- Konstruksjon: Hva skjer med data når de blir samlet inn. Blir data kryptert på noe punkt? Blir det foretatt korrelasjon mot andre data? Blir data lagret?
- Tilgjengelighet: Er innsamlet informasjon offentlig, tilgjengelig til spesielle grupper, personer, eller bare for den registrerte? Hva slags applikasjoner eller prosesser bruker data?
- Hensikt: Hva brukes informasjonen til? Hvordan kan den brukes i fremtiden?

Til hver av disse problemområdene stilles så spørsmål om hva slags kontroll og feedback som gis av systemet. Disse er presentert i tabell 1.

	Feedback om	Kontroll over
Innsamling	Når og hvilken informasjon som går inn i systemet	Når og hvilken informasjon som IKKE skal inn i systemet. Innstilling av egne preferanser
Konstruksjon	Hva som skjer med informasjonen når det har kommet inn i systemet.	Hva som skjer med informasjon om meg. Innstilling av automatiske *default* preferanser
Tilgjengelighet	Hvilke personer og programvare som har tilgang til informasjon om meg og hva slags informasjon disse kan få	Hvem og hva som har tilgang til informasjon om meg. Innstilling av automatiske *default* preferanser
Hensikt	Hvorfor personer vil ha informasjon om meg, muligens på grunnlag av informasjon om konstruksjon og tilgjengelighet.	Sosial og eventuell juridisk akseptabel bruk av data.

Tabell 1: Bellotti og Sellens designspørsmål for problemområder innen personvern. Fire ulike klasser av spørsmål stilles i forhold til hvilken kontroll og feedback brukeren får

For å systematisk å kunne evaluere løsningene som blir til etter å ha stilt slike designspørsmål har forfatterne satt opp en del testkriterier:

- Pålitelighet: teknisk stabilitet og dertil trygghet hos brukerne.
- Passende timing for feedback: Feedback må gis der det er mest effektivt å utøve kontroll.
- Oppfattelse: Feedback må kunne oppfattes.
- Tilbakeholdenhet: Feedback må ikke være unødvendig distraherende eller irriterende.
- Minimal invasjon av andre: Feedback må ikke gå på bekostning av andres personvern.
- Feilsikkerhet: Dersom bruker ikke gjør eksplisitt valg om noe annet må systemet være mest mulig restriktivt med innsamling, konstruksjon og tilgang.
- Fleksibilitet: Hva som regnes som private data kan variere, og systemet må ta høyde for dette ved å tilby og godta ulike brukerinnstillinger.
- Liten innsats: Brukeren må kunne ha kontrollen med liten innsats, altså så få handlinger som mulig.
- Meningsfull feedback: Feedback kan ikke være rådata, men en meningsfull representasjon/melding.
- Lett å lære: Intuitivt og brukervennlig design i kontroll og feedback miljøet.
- Lav pris: Som alltid ønsker vi rimelige løsninger, både av hardware, software og implementasjon.

Forfatterne ser for seg at deres system kan brukes til å klargjøre problemer i eksisterende systemer, og dermed vise veien for designløsninger som tar hensyn til balansen mellom åpenhet/bevissthet (*awareness*) og personvern. Målet deres er å tilby *awareness* uten å bli påtrengende.

3.4.3 Instant messenger

En populær versjon av et slags åpent gruppe-*awareness* system er *Instant messenger*[6] systemer. Systemene brukes i arbeidssammenheng, men er også svært utbredt som sosial kanal for å holde uformell kontakt med venner og familie., se for eksemplel Grinter et.al.[41]. Klientene har ofte innebygde muligheter for å dele filer, diskutere med meldinger (*chat*), lyd eller bildekontakt, eller til bruke programmer sammen. Klientene registrerer tastatur aktivitet, og inaktivitet i en viss tid blir registrert som om man ikke er til stede.

Forskjellen fra interne gruppebevissthet-systemer er at man aktivt må legge til nye kontakter og ofte få godkjenning av den andre part før man kan se andre personers status og eventuell kontakt kan opprettes. Man må dermed gjøre aktive valg for hvem man vil ha i sin kontaktliste. Prinsippet om at sosial kontroll opprettholdes ved at man gjensidig kan se hverandre er svekket i forhold til direkte arbeidsrelaterte bevissthetssystemer, ved at man ensidig kan endre sin status til å være usynlig for alle eller enkelte personer. På den andre side gir dette en form for kontroll, og man kan ha "sosiale alibi", og bli utilgjengelig for personer man ikke ønsker å være tilgjengelig for.

Instant messenger systemer bygger gjerne på en sentralisert tjener som klienter må registrere seg hos for å endre sin online status. I noen systemer lagrer den sentrale tjeneren kontaktlistene til alle brukere.

Instant messenger systemer har gjerne advarsler innebygd som fraråder personer å gi fra seg sensitive opplysninger over denne kanalen. Grunnen er at kanalen er usikker, ved at all kommunikasjon blir sendt åpent via TCP/IP på Internett.

Lignende systemer er også i markedet for mobiltelefoner, og integreres gjerne mot *Instant messenger* systemer på internett, slik at man alltid kan ha en online status. Disse er gjerne også utstyrt med muligheten til å avsløre lokasjonen til mobile kontakter. I Norge tilbyr både Netcom og Telenor slike tjenester[7].

3.4.4 Personvern = design av brukergrensesnitt?

Innspillene som kommer fra CSCW miljøene fokuserer på arbeidsrelaterte oppgaver. Gjensidig respekt og sosiale relasjoner i arbeidsmiljøet virker som regulatorer. Reguleringen skjer i stor grad ved at systemet tilbyr gjensidighet, altså at "jeg kan se det samme om deg som du kan se om meg". Feedback om bruk av informasjon gir datasubjekter en viss kontroll, og kunnskap om at systemet fungerer på denne måten vil begrense databrukere fra utidig bruk av informasjonen.

Alle typene av *awareness* er fokusert på å tilby best mulig verktøy for samarbeid. Tilbudet om sanntid bevissthet overfor andre medarbeidere blir automatisk gitt, mens ansvaret for eventuelt å begrense innsynet til informasjon blir gitt til den enkelte medarbeider, med muligheter for å endre sin status i systemet. Man forutsetter at dersom brukerne er bekymret for sin status eller personvernsikkerhet, er han også i stand til å forstå konseptene som regulerer hvilken *feedback* og kontroll han kan få. Medarbeiderne er gitt så mye tillit i

6 For eksempel MSN Messenger, Yahoo Messenger og ICQ, og kombinasjoner av disse.protokollene.

7 Tjenestene http://mother.netcom.no/ og http://www.colibria.com/ (Sett des.2004).

systemet at de er i stand til å endre egne innstillinger i systemet, altså hvordan de fremtrer for andre.

Personvern blir dermed et spørsmål om design av grensesnittsystemer som gir feedback om hvilken informasjon som vises for andre, og eventuelt muligheten for å kontrollere dette, som Bellotti og Sellen toneangivende skisserte i [5] . Mulighetene for bedre samarbeid og økt effektivitet virker imidlertid å være overordnet, og personvernet blir relativisert i forhold til dette. Muligheter for *feedback* og kontroll har kommet fordi man ved bruk og evaluering har sett at noen kan oppfatte systemene invaderende. Designanbefalingene gir den enkelte en viss kontroll og følelse av at personlig identifiserbar informasjon faktisk tilhører dem.

3.4.4.1 Sikkerhet og adgangskontroll

Awareness systemer har også en tendens til å kringkaste all tilgjengelig informasjon om lokasjon, aktivitet og identitet til alle som skulle være interesserte innenfor miljøet. Det blir opp til mottakere å filtrere hvilken informasjon han er interessert i, og for datasubjekter å kontrollere hvordan de fremtrer i systemet, gjennom feedback- og kontroll-mekanismene.

Systemet forholder seg som om at alle er brukere av informasjonen, og bryr seg ikke om eventuelle ikkebrukere. Alle er potensielt interesserte, og har tilgang til informasjonen.

Underforstått er det naturligvis de som har tilgang til systemet i form av en arbeidsrelasjon som er autoriserte brukere. Adgangskontroll og eventuell sikkerhet ligger altså utenfor kontroll og interesse av samarbeidssystemet, og man forutsetter samme form for ytre sikkerhet som for all annen trafikk i bedriften.

3.4.4.2 Relasjon til Palen/Dourish og O'Neill

Awareness-systemer befinner seg i utgangspunktet i den mest åpne enden i alle skalaer som Palen/Dourish snakker om i [6]. All tilgjengelig informasjon blir i utgangspunktet avslørt for alle, både når det gjelder identitet, aktivitet og lokasjon, og informasjon blir lagret i tid, eksempelvis som i rammeverket til Gutwin og Greenberg [9]. Den dialektiske og dynamiske prosessen fungerer fordi brukere har tilgang til *feedback* om bruk, og kontroll over avsløring. Den stående avtalen er at all informasjon som den enkelte brukeren ikke velger å kontrollere, er tilgjengelig for alle.

Relatert til O'Neills[7] dimensjoner fungerer arbeidsmiljøet som at all informasjonen er i en sosial informasjonsfære, i et sosialt informasjonsrom , gjennom et sosialt interaksjonsrom, nemlig *awareness*-systemet. Det er imidlertid mulig at noen brukere vil oppfatte at noe informasjon befinner seg i den private sfære, og får med kontrollsystemene mulighet til fleksibelt å regulere dette.

3.4.4.3 Billettsystemer og awareness

Bellotti og Sellens fire ulike problemområder var som tidligere nevnt bakgrunn for de designspørsmål om personvern som jeg stilte til Sporveiens system. Svaret jeg fikk fra Sporveien, beskrevet i kapittel 2, tydet på at dette var relevante spørsmål. Jeg valgte også å se på dimensjonen av *kontroll og feedback* som et viktig personvernkrav, også det inspirert av Bellotti og Sellens arbeid.

Elektroniske billettsystemer er ikke sanntids samarbeidssystemer. Den ene parten vil i hovedsak være datainnsamler, og den andre parten datasubjekt, det er ingen gjensidig innsikt som gir grunnlag for sosial kontroll. Informasjonen blir samlet inn i ettertid, det er ingen øyeblikksinformasjon om et datasubjekts status i systemet.

Hva kan vi så hente ut av *awareness* systemer som kan være nyttig for elektronisk billettering?

Kontroll og *feedback* virker som et godt prinsipp. Brukeren er gitt rett og ansvar for selv å gjøre endringer i sin personlige "profil" for hvordan han vil fremstå. Kjernen i en slik tillit er at det forutsettes at brukeren har tid og mulighet til å sette seg inn i hvordan systemet fungerer, og dette er naturlig i *awareness*-systemer fordi systemet er et hjelpemiddel i jobben. *Feedback* fungerer fordi man gjensidig kan se hvordan kolleger bruker informasjon, og sosiale normer setter grenser for slik bruk.

For billettsystemer fungerer det ikke slik. Den elektroniske billetten er til for å kunne gjøre reisen lettere. Å gi den reisende tilgang til kontrollfunksjoner i billettsystemet for aktivt å regulere informasjonen som samles inn i det han foretar sin reise vil ikke oppleves enkelt. Dette forutsetter at den reisende ser på billettsystemet som nyttig for han, samtidig som han er ekstremt opptatt av å beholde sin integritet. Begge deler er lite sannsynlig, og krav om at man skal foreta slik konfigurering vil oppfattes som unødvendig og vanskelig. Transaksjonskostnadene for kunden vil bli altfor høye.

Å gi tilgang til personlige konfigurering for hundretusener av reisende som gjør millioner av reiser vil også føre til høye transaksjonskostnader for kollektivtransportøren, og vil ha vanskelig for å skalere. Man kunne selvsagt tenke seg at selskapet bare gav reisende med kundeavtale mulighet til å gjøre konfigurasjoner, siden det er data om disse som vil være mest sensitive. Kanskje kunne man tilby at slik konfigurasjon kunne gjøres i kundens "profil" på Internett. Likevel vil nitti prosent av de reisende sannsynligvis ikke bry seg om å gjøre konfigurering, samtidig som kontroll av endrede konfigurasjoner vil medføre en overhead i prosesseringen av data.

Siden tilbakemeldingssituasjonen ikke er symmetrisk, altså at det ikke er to likeverdige parter som samtidig kan se hverandre, faller også *awareness* prinsippet om gjensidig sosial kontroll sammen.

Jeg tror likevel ikke vi totalt skal forkaste prinsippet om kontroll og feedback, men løsningene må skalere, og kontrollen og tilbakemeldingen må brukes annerledes. I følge EU Direktivet[11] og personopplysningsloven[12] må all innsamling og bruk av identifiserbare data være basert på samtykke, og det kan hende at prinsippene om kontroll og tilbakemelding kan brukes i en slik sammenheng.

Ansvaret for å ikke samle inn mer informasjon enn nødvendig ligger imidlertid hos innsamler. Den reisende kan ikke gis ansvar for å kontrollere og holde tilbake informasjon han ikke vil skal samles inn, slik det fungerer i *awareness* systemer.

3.4.5 Kontrakter og utveksling av personvernpolitikk

En annen tilnærming til personvern enn å la enkeltmennesker kontrollere i detalj hva de synes er akseptabelt er å opprette avtaler. Mange mennesker liker avtaler, fordi det gir dem

noe mer eller mindre konkret å forholde seg til i forhold til hva de kan forvente, og en referanse i tilfelle uoverenstemmelser. I dette avsnittet skal jeg se på noen aspekter ved å tilby avtaler for hvordan personlig identifiserbar informasjon skal behandles.

3.4.5.1 Bruk av etiske kontrakter

I en undersøkelse utført av Reynolds og Picard [42] ble et sett personer spurt om hvordan de ville oppleve systemer som hadde sensorer som var i stand til å oppfatte vanlige menneskelige reaksjoner og følelser. Dette var bare abstrakte systemer, men målet var å forstå mer om hvordan mennesker oppfatter slike systemer som etisk akseptable. Spørsmålene fokuserte på om forsøkspersonene syntes systemene tok vare på deres personvern, om de ville bruke dem, og om de i tilfelle ville føle at dette var behagelig. Hypotesen var at personene ville oppleve slike systemer som brudd på privatlivets fred dersom de syntes de var uetiske. Videre spurte man om en innføring av "etiske kontrakter" mellom datainnsamler og datasubjekter, altså forsøkspersonene, ville bedre på denne situasjonen.

Det ble opprettet ulike referansegrupper, der noen ble presentert for begrepet *etiske kontrakter*, og andre ikke. Blant de som ble tilbudt etiske kontrakter var det en betydelig større gruppe som mente at systemene var akseptable. Uten kontrakter opplevde de fleste at slike systemer ville virke invaderende, mens de tvertimot følte seg mer respektert dersom slike kontrakter ble opprettet.

Reynolds og Picard konkluderer med at systemer som vil respektere personvern bør innføre en eller annen form for etisk kontrakt med brukerne.

Undersøkelsene tyder på at mennesker foretrekker å oppleve bli respektert, og at kontraktualisme er en måte å oppnå denne respekten på.

3.4.5.2 Design basert på personvernpolitikk

Marc Langheinrich har i [16] gjort en del betraktninger på hvordan design av personvern innenfor *pervasive* systemer kan gjøres. Ut fra *Fair information practices[10]* og EU direktiv 95/46/EC [11] bygger Langheinrich opp noen noen prinsipper for systemdesign.

En arbeidsgruppe i W3C har kommet fram til en standard for utveksling av personvernpolitikk i Internett: *The Platform for Privacy Preferences Project* (P3P) [14]. I korte trekk går P3P standarden ut på at datainnsamler formidler hvilken politikk han bruker i forhold til en del kjernepunkter for databruk, samtidig som datasubjektet må gis valg i forhold til å godta denne innsamlingen. Når politikken er godtatt, og brukeren har gjort valg for hva han vil godta av datainnsamling, skal dette betraktes som en avtale for hva som er godkjent bruk av informasjon om denne brukeren. Langheinrich har selv vært med i P3P-arbeidsgruppa, og prinsippene som her presenteres har også vært grunnlaget for utviklingen av P3P standarden. P3P presenteres i større detalj i kap. 4.3.4.

Alle modeller som baserer seg på å opprette kontrakter baserer seg i bunn og grunn på tillit.

Grunnleggende for denne tilnærmingen er at man vil bygge systemer som muliggjør at parter kan respektere hverandres krav til personvern. Det innebærer at organisasjoner og personer som vil respektere reglene, også kan gjøre det, og dermed bygge opp tillitsforhold mellom

systemet og brukerne. Systemet bør også hindre uhell der data kommer på avveie og blir tilgjengelig for personer som ikke engang har spurt om dem. Dessuten bør systemet balansere mellom at brukeren skal kunne kontrollere tilgangen andre har til informasjon om han, og at det må være enkelt å bruke.

3.4.5.3 Melding

Åpenhet er et viktig prinsipp fra *fair information practices.* Det innebærer at et individ utsatt for identifisering av et system skal gis melding om at dette skjer.

Langheinrich ser for seg et slags annonseringssystem for når slik identifisering finner sted, på samme måte som trafikkmeldinger slår inn på en bilradio uansett hvilken kanal man lytter til. *Pervasive* systemer kan ha mange slags kapasiteter, alt fra enkle, passive RFID *tags* til sofistikerte enheter med egne sensorer. Energibruken ville bli stor dersom alle enheter konstant skulle kringkaste hva slags politikk de har.

For *pervasive* systemer trenger ikke nødvendigvis alle enheter i systemet være i stand til å kommunisere hvilken politikk den samler inn data under. Innenfor en kontorbygning ville det kanskje være nok med en annonsering i det en person kom inn døren for å informere om hvilke regler for sporing og identifisering som gjelder i dette området. Alle andre sensorer kan så referere til denne annonseringen. Likeså vil et bærbart system (f.eks en mobiltelefon) som en person bærer bare trenge å deklarere hvilke preferanser personen har én gang i en slik sone. Systemet bør da tilpasse seg disse preferansene og begrense sin identifikasjon i forhold til det personen tillater.

Som format for annonseringen ser Langheinrich for seg å dra nytte av deklarasjonsspråket for personvernpolitikk utviklet i P3P standarden.

3.4.5.4 Valg og samtykke

EU Direktivet krever eksplisitt samtykke fra et datasubjekt for at identifiserbare data skal kunne samles inn. Den vanligste formen for samtykke er fremdeles underskrift for hånd. Dette er et problem for elektroniske systemer. Digitale signaturer med bruk av *public key* kryptografi har eksistert lenge og har blitt innført i forskjellige versjoner steder, men er fremdeles ikke i utstrakt bruk. Et at problemene er at man må være sikker på at en person faktisk har initiert bruken av sin elektroniske signatur. Det kan ikke bare være en persons software som gjør dette.

I elektronisk handel bekrefter man gjerne et kjøp ved å trykke på en knapp i en nettleser. Brukere og nettbutikker har akseptert dette som en tilstrekkelig krav av samtykke, i tillegg til at bruker gir fra seg betaling- og leveringsinformasjon for å få kjøpe varen. I *pervasive* systemer kan det å måtte trykke på en knapp, f.eks på mobiltelefonen for å akseptere datainnsamling overalt, med kanskje hundrevis av forespørsler i timen, bli en helt umulig ordning. Dette står i kontrast til at datasubjekter skal ha melding når datainnsamling foregår.

Datasubjekter skal ha et faktisk valg. Det skal altså være flere valg enn at "enten går du med på våre betingelser, ellers kan du ikke benytte tjenesten/må du forlate området". Det kan være at man da ikke kan gå inn i en bygning, kjøpe en vare, eller benytte et transportmiddel. Ofte har man da ikke noe valg, og må gå med på systemets betingelser. Der det er mulig å

gjøre nøyaktig posisjonering og identifikasjon bør det være mulig å gjøre informasjonen mindre nøyaktig, basert på identiteten til datainnsamler (Nødsituasjon vs. kommersiell aktør).

3.4.5.5 Anonymitet og pseudoanonymitet

Vanskelighetene med alltid å alltid måtte få samtykke fra brukere for å kunne samle inn data leder til krav om at en bruker skal kunne være anonym, eller i alle fall til en viss grad: Pseudoanonym. Dette må til både for å kunne gi datasubjekter et valg, og for å tillate datainnsamling uten å trenge samtykke. Dersom data ikke kan knyttes til noen spesiell person trengs det nemlig ikke noe juridisk samtykke.

På Internett finnes det flere ulike løsninger som ivaretar dette ved å maskere brukerens IP adresse, ved å gå gjennom ulike slags proxier[8] når man gjør forespørsel på Internett.

For *pervasive* systemer er slike metoder sannsynligvis lite brukbare. En lokasjon på Internett en noe annet enn en faktisk fysisk lokasjon i den virkelige verden. Dersom et kamera har tatt bilde av en person, eller annet sensorutstyr har identifisert et element i tid og rom er det vanskelig å nekte for dette.

I dagens trådløse systemer, f.eks Bluetooth protokollen, og WiFi protokollene (IEEE 802.11x) er det lagt opp til å gjenkjenne trådløse objekter ved hjelp av nettverkskortets MAC adresse. Denne adressen er unik for hvert nettverkskort, og vil med andre ord identifisere objektet og lokasjonen til personen som bærer denne. Veien til å identifisere personen trenger ikke være lang. Langheinrich foreslår at slike protokoller bør tilpasses til å bruke engangsadresser i stedet for faste hardware adresser.

Ofte er det ønskelig å kunne være identifiserbar innenfor en viss grense. En del applikasjoner krever at en person skal autentiseres for å gi tilgang. Langheinrich innfører da begrepet pseudoanonymitet, der en person kan tilegnes en personlig ID når vedkommende er autentisert, og beholder denne inntil han skifter identitet. På den måten kan tjenesten personaliseres samtidig som brukeren har muligheten til å trekke seg ut av situasjonen. Dette er på lignende måte som sesjoner fungerer på webservere.

Selv med hardware som skifter fysisk identifikasjon periodisk trenger det ikke være så vanskelig å koble identiteter sammen. Dersom et objekt med en temporær ID på en lokasjon plutselig har en ny ID, men befinner seg på samme sted, så er det sannsynligvis det samme objektet.

3.4.5.6 Nærhet og lokale data

Portabelt utstyr kan ha muligheter til å lagre data. Langheinrichs eksempel er en "gjenglemt" kaffekopp som har lagringsmuligheter for lyd. Tanken er at utstyret ikke skal fungere så lenge eieren ikke er tilstede. På den måten vil det ikke være mulig å overvåke samtaler og situasjoner man ellers ikke ville være fysisk vitne til.

På samme måte tenker Langheinrich seg prinsippet om lokale data: Data skal bare eksistere i det miljøet de ble innsamlet. Dette kan i noen tilfeller være et alternativ til å utvikle og

8 Et eksempel er http://www.anonymizer.com/. (Sett des.2004)

innføre avanserte autentiseringsløsninger for hvordan data skal kunne spres. På samme måte som data kan bli kassert fordi de er for gamle, kan de også kasseres fordi de befinner seg utenfor området de var ment for. Innenfor et definert område er imidlertid all innsamlet informasjon og alle tjenester i prinsippet tilgjengelig til alle. Utenfor området blir det vanskelig eller umulig å finne den samme informasjonen og tjenestene.

3.4.5.7 Tilstrekkelig sikkerhet

I mange sammenhenger omtaler vi sikkerhet og personvern som om det skulle være det samme tema, og som om dersom vi bare får tilstrekkelig sikkerhet vil personvern komme av seg selv. Disse tingene henger selvfølgelig sammen, men sikkerhetsløsninger er bare et verktøy for å sikre data. Med allestedsnærværende systemer kan dette bildet endre seg. Passive RFID *tags* vil for eksempel ikke kunne ha nok regnekraft til å kunne drive kryptering på samme nivå som man har med for eksempel finanstransaksjoner, pasientjournaler og overføring av andre svært sensitive data.

Lavenergi transmisjonsutstyr, som det vil være snakk om i mange *pervasive* systemer, har imidlertid en begrenset rekkevidde. Man må da gjøre en avveining mellom hvor viktige data er mot hva konsekvensene ville være dersom noen skulle spionere på disse transmisjonene.

Dersom man anvender prinsippene om nærhet og lokale data med at data ikke skal spre seg utenfor områdene de var ment for, altså lokalt, kan man oppnå tilstrekkelig sikkerhet i slike systemer uten noen spesiell sikkerhetsmodell for data. Da unngår man også å legge grunnlaget for uønskede overvåkningssystemer.

3.4.5.8 Tilgang til lagret informasjon og bruken av denne.

Viktige prinsipper ut fra *fair information practices* er at den registrerte må ha tilgang til lagrede data om seg selv, og at den registrerte kan få informasjon om bruken av de lagrede data.

Langheinrich ser for seg at teknologi kan hjelpe til med å oppfylle disse kravene. Hans forslag er å utvikle *Privacy Aware* lagringsteknologi. Med det mener han databaser som lagrer innsamlet data og retningslinjer for bruk av disse samlet (Se kap .). Han ser også for seg utvidelser av P3P protokollen til å omfatte krav til f.eks bruk av digitale signaturer ved datautveksling, slik at data ikke kan spres uten samtykke, og at kommunikasjonen dermed kan bevises ved eventuelle uoverensstemmelser.

3.4.5.9 Langheinrichs prinsipper og personvernkrav i Sporveien

Langheinrichs har en tilnærming som ser på personvern fra et systemsynspunkt mer enn som et sosial regulering, slik som Palen og O'Neill har gjort. Han forholder seg til lovgivningen og prøver å operasjonalisere denne i noen krav til systemer. I motsetning til *awareness*-systemer forholder han seg også i større grad til hvordan personlig informasjon kan utveksles *mellom* entiteter, mer enn internt i entiteter.

Langheinrich peker på flere prinsipper som er aktuelle for Sporveiens system. Hans diskusjon om melding, valg og samtykke er knyttet nært opp til EU direktivets krav om samtykke. Han peker på at en kontinuerlig innhenting av samtykke for innsamling av data vil være funksjonelt uakseptabelt, både for kunden og for datainnsamler.

Han ser for seg å formidle en avtale i form av en P3P politikk bare én gang for hver gang en bruker kommer til et domene som er dekket av denne avtalen. For Sporveiens del kunne dette innebære å gi brukeren noen valg han kan samtykke i eller avvise i det han kjøper en billett, eller i det han oppretter en kundeavtale. Dermed blir det én avtale gjeldende per billett, eller per kunde, dersom kunden er identifisert. Dette vil likevel innebære en transaksjonsbyrde for kunden i forhold til at valgene kan være vanskelige å forstå. Kundene må i så fall læres opp i å skjønne personvernterminologi eller relevante spørsmål etterhvert. Selskapet får ekstra prosessering i å kontrollere hvilket samtykke som er gitt, spesielt dersom samtykke skal få innvirkning på *hvilke* data som samles inn, ikke bare hvordan de skal brukes. Da må nemlig funksjonaliteten i å kontrollere dette distribueres, i prinsippet helt ut til validatorene.

Alternativt kunne man jo tenke seg å kombinere en slik avtalekontroll med Langheinrichs prinsipp om nærhet og lokale data. En del prosessering kan foregå lokalt i miljøet der som billettene ble samlet inn, og bare aggregerte data sendes oppover i systemet.

Dette ville imidlertid øke kompleksiteten i de lokale systemene. Man måtte ha distribuert tilgang til å gjøre oppslag på basis av billettinformasjon, noe som kanskje vil være vanskelig å administrere. Det ville også utgjøre en sikkerhetsrisiko i forhold til mulig uautorisert tilgang på de samme sensitive data.

Et alternativ er det som Sporveien mener de har valgt, nemlig å anonymisere billetter. Langheinrich peker på at slik anonymisering kan være mulighet for å unngå kravet om samtykke, selv om han minner oss på at anonym informasjon ofte kan personifiseres.

Sporveiens løsning anonymiserer ved *ikke* å knytte en den reisendes identitet til billettens serienummer. Serienummeret kan brukes til å rekonstruere reisemønster i en billett. En versjon der man bruker engangs-ID/pseudonym for hver reise kan ytterligere anonymisere reisen, siden reiser i billetten da ikke vil ha noen sammenheng. Men slik som Sporveien har planlagt sitt system er serienummeret tenkt som en del av en digital signatur som sikrer økonomisk integritet i billettene. Dersom pseudonym skulle bli aktuelt, måtte digital signering foregå på en annen måte.

Langheinrich ser på sikkerhet som en forutsetning for å bevare personvern, og har dette med i sin diskusjon. Han er imidlertid pragmatisk i forhold til mengden, spredningspotensiale og sensitiviteten av informasjon på ulike nivå av datainnsamlingen, og design av adgangs- eller sikkerhetssystemer er ikke en del av hans designprinsipper.

Langheinrich vil bruke teknologi for å kunne gi den enkelte tilgang til informasjon som er lagret om seg selv og om bruken av disse. Det samme har Sporveien tenkt i sitt system, blant annet med tjenester gjennom Internett. Et spørsmålet er om slik tilgang kan medføre et nytt sikkerhetsproblem i forhold til på nytt å måtte beskytte mot spredning gjennom førstehåndsinformasjon og observasjon. Det som datasubjektet kan få tilgang til, kan også andre potensielt få tilgang til, og dette må det tas høyde for ved design av sikkerhetsløsninger for disse delene av systemet.

3.5 Oppsummering av personvernteori og design

I dette kapitlet har jeg beskrevet og relatert diverse teoretisk arbeid innenfor lovgivning, sosial regulering og design av personvernsystemer. Jeg vil nå oppsummere dette i forhold til mine personvernkrav identifisert for mitt scenario.

Mitt personvernkrav om kontroll og *feedback* er et prinsipp som kan fungere i en del domener for allestedsnærværende systemer. Samtidig kan det virke som tilbakemelding og kontroll gjør det vanskelig å ta i bruk personvernsystemer for de fleste brukere som ikke har direkte interesse eller nytte av systemet i seg selv.

Kontroll og feedback tolkes også ulikt i forskjellige miljøer. I awareness systemer og i Palen/Dourish og O'Neills teorier gjør kontroll og feedback det til den enkeltes ansvar å holde tilbake informasjon. Av lovgivning og i Langheinrichs diskusjon, blir alt som det ikke er gitt samtykke til å dele, holdt tilbake. Kontroll innebærer dermed å frigjøre informasjon mer enn å holde tilbake.

De aller fleste har "ryggmargsreflekser" for hva som er godt personvern. Hvor de sosiale grensene for disse refleksene går kan variere. Kanskje kan vi omtale slike følelser for god databehandling som implisitte avtaler. Vi har også sansen for eksplisitte avtaler, og kanskje kan slike brukes for å opprette kontrakter mellom datainnsamler og datasubjekt om hvordan informasjonen skal håndteres.

Både kontroll-og-tilbakemelding og avtaler medfører økt kompleksitet i systemet som skal håndtere transaksjoner, samt økt vanskelighetsgrad og økte krav til opplæring av brukere av systemet. Transaksjonskostnadene ved å operasjonalisere teknologi av disse teoriene kan altså blir store.

Sikkerhet blir behandlet ulikt av de forskjellige miljøer. I de fleste miljøer er beskyttelse av førstehåndsinformasjon satt utenfor diskusjonen om personvern. Innenfor CSCW miljøet er sikkerhet betraktet som noe som ligger fullstendig utenpå deres domene. Andre igjen ser på sikkerhet som relativt i forhold til sensitiviteten og mengden av kommunikasjon. I tillegg må man i design av sikkerhetsløsninger ta hensyn til at datasubjekters rett og krav på tilgang til egne data gjennom usikre kanaler kan medføre en ny trussel for at informasjon kommer på avveie. Dessuten er sikkerhetsløsninger også avhengig av å skalere, og dette vil få betydning for hvor avansert adgangskontroll og beskyttelse av data man kan bruke i de ulike nivåer.

I neste kapittel vil jeg se nærmere på noen av de løsningsmodeller som finnes for personvern i de teknologiene som ser ut til å konvergere, og forsøke å belyse disse ved hjelp av de personvernkrav og teorien jeg har presentert i dette kapitlet.

4 Konvergerende teknologi og løsningsmodeller for personvern

I dette kapitlet vil jeg først se på noen av beskyttelsesmekanismene som brukes på tvers av domener for beskytte informasjon mot uautorisert adgang og observasjon. Jeg vil så se på hva som karakteriserer de personvernmodeller og problemer som finnes for teknologiene som konvergerer: mobiltelefonsystemer på den ene side og distribuerte systemer/Internett på den andre. Deretter vil jeg presentere noen modeller som påstår å tilby personvernløsninger for allestedsnærværende systemer.

Teknologi omkring personvern har så langt vært delt i grovt sett 2 metoder.

Den første metoden fokuserer på å beskytte førstehåndsinformasjon fra å bli observert eller gitt direkte til tredjepart. Dette er modeller som anonymiserer meldinger som blir sendt, får kommunikasjon til å fremstå som støy for uinnvidde parter, systemer som blokkerer for innsamling av informasjon, klienter som bare bruker andre systemer passivt uten selv å gi seg til kjenne (som f.eks GPS-klienter), krypteringsystemer, og adgangskontrollsystemer.

Den andre metoden fokuserer på å opprette "kontrakter" for innsamling og bruk av informasjon, enten i form av full-tekst kunngjøringer eller som maskinlesbare kunngjøringer som kan prosesseres med bakgrunn i brukerens innstillinger. Data blir så eventuelt delt med datainnsamler dersom brukeren godtar personvernpolitkken. Omkring dette kan man bygge rammeverk som begrenser hvilken informasjon som blir delt, nøyaktigheten av disse, samt delvis kontroll på om de avtalte kjøreregelene for informasjonen blir fulgt.

La oss først se litt på noen beskyttelses teknikker.

4.1 Sikkerhet og anonymisering

4.1.1 Kryptering

Kryptografiske teknikker er basis for de fleste metoder for autentisering, sikkerhet, og integritet i distribuerte systemer. Valg av kryptografiske algoritmer og håndtering av kryptografinøkler er kritisk for om sikkerhetsløsninger fremstår som effektive og brukbare. *Public-private key*[9] kryptografi gjør det mulig å distribuere hemmelige nøkler på en sikker måte. Denne slags algoritmer baserer seg på asymmetriske enveisalgoritmer basert på store primtall. To parter i en kommunikasjon utveksler *public keys,* som brukes til å kryptere informasjon som sendes den andre parten. For dekryptering kreves en korresponderende *private key*, og denne er det bare mottaker som har. Ved transmisjon av store mengder av data er denne teknikken altfor ressurskrevende og sakte. Protokoller slik som *Secure Socket Layer* (SSL) etablerer en sikker kanal ved hjelp av *public-private key* kryptografi, for så å bruke denne til utveksle hemmelige nøkler som brukes til symmetrisk kryptering av informasjon, altså at kryptering og dekryptering skjer med den samme nøkkelen. *Public-private key* algoritmen brukes også til digital signering og opprettelse av digitale sertifikater, som kan være med å sikre integriteten og tilliten i den informasjonen som er utvekslet. En oversikt av krypterings- og sikkerhetsteknikker finnes for eksempel i Couloris' bok om distribuerte systemer [21].

9 Ofte omtalt som *RSA public key* kryptering, etter navnet på utviklerne: Rivest, Shamir og Adelmann.

4.1.2 Unlinkability og Unobservability

Det finnes teknologier for totalt å maskere lokasjon, kommunikasjon og identitet mellom en avsender og en mottaker. Kong og Hong beskriver i [22] *unlinkability* som metoder for å kunne maskere hvem avsender og mottaker av en melding er, og *unobservability* som metoder for å maskere meldinger slik at de for uinnvidde ser ut som støy i radionettet. Slik maskering har blitt utviklet i militært øyemed, og spesielt for kommunikasjon over radiofrekvensbånd. Maskering for *unlinkability* bygger på en artikkel av Chaum fra 1981 [24] (MIX) om anonymisering av mottaker- og returadresse i elektronisk epost, ved bruk av *public-private key* kryptering. Dette skjer ved at meldingen til mottakeren, inkludert adressen, blir kryptert med hans *public key*, og dermed kan den bare pakkes ut og forstås av den rette mottaker. På samme måten er returadressen kryptert med senderens *public key,* og dermed er det bare senderen som kan pakke den opp.

I Kong og Hongs system, ANODR[22], skjer dette på samme måte ved at man først etablerer en rute til mottaker ved hjelp av *forwarding* og *broadcasting*. I tillegg til sending av ekte meldinger fra noden og videresending av meldinger som fra en andre avsendere, genererer også noden falske meldinger, slik at trafikken ut fra noden er nokså konstant. Alle meldinger blir kringkastet. Man benytter seg så av såkalt *onion routing,* der alle mellomliggende noder bare deler sin *public key* med neste node på veien, og dermed er det bare denne som kan dekryptere meldingen for å finne ut hvem som er neste node i ruten. Alle andre noder som hører kringkastingen vil altså ikke kunne dekryptere meldingen. Den faktiske senderen og mottakeren av en melding er derfor anonym fordi man ikke kan avgjøre om en node sender en melding, *forwarder* andres meldinger , eller bare sender genererte meldinger.

Det er selvsagt flere haker med slike system: Det blir generert mye unødvendig trafikk, det kreves mye prosessering, og hele frekvensbåndet blir brukt til kringkasting.

Andre, som Beresford i [27], har sett på muligheter for å opprette *mix*-soner, der det ikke genereres unødvendig trafikk, men der meldinger som blir sendt forsinkes og endrer rekkefølge i infrastrukturen slik at eventuelle observatører ikke kan koble meldinger sammen etter rekkefølge eller tidspunkt. Dette krever selvfølgelig en ganske høy trafikk; med bare en sender er denne unikt identifisert. En lignende fremgangsmåte er presentert av Gruteser og Grunwald i [23]. De bruker begrepet *k-anonymitet*, som innebærer å redusere nøyaktigheten til frigjort informasjon, spesielt om lokasjon, slik at en person blir umulig å skille fra *k-1* andre personer, der *k* er variabel etter ønsket om anonymitet. Dette kan gjøres ved å endre størrelsen på området som blir angitt for lokasjon, eller ved å endre tidsrommet slik at *k* personer har vært inne i et gitt område.

I forhold til å gi personer tilgang til tjenester basert på egen lokasjon er det tryggeste å bare passivt innhente informasjon, og ikke selv slippe ut noe informasjon. Utendørs fungerer GPS [43] på denne måten, og for innendørs miljøer har Priyantha [44] presentert et slikt passivt system, kalt *Cricket location system.* I slike miljøer blir det opp til bruker å avgjøre når de vil gi seg til kjenne, i form av lokasjon eller identifisering mot en tjeneste de vil benytte.

4.1.3 Sikkerhet i RFID tags

RFID teknologi, kort beskrevet i fotnote 1, kap 1.1, er aktuell teknologi for automatisk

innsamling av informasjon.

Strekkoder har lenge blitt brukt til å identifisere produkttyper, men med RFID merking kan hvert enkelt produkt unikt identifiseres i produktlinjer. Relativt enkle RFID brikker kan selv lagre informasjon om sitt eget livsløp, spesielt dersom de har såkalte MEMS (Mikroskopiske Elektro Mekaniske Systemer) innebygd. RFID *tags* trenger ikke direkte øyesyn for avlesing, mange *tags* kan effektivt leses samtidig. Bedrifter kan bruke teknologien til å overvåke hvor alle produkter er i produktkjeden, og bruke dette for produksjonsplanlegging og som anti-tyveri middel.

RFID *tags* brukt i produktmerking vil følge produktene også når de er kjøpt av mennesker, og kan fremdeles avleses, og dermed være med på å identifisere og lokalisere mennesker etterhvert som generaliserte lesere blir vanlig. Det samme er tilfelle med andre RFID produkter som er innebygd i eksempelvis billetter og i Autopassbrikker.

Antikollisjonsalgoritmer for kommunikasjon mellom RFID *tags* og lesere er en sikkerhetsrisiko i seg selv (Sarma et.al [2] s.460). Leseren vil ende sitt binærsøk for hver *tag* ved å ende opp med å bare ha en *tag* som svarer, og da med sitt serienummer. Både leseren og tagen vil altså sende det unike serienummeret, som identifiserer tagen, og potensielt den som tagen tilhører. Utenforstående observatører kan lytte på denne kommunikasjonen, eller utgi seg for å være en autorisert leser. Sarma et. al. har i [2], 464ff beskrevet noen metoder for å bedre sikkerheten. For å umuliggjøre sporing etter salgsøyeblikket har de foreslått en *kill-tag* prosedyre, der man fysisk ødelegger de elektriske egenskapene i en *tag* ved å bruke en passordbeskyttet *Self Destruct* kommando.

Selv-ødelegging fungerer ikke i de tilfeller der det er ønskelig at tagen kan brukes videre, eller dette er en del av tagens funksjonalitet, som vil være tilfellet for de fleste andre applikasjoner enn produktmerking. I disse tilfellene ønsker man å kunne kryptere kommunikasjonen mellom *tags* og lesere. Symmetrisk kryptering kan kanskje fungere, mens avansert *public-key* kryptering foreløpig krever for mye prosessering i forhold til kravet om enkle og billige *tags*[10].

Sarma skisserer en metode med *hash-locks* der en tag kan låses, og låses opp ved en enveis *hash* algoritme som bare er kjent av en autorisert part. Når en tag er låst, vil den bare svare med en *hash*-generert meta-ID, og ikke frigi annen informasjon som ligger i tagen.

Sarma mener likevel at sikkerhetsrisikoen i forhold til observatører er begrenset, da enkle RFID brikker vil ha en svært kort transmisjonslengde og gjennomtrengingsevne[11].

En alternativ metode for å beskytte RFID brikker fra avlesing er presentert av Juels et.al. i [28]. De foreslår å innføre en *blocker tag* som benytter seg av antikollisjonsalgoritmen for RFID systemer til selektivt å blokkere leserens forsøk på å identifisere RFID *tags*.

4.1.4 Sikkerhet for Mobiltelefoni

I GSM nettverk er lokasjonsinformasjon viktig for at man skal kunne rute innkommende samtaler til mobiltelefonen. Tjenesteleverandøren lagrer informasjon om en mobilabonnent i

10 Industrien ønsker prisen under 5¢ per tag for å kunne erstatte strekkoder i produktmerking.

11 13.56Mhz *tags* har ca 1m rekkevidde, og bølger fra 915Mhz *tags* vil ikke kunne trenge gjennom noe materiale.

et såkalt *Home Location Register (*HLR) (Tisal [31] kap 6). I HLR finnes statisk informasjon som identifiserer abonnenten og beskriver tjenestene han abonnerer på, samt dynamisk informasjon om mobilterminalens gjeldende lokasjon, samt siste kjente status for terminalen (ledig, opptatt, avslått, ute av dekning). Lokasjon vil være hvilken celle og basestasjon terminalen sist var aktiv. HLR er plassert i en sentral lokasjon hos tjenestetilbyder, men med begrenset adgang, og alle data er lagret kryptert.

HLR blir kontinuerlig oppdatert med dynamisk lokasjon- og statusinformasjon fra *Visitor Location Register* (VLR), som er databasen tilknyttet den mobil-*switchen* som har ansvaret for cellen som brukeren befinner seg i. Ved innkommende anrop blir det så gjort gjentatte oppslag i disse databasene for å finne riktig celle, før man gjør en *broadcast* i denne cellen med mobilterminalens identifikator. Protokollen fungerer slik at bare den telefonen som har riktig identifikator svarer på anropet, og genererer en ringetone i telefonen.

Teknologier som muliggjør mobiltelefoni forutsetter altså at mobilterminalen er knyttet til en celle, og at denne tilknytningen er kjent i systemet. En mobiltelefoncelle kan variere fra 200m i utstrekning i tettbygde strøk, til ~30km i utkantstrøk, avhengig av transmisjonseffekten til basestasjonene. Mobiltjenesteleverandøren vil altså grovt sett alltid vite i hvilket område en abonnent befinner seg, og kan eventuelt bruke dette til å spore sine kunder. Ytterligere lokalisering kan gjøres ved *triangulering.* En celle vil som regel ha delvis dekning av flere basestasjoner, og ved å måle tidsforsinkelse på signaler som går til ulike basestasjoner kan posisjonen bestemmes (Se f.eks lenke i fotnote 2, side 7). Triangulering kan gjøres av tjenesteleverandør eller av ytre observatører.

Görlach refererer i [4] til Federrath et.al [26] som har sett på muligheter for å hindre triangulering ved hjelp av frekvensmoduleringsteknikker som gjør det vanskelig å skille mobiltelefonsignaler fra bakgrunnsstøy. I [25] foreslår Federrath et. al. også et system som ved hjelp av MIX konseptene presentert i 4.1.2 kan maskere lokasjonen til en mobilterminal.

En del sikkerhetsløsninger er bygd inn i GSM standarden som gjør det vanskelig å benytte et mobilnettverk ulovlig eller observere kommunikasjon som foregår der.

For å beskytte nettverket mot inntrengere, og for å sikre mobilbrukere at de blir fakturert for faktisk bruk av mobiltjenesten, må alle mobile stasjoner autentiseres og deres rettigheter i systemet kontrolleres hver gang en mobilterminal melder seg på nettverket. Dette skjer i *Authentication Center (*AUC), en database tilknyttet HLR, som lagrer konfidensiell informasjon. AUC lagrer en hemmelig algoritme og en personlig krypteringsnøkkel, som også finnes i mobilbrukerens *Subscriber Identity Module* (SIM) kort. En kalkulasjon med bruk av nøkkelen og algoritmen gjøres både i mobilbrukerens SIM kort og i AUC. Resultatet sendes fra mobliterminalen til AUC, som autentiserer brukeren kun dersom svarene stemmer overens ([31] s 78ff).

Kryptering av tale- eller datakommunikasjon over radiokanaler i GSM er også en del av standarden, og man benytter seg også da av krypteringsnøkler som blir lagret i SIM kortet når abonnementet blir initialisert.

Identiteten til en abonnent blir maskert i nettverket. I autentiseringsprotokollen med HLR og AUC sendes brukerens *International Mobile Subscriber Identity* (IMSI) nummer til nettverket.

IMSI identifiserer abonnementsnummeret, landet og tjenesteleverandøren til en abonnent ved autentisering. Når brukeren er autentisert får han tildelt en midlertidig identifikator, et *Temporary Mobile Subscriber Identity* (TMSI) nummer, som endres for hver gang brukeren kommer inn i en ny mobilsone. Ved senere kommunikasjon er det dermed vanskelig for utenforstående å knytte abonnenten til den midlertidige TMSI identiteten.

Ved hver utgående samtale kontrolleres forøvrig mobilterminalens *International Mobile Equipment Identity* IMEI nummer, som unikt identifiserer mobilutstyret uavhengig av SIM kortet. Dette kan brukes til å spore bruk av uautorisert eller stjålet utstyr.

Måten GSM standarden tilbyr mange mobilbrukere å bruke det samme begrensede frekvensbåndet samtidig er en viss sikkerhet i seg selv. For uinnvidde, altså de som ikke har algoritmen og nøkkelen for hvordan transmisjonen konstant endrer seg, vil bruk av *Multiple Access* teknikker i kombinasjoner av *Frequency Division Multiple Access* (FDMA) og *Time Division Multiple Access* (TDMA) bli uforståelig. Med *Code Division Multiple Access* (CDMA) vil all kommunikasjon se ut som det bare er støy i frekvensbåndet. To kommuniserende parter kjenner hvordan kodingen endrer seg for deres kommunikasjon, men vil anse alle andre parter som støy[12].

4.1.5 Sikkerhet i smartkort

Smartkort er ofte brukt som en samlebetegnelse for alle slags kort av kredittkort-størrelse som har mer minnekapasitet enn tradisjonelle magnetstripekort (Shelfer [30]). Smartkort er imidlertid ikke begrenset til å bygges inn i kredittkort. Jeg har alt nevnt at SIM kort i mobiltelefoner er en type smartkort. I Sporveiens elektroniske billettsystem ser man også for seg å bruke slike kort, i det minste som kundekort. I tillegg finnes smartkort for mange andre tjenester, blant annet som kreditt/debet/kontantkort, helserettighetskort, dekoderkort for kabel-TV, og avanserte identifikasjonskort.

Smartkort kommer i to kategorier: minnekort og kort med innebygd prosessor. Minnekort er gjerne utstyrt med et variabelt *Read Only Memory* (ROM) på mellom 8Byte og 2KByte, mens vanlige magnetstriper kan holde 220byte. Minnekort har som regel liten eller ingen systemer for sikkerhet, så informasjonen kan som regel enkelt avleses. De vanligste formene for bruk er som forhåndsbetalte kort, som telefonautomat-kort, eller enkle billetter og klippekort. Minnekort kalles også asynkrone kort, fordi data som regel bare går en vei: fra kortet til leseren. Den elektroniske ekvivalenten av kontanter blir overført til leseren, og dermed registrert som betaling.

Smartkort med prosesseringskraft er for mange de *ekte* smartkort, og er også kalt synkrone smartkort, siden de både kan leses fra og skrives til. Kortene har både *Random Access Memory* (RAM), en liten 8-bit prosessor som kan brukes til å kjøre programmer, ROM minne, samt *Electric Erasable Programmable Read Only Memory* (EEPROM) minne, som kan brukes til å programmere data, nøkler og passord. Slike kort har også gjerne innebygde kretser som kan foreta avanserte krypteringsoperasjoner, slik som *public key* kryptering, digital signering og verifisering. I tillegg til aktiv kryptering av data på kortet kan data sikres ved kombinasjon med såkalt *biometrisk* identifikasjon, slik som iris-avlesing eller fingeravtrykk, for unik

12 Se Tisal [31] s.20ff og 35ff for flere detaljer.

identifikasjon av den autentiserte brukeren av smartkortet. Slike innebygde sikkerhetsmekanismer gjør smartkort mye vanskeligere å duplisere enn tradisjonelle magnetkort. Smartkort er sertifisert som "sikre" av ITSEC[13].

Smartkort er standardisert i ISO/IEC 7816. For begge typene av smartkort er det utviklet løsninger som kan avleses kontaktløst, altså på avstand, uten fysisk kontakt med leseren. Dette innebærer at smartkortene har RFID kretser bygd inn i kortene. Kontaktløse kort er standardisert i ISO/IEC 14443, og som ISO/IEC 15963 for kort som kan avleses fra større avstander.

4.1.6 Sikkerhet og anonymitet i Sporveiens system

4.1.6.1 Anonymitet

Teknologi som maskerer mottaker og avsenders lokasjon og kommunikasjon mellom disse er åpenbart viktig i noen sammenhenger, eksempelvis militære, der slike avsløringer ville kunne medføre ekstrem fare for personell. Man kunne jo selvsagt tenke seg at denne slags maskeringsprotokoller mot ekstern observasjon ble lagt inn for all kommunikasjon som foregår i et billettsystem. Dette ville medføre ekstreme prosesseringskrav i alle ledd, inkludert billettmedia, for kryptering og dekryptering, eventuell generering av falsk kommunikasjon, samt synkronisering av kommunikasjonsprotokoller (f.eks CDMA). I tilfellet med avlesing av billett ville det også være totalt bortkastet fordi observatøravstanden er i størrelsesorden *meter*, og da kan man bruke andre og enklere metoder for å oppdage personer enn å finne ut om trådløs kommunikasjon foregår.

4.1.6.2 Sikring av kommunikasjon

Mye oftere er det viktigere å beskytte identitet og informasjon som blir sendt mellom to parter, mer enn det faktum at kommunikasjon mellom dem foregår. Det er også disse situasjonene de fleste krypteringsmetoder adresserer, og i alle fall midlertidig løser. Midlertidig, fordi det med dagens matematiske metoder og prosessorkraft ikke er mulig å knekke krypteringen, altså å finne de hemmelige nøklene, innenfor en overskuelig tidsramme dersom nøklene er store nok (f.eks 128bit).

Også for elektroniske billettsystemer vil beskyttelse av identitet og informasjon være det viktigste i alle kommunikasjoner. Jeg har beskrevet en del problemer knyttet til beskyttelse av informasjon ved bruk av RFID *tags*, der antikollisjonsalgoritmen byr på problemer i forhold til avsløring av det unike serienummeret, fordi disse som regel har begrenset prosesseringskraft til bruk i kryptering. Disse problemene er kraftig redusert for RFID i kombinasjon med bruk av kontaktløse smartkort, som for eksempel kan kreve autentisering av leseren og kryptering av informasjonen.

Kontaktløse smartkort er forøvrig allerede i bruk i flere andre storbyers billettsystemer, for eksempel i London[14].

13 ITSEC: Information Technology Security Evaluation Certification representerer et sett av software og hardware sikkerhetsstandarder som er godkjent i Europa og Australia, iflg.[30]

14 Londons elektroniske billettsystem: http://www.oystercard.com/ (Sett des.2004)

For de "enklere" elektroniske billettene er situasjonen imidlertid en annen. Sporveien sier at disse også skal være sikre. De bør på den andre side være billige, siden de bare er beregnet for korttids bruk, og sikkerhet koster, i form av krav til prosesseringskraft. Sannsynligvis er det en variant av den enkle typen av smartkort, minnekortene, som vil bli brukt. Disse må likevel være avanserte nok til å lagre transaksjonsinformasjon i kortet.

Fra et personvern-ståsted er fordelen med disse "enkle" billettene at den reisende er så godt som anonym, i alle fall så lenge han betaler kortet kontant. Men siden de er teknisk og sikkerhetsmessig enklere, vil de også være enklere å forfalske, noe som sannsynligvis er uønsket fra Sporveien side. Mange banker og kredittkortselskaper har erfart at problemene med forfalskning har sunket betraktelig ved innføring av smartkort i stedet for enklere kort, som magnetstripekort. Slike forhold kan medføre at Sporveien kommer til å sette i gang tiltak for å få flest mulig til å skaffe seg kundekort, som er et smartkort. Sporveien har designet at alle billett-typer kan lagres på et kundekort. Disse kortene er sikrere, mange slags tilleggs-tjenester kan tilbys, og dermed burde det være få grunner til ikke å skaffe seg et slikt kort.

Smartkortene er dyrere å dele ut til kundene enn de "enklere", men likevel ganske avanserte billettene. Dette kan fra Sporveiens side veies opp ved at man ved sikrere kort kanskje øker tilliten hos kundene og reduserer mulighetene for forfalskninger, samt at man selger færre "enkle" billetter som blir kastet etter kort tid.

På den andre side har man da kommet i en situasjon at de fleste reisende kan identifiseres og deres reisemønster rekonstrueres. Teknologien som skal til for å beskytte informasjonsutveksling best mulig fra å bli observert av utenforstående krever at den reisende må oppgi sin anonymitet og identifisere seg i systemet ved å anskaffe et avansert kundekort. Dette åpner opp for informasjonsmisbruk av andre typer, og vern av kundens personopplysninger avhenger da igjen av at systemet, altså Sporveien, er tilliten verdig.

4.1.6.3 Transaksjonskostnader

For kunden vil en sikring av informasjonsutveksling ved hjelp av smartkort ikke utføre noen øket transaksjonskostnad med at valideringen blir vanskeligere, sett bort i fra at valideringen vil ta noe lenger tid enn om enkle RFID brikker ble brukt. I produktlinjer skaleres systemene til å lese hundrevis av *tags* per sekund. For billettavlesning vil noen få kunne avleses per sekund. Den reisende vil sannsynligvis ikke ha noen problemer med dette. Grunnen er at krypteringsprotokoller og kalkulasjoner tar tid, og prosesseringskraften i smartkort er begrenset. For Sporveien medfører dette at det må benyttes utstyr i alle ledd som er avansert nok til å håndtere krypteringen. Men ifølge designet og opplysningene jeg har fått, er dette noe som uansett er nødvendig for å sikre transaksjonenes økonomiske integritet.

4.1.6.4 Indre sikkerhet

Foruten sikring av den trådløse kommunikasjon mellom de eksterne enheter og det sentrale systemet, vil det også være behov for å etablere sikkerhetsrutiner for adgang og bruk av informasjonen i det sentrale systemet. Ikke minst handler det om hvordan adgang til systeminformasjon og tjenester skal gis for kunder som har kundeavtale f.eks. via Internett.

I utgangspunktet kan man tenke seg å bruke de adgangs- og sikkerhetsmekanismene som

allerede finnes, som kryptering over Internett med SSL over http; *https* protokollen. Kunden kan da for eksempel ha et passord som kan gi han tilgang til sin profil, faktura, reiseoversikt, eller hva slags tjenester Sporveien ønsker å tilby. Det er imidlertid en kjent sak at brukerbestemte passord er relativt lett å avsløre ved automatiske angrep. Sånn sett kan slik informasjon ses på som dårligere sikret enn informasjon som blir utvekslet ved billettvalidatoren. Informasjonen som tilbys kunden på Internett vil sannsynligvis også være av større verdi enn den som kan skaffes ved observasjon av billettkommunikasjonen.

Det finnes måter å begrense dette problemet på, for eksempel ved hjelp av digitale sertifikater og begrenset antall innloggingsforsøk. Slike løsninger er mye brukt i f.eks. nettbanker. Denne slags løsninger øker imidlertid transaksjonskostnadene for kunden, ved at systemet er vanskeligere å forstå, det er mindre rom for å gjøre feil, og det kan kanskje være vanskelig å forstå hvorfor så strenge sikkerhetstiltak er nødvendige. For Sporveiens del vil det medføre større kostnader å administrere sertifikater. Kanskje blir det også større pågang på kundesenteret fra kunder som har vansker med løsningen, og derfor heller velger å handle over disk eller per telefon.

Oppsummert kan man si at ved eksponering av systeminformasjon og kundeinformasjon på Internett gjør systemet seg tilgjengelig for de angrep som vil skje og de sikkerhetshull som finnes og vil oppstå. På den andre side vil økte sikkerhetstiltak oftest også øke transaksjonskostnadene både for brukeren og systemet.

4.2 Personvern i mobiltelefoni

I kap. 4.1.4 så jeg på hvordan tjenesteleverandøren av mobiltelefoni er nødt til å holde på relativ detaljert informasjon om alle abonnenter og deres lokasjon til enhver tid. Svært mange personer i Norge har i dag en mobiltelefon, og vi har altså allerede et system som er i stand til å spore oss hvor vi skulle befinne oss[15]. Vår kontroll over dette systemet er enkel, vi kan velge å skru av telefonen. Dersom vi vil ha telefonen på for å være tilgjengelige eller ha tilgang, må vi også godta at teknologien må vite hvor vi er for å fungere.

4.2.1 "Tradisjonell" mobiltelefoni

I "tradisjonelle" mobiltelefonsystemer som GSM har vi idag en *installed base* av telefoner og tjenester som er adskilt fra generelle datatjenester. Mobiltelefoner er konstruert for taletjenester og "enkle" meldingstjenester (SMS[16]) som passet da teknologien for mobilnett ble utviklet og kommersialisert.

Teknisk er tjenestene pakkesvitsjet som i datanettverk. I motsetning til datanettverk har leverandøren av teletjenester oftest kontroll over hele nettverket og garanterer i de fleste tilfeller nok båndbredde til at vanlige taletjenester fungerer fint. Dette sikrer en høy grad av forutsigbarhet i tjenestetilbud i mobiltelefoni som vi ikke alltid ser i datanettverk.

Ved inngåelse av avtaler om telefoniabonnement blir det som regel opplyst hvordan leverandøren behandler data. Denne politikken annonseres også gjerne gjennom

15 Det er imidlertid ikke alltid man kan vite identitet: Kriminelle bruker i stor utstrekning anonyme kontantkort. http://www.vg.no/pub/vgart.hbs?artid=257822 (sett des 2004)

16 Short Message Service(SMS) tilbyr brukere å sende meldinger på opptil 160 tegn per melding.

leverandørens nettsider. Mye av tilliten til telefontjenester følger også med arven av tillit fra fasttelefonisystemet, og kombinert med pålitelige tjenester har leverandører av mobiltelefoni mer eller mindre fortjent opparbeidet seg en posisjon der de tilbyr et *trusted network.* Brukere stoler på at leverandøren behandler opplysninger om dem ordentlig og ikke deler informasjonen med andre enn det som er lovpålagt, slik som nummeropplysning og eventuelle rettslige kjennelser om overvåking eller utlevering av data.

En jevn tilbakemelding om at mobilleverandøren overvåker vår bruk av telefonen er detaljerte fakturaer, der alle oppringte nummer, tidspunkt og varighet er vist. De fleste av oss tenker nok det er betryggende at vi ut fra dette at kan kontrollere at vi blir belastet et korrekt beløp for mobiltelefonbruk, og at vi kan klage ved uoverenstemmelser. Samtidig er dette et håndfast bevis på at systemet lagrer informasjon om våre digitale bevegelser i telenettet.

4.2.2 Sosiale bekymringer med mobiltelefonbruk

Det finnes egentlig lite arbeid omkring personvernproblemer ved tjenesteleverandørens innsamling av informasjon ved mobiltelefoni. Kontrollmekanismer i forhold til mobilnettverket har vært begrenset til å skru av telefonen, og eventuelt reservere seg mot å bli oppført i nummeropplysningstjenester.

De sosiale sider ved mobiltelefonbruk, spesielt bruken av mobiltelefon på offentlige steder har imidlertid resultert i en del diskusjoner. Blant andre peker Palen og Dourish i [32] på dette i en studie av nye moblitelefonbrukere. De ser potensiale for personvernproblemer, ikke nødvendigvis bare i forhold til brukeren av mobiltelefonen, men også i forhold til andre personer som er tilstede. Det kan være at en person snakker så høyt i mobiltelefonen at alle omkring hører hva vedkommende sier, og føler at de er tilhørere på en privat samtale de ikke burde eller ville høre. Palen og Dourish refererer til sine egne teorier om personvernakser som jeg refererte til i 3.2.2. De mener at spenningen i slike situasjoner pågår i identitetsaksen, mellom *selvet* og *de andre.* Mobilbrukeren tenker kanskje at åpenheten han eller hun viser ved å snakke høyt i mobiltelefonen er akseptabel, eller at det han eller hun snakker om er interessant, selv om andre tilhørere ville foretrekke å slippe å høre på informasjonen. Tilhørere har ofte ingen andre muligheter enn å flytte seg eller be mobilbrukeren flytte seg.

En annen part er personen i den andre enden av samtalen. Denne antar kanskje at dette er en samtale uten publikum og oppfører seg deretter, uvitende om at den han snakker med befinner seg i et offentlig rom. Erfaringen med slike situasjoner er kanskje en av årsakene til at vi gjerne spør en mobilbruker hvor han er når vi innleder en samtale, nettopp for å skjønne den sosial konteksten.

Palen og Dourish mener at vi er i ferd med å utvikle en kombinasjon av to aktivitetsdomener: Opphold i offentlig rom og personlig samtale. Man oppfører seg annerledes når man snakker i telefonen enn når man er fysisk tilstede og snakker med en person.

Det utvikles nye sosiale normer rundt mobiltelefoner. Ved bruk av fasttelefon var tendensen at publikum følte seg påtrengende når man kom inn i et område der en person snakket i telefonen. Nå kan telefoner eksistere på steder der det ikke tidligere var telefoner. Personlige samtaler kan dermed bli en del av det offentlige lyd-rom, og det er telefonbrukeren som bryter personverngrensene.

Hva som er akseptabelt er imidlertid i endring. Palen og Dourish sin undersøkelse [32] viser også at holdningene personer har til offentlig bruk av mobiltelefon varierer med tre forhold: Om de selv er mobiltelefonbrukeren, om de ikke selv har mobiltelefon, men er vitne til at andre bruker mobiltelefon på offentlig sted, eller om de selv har og bruker mobiltelefon og er vitne til at andre gjør det. Ikkebrukere er generelt mer negative til slik offentlig bruk enn brukere selv. Ikkebrukere har også ofte innvendinger om at det ikke er ønskelig/nødvendig å være konstant tilknyttet omverdenen og å være tilgjengelig. Etter kort tids bruk modifiserte mange av brukerne sine uttalelser, og så heller på telefonen som frigjørende, geografisk og sosialt, og mente at mobiltelefonen muliggjorde aktiviteter og samtaler som ellers ikke ville funnet sted.

4.2.3 Nye nettverk og systemer

Software i *"tradisjonelle"* mobiltelefoner har tradisjonelt vært begrenset til standard funksjonalitet som er tilgjengelig i mobilterminalen i salgsøyeblikket, og denne funksjonaliteten er generelt pålitelig. Det er sjelden en mobiltelefon krasjer på grunn av uforutsette hendelser.

Fra en applikasjonsutviklers synsvinkel er denne faste konfigurasjonen med ulike operativsystemer og brukergrensesnitt i mobiltelefoner et problem, fordi man har hatt begrensede muligheter til å bygge generelle applikasjoner på toppen av disse.

Denne situasjonen er i ferd med å endrer seg. Mange telefoner har etterhvert fått muligheten til å kjøre generell programvare, for eksempel basert på Java(J2ME).

Mobiltelefoner skiftes ut i et høyt tempo, men en stor base av telefoner vil likevel være begrenset av tjenestene som initielt tilbys i telefonen. Eventuell integrasjon av nye tjenester for mobiltelefoni må dermed også måtte tilpasses disse tradisjonelle kanalene. Dette ser vi allerede mange eksempler på, ved at mange typer meldingstjenester, avstemminger, kjøp og salg tilpasses en kanal folk har blitt vant til; SMS. Vi ser også en viss utbredelse av talestyrte applikasjoner. Suksess for mobile tjenester er avhengig av lave transaksjonskostnader, altså at tjenestene er så enkle og intuitive at folk vil bruke dem uten å måtte lese bruksanvisninger[17].

Internett og datanettverk har blitt utviklet parallelt med eksisterende mobiltnett. Det har blitt gjort tilpasninger for å tilby datatjenester også gjennom mobiltelefon, både som nettverksleverandør for håndholdte elektroniske assistenter eller bærbare datamaskiner, og for direkte aksess gjennom mobiltelefonen, som f.eks WAP[31]. I vår del av verden har innføringen og ikke minst bruken av datatjenester over mobiltelefon gått sakte. Kanskje er det på grunn av at hastigheten som oppnås med datautveksling over mobiltelefon har vært svært mye saktere enn i det trådbaserte nettverk, og på grunn av mye bedre ytelser som har blitt tilbudt gjennom parallell utvikling av trådløse nettverkssoner. Erfaring og suksess med *IMode* for mobiltelefoner i Japan kan imidlertid tyde på at det er mulig å tilby gode tjenester

17 Aftenposten nettutgave Publisert: 17. oktober 2004-http://www.aftenposten.no/viten/article892082.ece ...Calvet (har) tatt patent på en teknologi som integrerer radiofrekvenser (RFID-teknologi) i SIM-kortet.....(..) Poenget med innovasjon er å forenkle, sier forskningssjef Kristin Braa i Telenor-avdelingen.(..) Målet for Telenors utviklingsarbeid er en løsning som kan brukes uavhengig av telefontyper (..) - Vi fokuserer derfor på SIM-kortet. Det er din eiendom, og kan byttes fra telefon til telefon."

også med lav båndbredde, og det er kanskje andre årsaker til til den sakte utbredelsen i Europa og USA (Barnes[34]). Uansett er det store forventninger til hvordan neste generasjons høyhastighets mobilnettverk som UMTS[18] vil få datanettverk og mobilnettverk til å konvergere.

Denne konvergensen eller integrasjonen av tjenester kan imidlertid medføre problemer i forhold til sikkerhet og personvern. Med WAP og IMode i Japan[34] har brukernes tilgang til tjenester helt eller delvis blitt begrenset av mobilleverandørens utvalg av godkjente. Kanskje vil en mer direkte tilgang til Internett via telefonen gjøre at mobiltelefonen arver en del av Internetts sikkerhets- og personvernproblemer, men nå også kombinert med mobiltelefonens muligheter for lokalisering og allestedsnærværende tilgjengelighet.

4.2.4 Awareness og mobiltelefoni

Gruppebevissthet og samarbeidsapplikasjoner som omtalt i kap. 3.4.1 kan fungere som en regulator for om det passer å kontakte en person på et tidspunkt. Slike systemer er tradisjonelt fraværende innen mobiltelefoni. En bruker er i stand til å tilpasse sin egen profil til konteksten han befinner seg i, for eksempel ved å endre måten samtaler blir varslet på: I stille soner kan dette være med vibrasjon, i støyfulle soner med ekstra høy ringelyd.

Dette er en måte å filtrere innkommende samtaler på. Informasjonen om profilen som er satt er likevel bare tilgjengelig for mottakeren av en samtale, som likevel kan synest at det er forstyrrende å bli oppringt i et opptatt øyeblikk. *Instant Messanger* klienter som omtalt i kap. 3.4.3 har mulighet til å sette status som vises også til den andre parten, og slike klienter er i ferd med å få utbredelse også på mobiltelefoner (Se fotnote 7 s48).

Peter Ljungstrand ser i [33]for seg at slike slike *awareness* systemer blir mer utbredt ettersom tredje generasjon mobiltelefoni utvikles (UMTS). Med en telefon som alltid er tilkoblet kan slik statusinformasjon også vises til personer som vil ta kontakt, og disse får da mulighet til å tilpasse sitt anrop og samtale, for eksempel ved å vente med å gjøre et anrop.

En slik *feedbackloop* for kontekstinformasjon kunne samles inn ved manuelt å sette status, eller telefonen kunne ved hjelp av ulike sensorer beskrive en brukers status og tilgjengelighet uten eksplisitt handling fra brukerens side. *Instant Messenger* systemer har ofte et system der man får status satt til "borte" når det ikke er registrert tastaturaktivitet i en viss tid. Man kan også overstyre innstillingene som blir satt automatisk, og bli satt avkoblet eller opptatt selv om man strengt tatt ikke er det. Ljungstrand ser på innføringen av automatisk statusendring samt muligheten til å overstyre disse som viktig for at et slikt system skulle kunne fungere.

Nye *friends finder* tjenester referert til i fotnote 7 s.48, samt andre tjenester[19], tilbyr også muligheter til å få tilgang til den geografiske lokasjonsinformasjonen som mobilselskapene sitter med. Man kan registrere seg og invitere sine venner og kjente til å bli tilgjengelig for lokasjonssøk, slik at man kan lokalisere hverandre. Tjenestene tilbys både som "alltid online" tjenester som GPRS[31] og via "tradisjonelle" SMS tjenester. Brukeren er gitt en viss kontroll i tjenesten ved at man eksplisitt må melde seg inn i tjenesten, og ved at man eksplisitt må tillate hver enkelt venn å få tilgang til lokasjonsinformasjon. Dessuten kan man midlertidig

18 UMTS: Universal Mobile Telecommunications Service

19 En versjon i USA:http://www.attwireless.com/personal/features/organization/findfriends.jhtml (sett des.2004)

bli usynlig for søk fra andre personer i tjenesten, og man får en tilbakemelding dersom noen har gjort et lokaliseringssøk. Andre personer har tilgang til å gjøre søk gjennom flere kanaler, både via Internett og mobiltelefonen.

Denne slags tjenester er noe nytt i forhold til et av forholdene man tidligere har basert tilliten til mobilleverandøren på; at identifiserbar informasjon bare finnes i systemet for å tilby telefonitjenesten. Leverandøren eksponerer at man innehar identitets- og lokasjonsinformasjon og tilbyr altså disse data utenfor det systemet som anses for *trusted.*

Det finnes flere typiske tjenester fra *awareness* miljøet der informasjon om aktivitet på et sted blir gjort tilgjengelig andre steder, eksempelvis muligheter for ta bilder og video og dele disse. Til en viss grad har man også adoptert *awareness* miljøets *kontroll og feedback* mekanismer. I forhold til de arbeidsoppgavene som deles gjennom arbeidsbaserte *awareness* systemer er informasjon som utveksles over mobiltelefon i større grad privat og uformell, også når telefonen brukes i arbeidssammenheng. Uten å ta høyde for at informasjonen nå potensielt befinner seg i andre sosiale rom enn der disse konseptene ble utviklet , fremheves helst bare de sosiale fordelene med tjenestene.

For å kunne tilby *awareness*-tjenester til brukeren selv, og eventuelt andre brukere, må mobilnettverket samle inn og holde på statusinformasjon fra mobilterminalene. Hva som skjer med denne informasjonen inne i systemet er som regel i liten grad i fokus for brukernes oppmerksomhet.

4.2.5 Mobiltelefoni og Sporveiens system

Mobilnettverk har en del til felles med det som er Sporveiens billettsystem ønsker å få til.

4.2.5.1 Likheter

Teleleverandørene framstår som aktører som har tillit hos kundene i det å levere åpne telefonitjenester som alle kan bruke til kommunikasjon. Tilliten har de delvis arvet fra lang tids erfaring som leverandør av fasttelefoni, og god databehandling i et lukket system.

Sporveien har tillit hos kundene for at de kan levere åpne transporttjenester for fysisk transport. Nå vil de gjerne ha med seg litt av denne tilliten fra kunden over til at de også kan håndtere en datainnsamlingstjeneste på lik linje med med mobilselskapene: Et åpent system alle kan bruke, men der databehandlingen er strengt regulert i et nettverk de selv kontrollerer.

For begge systemer er datainnsamlingen nødvendig for å sikre transaksjonsintegritet, altså at kundene belastes riktig for tjenesten, og at ingen misbruker systemet ved forfalskninger. Dermed er det behov for å holde transaksjonsinformasjon over tid, som kan brukes til å rekonstruere en persons handlinger.

Begge systemer legger også omtrent det samme nivå på sikkerhetsløsninger, ved at begge ser for seg å bruke smartkortløsninger for å beskytte informasjonen hos kunden, og begge vil ha et distribuert, men strengt adgangskontrollert system.

For kunden er det i begge systemer så godt som ukjent hvordan innsamlede data brukes og potensielt deles. Kundene tilbys bare en svært begrenset mulighet til å få kontroll og

tilbakemelding i forhold til datainnsamlingen i systemet.

Det er behov for lave transaksjonskostnader for kunden, systemene må være enkle å bruke. Begge systemene tilbyr i utgangspunktet tjenester som er svært enkle å forstå for brukeren (tale- og meldingstjenester vs. billettbetaling).

4.2.5.2 Forskjeller

Det er likevel en del forskjeller, spesielt ettersom tredje generasjons mobiltelefoni utvikles. For mobilsystemer er tendensen at det adopteres en del applikasjoner fra *awareness* systemer. Mobilterminalene blir mer avanserte, og gir mulighet for en større grad av tilbakemelding og kontroll, spesielt i forhold til sosiale relasjoner. Kundene er sannsynligvis interessert i en slik kontroll og tilbakemelding i sine sosiale forhold, selv om det skulle øke vanskelighetsnivået og transaksjonskostnadene for dem.

Sporveiens system er ikke beregnet for sosiale relasjoner, det er kun beregnet for å ha et forhold til billettsystemet. For Sporveien vil det derfor være et poeng å holde brukerterminalene, altså billetter og smartkort, enkle å bruke for brukerne. Dette gjelder også ved eventuell innbygging av kundekortinformasjon i en mobiltelefons SIM kort.

Naturligvis er også rekkevidden i transmisjonen og utbredelsen av det distribuerte nettverket mye større for mobilnettverk. Det vil sannsynligvis bli behov for å benytte mobilnettverk som nettverksleverandør til Sporveiens distribuerte system, for eksempel for billettvalidatorer utenfor tettbygde strøk.

I forhold til Palens og Dourish sine identifikasjonakser er systemene også forskjellige. I mobiltelefonisystemer blir alle personer unikt identifisert. I billettsystemet er det intensjonen at det er *billetten* som skal unikt identifiseres, og denne informasjonen skal i prinsippet holdes adskilt fra kunden.

4.2.6 Oppsummering av Mobiltelefoni og personvern

Mobiltelefoni er i stor grad et sosialt middel for tilgjengelighet, og vil sannsynligvis bli det i enda større grad ved innføring av neste generasjons mobiltelefoni. Det er lite fokus på hvordan data behandles i systemet, og det meste av forskning omkring personvern går på sosial bruk. Brukere har grunnleggende tillit til systemet, selv om dette kan endre seg når mange systemer integreres og kan gi grunnlag for flere feil og brudd på personvern. De fleste mobilleverandører formidler sin personvernpolitikk gjennom abonnementsavtaler og eventuell annen annonsering, men storparten av tilliten er bygd på lang tids leveranse av stabile tjenester.

I forhold til billettsystemer er det mange likhetstrekk mellom mobiltelefoni og hvordan Sporveien ønsker at deres system skal bli tatt imot og brukt. De viktigste er kanskje likheten i kravene de stiller til transaksjonsintegritet, og behovet for å blir ansett som et *trusted network.*

4.3 Personvern i Internett

4.3.1 Sikkerhet, transaksjonskostnader og kontroll

Internetts åpne systemmodell, der heterogene datasystemer er i stand til å kommunisere gjennom etableringen av felles protokoller, er en av Internetts store fordeler, men også et av de store problemene. Dette har resultert i at sikkerhetsaspekter har blitt ulikt prioritert. Mye arbeid har vært lagt ned for å bedre sikkerheten i kommunikasjonen, da spesielt innen autentisering og etablering som sikre kanaler for kommunikasjon, slik som *https* og andre sikkerhetsmetoder referert til i kap. 4.1.

Gjennom utviklingen av datamaskiner de siste femti år har utviklere og ekspertbrukere hatt fokus på *kontroll.* Man har visst hvordan systemet fungerer, og har kontroll med hva som skjer. Med utviklingen og den enorme utbredelsen har dette endret seg. Man har fått millioner av brukere som er interessert i bare å *bruke* systemet, ikke forstå det. Noen aktører (f.eks Microsoft) forstod dette raskt, og laget systemer som var enkle å bruke, og ikke la noen særlige hindringer på veien for bruk ut på Internett. Dette medførte også at det for mennesker med ikke altfor hederlige hensikter var ganske enkelt å komme inn på brukernes maskiner via nettverket. Dette har medført at man har måttet legge ned mye arbeid i å identifisere og stenge igjen sikkerhetshuller i etterkant, og heller gi brukerne kontrollen til å åpne opp tjenestene igjen dersom det skulle være behov for det.

Andre aktører (som Unix/Linux) har hatt en mer passiv innstilling til å legge til rette for tjenester, ved at brukere hele tiden har måttet hatt nok innsikt til aktivt å kontrollere hvilke tjenester man vil bruke. Heller ikke disse har sluppet unna sikkerhetsproblemer, men i mye større grad enn den første gruppen.

Internett var jo i begynnelsen egentlig bare et meldingsforum, og fungerer fremdeles slik i mange sammenhenger. Det at informasjonen er offentlig tilgjengelig har ført til at svært mange andre slags applikasjoner har blitt oppfunnet. Og i Internett, som mange andre steder, har man funnet ut av hva slags sikkerhets- og personvernproblemer som må utbedres etterhvert. I noen tilfeller har sikkerheten blitt bedret gjennom forbedringer i software og protokoller, mens i svært mange situasjoner er det opp til brukeren selv å finne ut av hvordan han kan holde kontroll med sin egen sikkerhet og sine egne personlige opplysninger. Dette er ikke alltid så enkelt, og kan medføre store transaksjonskostnader for en vanlig bruker.

Man har kommet ganske langt når det gjelder å sikre førsthåndsinformasjon fra observasjon og uautorisert tilgang, selv om angrepsforsøk, datainnbrudd og utnyttelse av sikkerhetshuller skjer hele tiden. Så lenge man sørger for å holde software og antivirusprogramvare rimelig oppdatert (altså en transaksjonskostnad i seg selv) er man noenlunde sikret mot generelle automatiske angrep og trusler. Men dersom en innsiktsfull person virkelig ønsker å bryte seg inn kan han nok uansett klare det.

4.3.2 Digitale spor

Likevel legger vi fra oss utallige digitale spor ved å benytte Internett. IP-adresser er som regel synlige og kan knyttes til et land og vanligvis identifiseres som en abonnent hos en internett-tilbyder. Utlevering av slik informasjon er imidlertid bare vanlig i tilfeller med rettslig

kjennelse.

4.3.2.1 Cookies

I mange tilfeller legger websider igjen *Cookies* eller informasjonskapsler på brukerens maskin. Disse brukes til å personalisere informasjon og lagre innstillinger i brukerens nettleser, og leses og skrives når en bruker besøker dette nettstedet. *Cookies* kan brukes til å samle inn informasjon om brukeren og hans aktiviteter og sende denne informasjonen tilbake til utstederen av informasjonskapselen.

De fleste nettlesere har relativt strenge standardinnstillinger på hva slags *cookies* de skal akseptere, for eksempel at tredjepart *cookies* ikke kan lagres, det vil for eksempel si *cookies* som tilhører reklamebannere for andre bedrifter enn domenet nettsiden tilhører. Man gir også ofte muligheter til å justere disse begrensningene i forhold til *cookies* og i forhold til hva slags aktivt innhold som skal kjøres automatisk, noe som kan bedre sikkerheten for virus og andre uønskede programmer.

4.3.2.2 Datamining

Vi legger også fra oss mange andre spor som kan gi grunnlag for *datamining,* ikke minst med opplysninger som vi publiserer som på hjemmesider eller i jobbsammenheng, for eksempel kontaktinformasjon med epostadresser.

Ikke minst gir vi også ofte frivillig fra oss informasjon til nettsteder for å kunne benytte deres tjenester på Internett. Både uidentifiserbar og identifiserbar informasjon på Internett befinner seg i det offentlige rom, så lenge kommunikasjonen og informasjonen ikke aktivt sikres.

Problemene rundt annenhåndsinformasjon som blir delt med tredjeparter, automatisk innsamling og misbruk av informasjon som er publisert på Internett, samt at ikke-identifiserbare data blir identifisert gjennom *datamining*-teknikker er til stede i fullt monn. Dette er for eksempel en av årsakene til den store utbredelsen av uønsket epost (*spam)*.

4.3.3 Utveksling av personvernpolitikk

Nettsteder tilbyr i mange tilfeller en beskrivelse av sine rutiner for behandling av informasjonen de samler inn. Av og til inkluderes det egne punkt om deres bruk av *Cookies*. Lenker til slike *Privacy Policies* finnes ofte i en nettsides nedre del (*footer)*¸ men det hender at man må aktivt lete etter dem, og de inneholder ofte mye informasjon i et juridisk språk som kan være vanskelig å forstå. Det er gjerne også forbehold om at avtalen kan endres når som helst. Ved å bruke en nettside aksepterer man implisitt den databehandlingspolitikken som er uttrykt i disse *Privacy Policies.*

Ideen med å publisere en *privacy policy* er basert på regler for datainnsamling, som *fair information practice og The Directive.* Disse krever at personer skal informeres om at datainnsamling pågår, at innsamlingen skal være tilpasset formålet, og at brukeren eksplisitt må gi sitt samtykke for at identifiserbare data skal kunne samles inn.

Da må jo datainnsamlere på forhånd opplyse om hva de har tenkt å bruke data til, og hvem de har tenkt å dele den med, og gi brukeren muligheter til samtykke. Man bør så selvsagt

ikke misbruke tilliten ved å bruke eller dele data annerledes enn avtalt.

Implisitt godtagelse av *privacy policies* er ingen god løsning for å akseptere datainnsamling.

For å forsøke å bøte på noen av disse problemene har en arbeidsgruppe ved W3C kommet fram til en standard for eksplisitt utveksling av personvernpolitikk mellom brukere og nettsteder: P3P1.0 [14]. Arbeidsgruppen i W3C består av representanter fra IT-industrien, personverngrupper og universiteter.

4.3.4 P3P - The Platform for Privacy Preferences Project

P3P[14] har definert en standard for deling av personvern politikk, samt et språk APPEL[15] (*A P3P Preference Exchange Language*) som brukeragenter (for eksempel nettlesere) kan bruke for å definere hvilke politikker brukeren godtar. P3P er hovedsaklig tenkt for *clickstream* informasjon, altså informasjon som utveksles over Internett. Flere har gjort arbeid for også å kunne bruke denne for andre domener.

Ideen bak P3Ps spesifikasjon er å etablere et standard "harmonisert" vokabular og format for å utveksle krav og preferanser som er maskinlesbare og som dermed kan brukes for å kommunisere og forhandle kontrakter. Datanavn og typene som brukes er koordinert, for om mulig å korrespondere med andre innsamlingsformat som finnes, f.eks VCARD[45]. Opprinnelig er P3P ment for Internett og fungerer ved at man på *webservere* kan definere hva slags politikk organisasjonen har for bruk av innsamlede data. Disse definisjonene er lagret på et velkjent sted, og brukerens agent eller nettleser vil kunne lese disse og sammenligne den med brukerens personverninnstillinger, definert i et tilsvarende språk, f.eks APPEL , også spesifisert av W3C. Nettleseren kan dermed automatisk avvise krav fra webserveren som brukeren ikke er villig til å akseptere. Eventuelt kan nettleseren konfrontere brukeren med et valg om han vil akseptere den politikken organisasjonen forteller at den har.

P3P deklarerer politikk positivt. Det innebærer at deklarasjonen inneholder informasjon om hva bedriften gjør med innsamlede data, og ikke hva de ikke gjør. På den måten blir bedriften ansvarlig for all håndtering de ikke har meldt fra om ved innsamlingen.

P3P har brukt XML som sitt kodingformat, og definert et hierarkisk system der man blant annet kan beskrive hva slags data som blir samlet inn, hvorfor man gjør innsamlingen, hvem som tar imot data, hvordan data videre kan bli spredd, og hvordan en kunde eventuelt kan klage. Det er også gjort plass til videreutvikling av protokollen. Som hovedregel gis alle mulige alternativ på en gang i en avtale, det er dermed ikke rom for videre forhandling, men brukeren bør i prinsippet ha ulike valg.

Disse valgene kan gå på om brukeren vil godta innsamling av data i de oppgitte kategorier, la data bli brukt til de oppgitte formål og at deling av informasjon skal kunne skje med de oppgitte parter. Brukeren skal da kunne velge alternative *policies* , eller man kan definere *opt-in* eller *opt-out* (*optional* -valgfritt)attributter og gi en forklaring på hvordan brukeren må henvende seg til nettstedet for eksplisitt å få benytte seg av sine valgfrie muligheter på de oppgitte områdene.

For å forsikre brukeren om at man virkelig overholder politikken oppnevner man ofte en *trusted* tredjepart som etterser dette. Brukeren kan kontakte tredjepart for å få dette bekreftet.

Flere detaljer om P3P standarden finnes i tabell 3 på side 75.

4.3.4.1 APPEL - A P3P Preference Exchange Language

APPEL[15] er et komplement til P3P standarden, ved at den spesifiserer et språk til å beskrive samlinger av preferanser for politikk mellom agenter som utveksler P3P personvernpolitikk.

En bruker vil uttrykke sine preferanser ved å sette preferanse-regler, eller såkalte *rulesets*. Dette regelsettet vil brukerens agent bruke som grunnlag for å gjøre automatiske eller halv-automatiske avgjørelser i forhold til politikken tjenestetilbyderne har.

Slik automatisk databehandling blir mulig ved å uttrykke både regelsettene og politikken i maskinlesbart språk (XML) . Å skrive disse *policies* har imidlertid en viss terskel, derfor finnes det også verktøy både for tjenestetilbyder og bruker for å generere slike dokumenter.

En brukeragent implementerer APPEL ved å ha en regel-evaluator som evaluerer *policy* mot brukerens preferanser. Resultatet av en evaluering kan ha tre ulike utfall:

request- Tjenestetilbyder ser ut til å oppfylle brukers krav; den ønskede informasjon frigjøres.
limited - Tjenestetilbyder oppfyller delvis brukers krav; noe informasjon kan frigjøres.
block - Tjenestetilbyder oppfyller ikke brukers krav; ingen informasjon frigjøres.

I tillegg kan man spesifisere om bruker skal få en notifikasjon/*prompt* ved mulige utfall.

Ideen er altså at man kan sette opp regler, samlet i *rulesets*. Man kan definere regler basert på hvilke data som samles inn, dvs kategorien, formålet (*purpose*) for innsamlingen, hvem tjenestetilbyder har tenkt å dele data med (*recipient*), samt spesialregler for enkelte domener. Man kan også bygge regler av kombinasjoner av disse.

4.3.4.2 Eksempel på P3P policy og APPEL rulset

En P3P policy kan gis på ulike måter. Et eksempel på en P3P policy på standardformen vises i venstre kolonne i tabell 2 på side 74.

Det finnes også en kortform eller *Compact policy* som kan brukes for å formidle politikk i miljøer der båndbredden er lav. Dette er en del av P3P definisjonen .

Man mister da noe informasjon, men de viktigste delene om hvilke data som samles inn og til hvilket formål data blir samlet inn er med. Dette kan være interessant med tanke på å formidle *policies* i systemer med lite minne eller prosesseringskraft. Politikken i tabell 2 ser slik ut i kortform:

”NON DSP ADM DEV PSD IVD OUR IND STP PHY PRE NAV UNI“

Et eksempel på en APPEL regel finnes i høyre kolonne i tabell 2 på side 74. Dette *ruleset* blokkerer deling av informasjon med alle tjenester som sender informasjon videre til tredjeparter. Videre kan man se at det er mulig å definere logiske regler; *connective*=“*or*“ betyr at hvilken som helst av kategoriene for identifiserbare data som er nevnt i kombinasjon med hvilken som helst type deling med tredjepart, vil få regelen til å slå til, og videre informasjonsdeling til å blokkeres.

P3P Policy	Appel rulset
<POLICY name="sample“ discuri="http://www.example.com/cookiepolicy.html" opturi="http://www.example.com/opt.html"> <ENTITY> <DATA-GROUP> <DATA ref="#business.name">Example, Corp.</DATA> <DATA ref="#business.contact- info.online.email">privacy@example.com</DATA> </DATA-GROUP> </ENTITY> <ACCESS><none/></ACCESS> <DISPUTES-GROUP> <DISPUTES resolution-type="service" service="http://www.example.com/privacy.html" short-description="Please contact our customer service desk with privacy concerns by emailing privacy@example.com"/> </DISPUTES-GROUP> <STATEMENT> <PURPOSE><admin/><develop/><pseudo-decision/></PURPOSE> <RECIPIENT><ours/></RECIPIENT> <RETENTION><indefinitely/></RETENTION> <DATA-GROUP> <DATA ref="#dynamic.cookies"> <CATEGORIES><preference/><navigation/></CATEGORIES> </DATA> </DATA-GROUP> </STATEMENT> <STATEMENT> <PURPOSE><individual-decision required="opt-out"/></PURPOSE> <RECIPIENT><ours/></RECIPIENT> <RETENTION><stated-purpose/></RETENTION> <DATA-GROUP> <DATA ref="#user.name.given"/> <DATA ref="#dynamic.cookies"> <CATEGORIES><preference/><uniqueid/></CATEGORIES> </DATA> </DATA-GROUP> </STATEMENT> </POLICY>	<appel:RULE behavior="block“ description="Service collects personal data for 3rd parties"> <p3p:POLICY> <p3p:STATEMENT> <p3p:DATA-GROUP> <p3p:DATA> <p3p:CATEGORIES appel:connective="or"> <p3p:physical/> <p3p:demographic/> <p3p:uniqueid/> </p3p:CATEGORIES> </p3p:DATA> </p3p:DATA-GROUP> <p3p:RECIPIENT appel:connective="or"> <p3p:same/> <p3p:other-recipient/> <p3p:public/> <p3p:delivery/> <p3p:unrelated/> </p3p:RECIPIENT> </p3p:STATEMENT> </p3p:POLICY> </appel:RULE>

Tabell 2: En P3P Policy og et APPEL Ruleset. Eksempler fra P3P [16] og APPEL[15] spesifikasjonene.

P3P Policy Element	Beskrivelse
Policies Policy	Flere *Policies* kan gis samtidig. På overordnet nivå gis informasjon som gjelder for hele politikken. En *policy* er en komplett personvernpolitikk.
Disclosure Uri:	Hvilke *uri* som dekkes av denne policy. Ulike *policies* kan angis for ulike deler av en *website*.
Entity	Kontaktinformasjon for bedriften, organisasjonen eller eieren av en webside. Data er tagget i standard format, eksempelvis som vCard: <DATA ref="#business.name"/>Bedriftsnavn</DATA>
Access	I hvilken grad personer kan finne ut hvilke data en entitet holder om dem, og om de har tilgang til å få endret på eller slettet disse. 6 ulike nivåer definert som subelementer, fra ingen til full tilgang.
Disputes	Hvordan eventuelle konflikter med tjenestetilbyderen kan adresseres. Inkluderer også et *Remedies* subelement for hvordan tjenestetilbyderen vil gjøre opp for brudd på sine *policies*: Det kan inkludere å rette opp feilen, betale penger, eller la en domstol avgjøre.
Statement	*Statements* beskriver praksis for behandling av data av en spesiell type.
Data	Definerer hva slags data som samles inn. 17 kategorier (*Category*) av data er definert, samt mange flere spesifikke dataelementer, harmonisert med f.eks vCard[45] standarden. Datakategorier er listet under: <physical/> Fysisk kontaktinformasjon <online/> Online kontaktinformasjon <uniqueid/> Unike Identifikatorer <purchase/> Kjøpsinformasjon <financial/> Finansinformasjon <computer/> Computer informasjon <navigation/> Navigasjon og *Click-stream* Data <interactive/> Interaktive data <demographic/ Demografiske og Sosioøkonomiske Data <content/> innhold <state/> Statushåndteringsmekanismer <political/> Politisk informasjon <health/> helseinformasjon <preference/> Preferansedata <location/> lokasjonsdata <government/> Identifikatorer fra myndighetene <other-category> Andre data
Purpose	Predefinerte formål for hvordan innsamlede data er tenkt brukt. 11 ulike formål er definert, i tillegg til en samlegruppe *other-purposes*. Formål varierer fra statistisk bruk av informasjon, individanalyse, kontakt av brukeren for markedsføring, telefonsalg, samt bare for å gjennomføre gjeldende transaksjon. Minst et formål må oppgis. Brukere kan gis valg ved å definere *opt-in* eller *opt-out* attributter på noen eller alle formål. Fremgangsmåte for dette må da foreligge *policy* elementet. <current/> Fullføring og støtte av en aktivitet, som å svare på et web-søk, sende en epost, eller fullføre en ordre <admin/> Web/system administrasjon <tailoring/>,<pseudo-analysis/>,<pseudo-decision/>,<individual-analysis/>,<individual-decision/> Ulike grader av individualisering av tjenesten, fra analyse av brukerens bevegelser, til beslutninger på basis av disse pseudonymiserte eller individualiserte data. <develop/> Forskning og utvikling <contact/>,<telemarketing/> Å kunne kontakte brukeren og tilby produkter og tjenester <historical/> Informasjonen kan oppbevares av historiske årsaker og for analyse. <other-purpose/> Annen bruk, som må beskrives med menneskelesbar forklaring.
Recipient	Definerer om og under hvilke omstendigheter data kan bli delt med andre parter. Kan også definere muligheter for brukeren til å reservere seg mot at data blir delt med disse parter ved å definere opt-in og opt-out muligheter. Mottakere er andre juridiske entiteter. Seks ulike mottakergrupper er definert. <ours/> Eniteten policy gjelder for eller deres agenter. <delivery/> Leverandør som kan ha annen datapraksis, og bruke data annerledes. <same/> Andre entiteter som følger samme praksis. <other-recipient/> Annen entitet som er ansvarlig ovenfor denne, men kan komme til å bruke data annerledes. <unrelated/> Annen entitet der tjenestetilbyder ikke kjenner datapraksis <public/> Data kan bli delt via offentlige kanaler
Retention	Hvorvidt entiteten har praksis for periodisk å slette data som er samlet inn, altså hvor lenge data blir lagret. Fem ulike nivåer er spesifisert, fra ingen lagring, via oppgitt politikk for å oppfylle de formål som er gitt, myndighets- eller lovpålagte krav, eller bedriftens egne rutiner, til uendelig.
Consequence	Menneskelesbar forklaring på hvordan og hvorfor entiteten behandler data som de gjør. Evt. grunner til å akseptere datainnsamling man ellers ikke ville godta.

Tabell 3: Detaljer i P3P1.0 standarden

4.3.4.3 P3P utbredelse: En brukeragent: AT&T Privacy Bird

P3P ble standardisert som en anbefaling fra W3C i april 2002 . Utbredelsen av bedrifter og organisasjoner som bruker P3P har ikke akkurat tatt av, men noen av de store har tilpasset seg standarden og inkludert politikk på sine sider, for eksempel Microsoft, IBM og AT&T.

Som et eksempel på en brukeragent som kontrollerer personvernpolitikk har AT&T implementert en prototype som baserer seg på bruk av P3P policies og APPEL brukerpreferanser. I en undersøkelse gjort av Cranor [18] i 2002 har de diskutert sine erfaringer med bruk av agenten. Agenten deres, en såkalt *Privacy bird* fungerer som en *plugin* til nettleseren Internet Explorer, og evaluerer en websides politikk mot brukerens innstillinger. En del ferdige innstillinger, definert i APPEL, leveres i prototypen, og kan konfigureres i verktøyet.

Verktøyet installerer seg på vinduslinjen og viser ulike statussymboler avhengig om nettsiden har en politikk, og om denne oppfyller preferansene.

Illustrasjon 3: AT&T Privacy Bird sier fra om en nettside har en P3P politikk og om disse oppfyller mine preferanser. Illustrasjon fra www.privacybird.com.

Forskerne bak *Privacy bird* konstaterte at lite arbeid er gjort for å finne ut hvordan mennesker forholder seg til personvern-software, og enda mindre på hvordan man skal få kunnskap om personvern ut til massene. Hovedresultatet av undersøkelsen AT&T gjorde var at deres *Privacy bird* var med på å lære opp Internettbrukere i personvern. Mange av deltakerene i undersøkelsen oppgav at de leste *privacy statements* mye oftere enn før dersom de skulle gi fra seg informasjon, uavhengig av om nettsidene implementerte P3P eller ei.

4.3.5 Platform for Enterprise Privacy Practices

IBM er en av aktørene som lenge har satset på på forskning og utvikling innenfor personvernsystemer. De har støttet og videreutviklet systemer basert på P3P standarden, spesielt med tanke på å forvalte den tilliten en tjenestetilbyder har opprettet med sine kunder ved inngåelse av personvernkontrakter, for eksempel gjennom P3P politikk. IBM har en egen forskingsavdeling som er dedikert til personvernsystemer .

Karjoth et al. beskriver i [19] IBMs *Platform for Enterprise Privacy Practices*, også kalt E-P3P. Dette er et rammeverk og et språk for personvernpolitikk. Det er en utvidelse av P3P sitt arbeid, men er fokusert mot intern automatisk forvaltning av politikk og forretningsregler, mer enn å uttrykke dette til en brukeragent. Det innebærer at de ser for seg å uttrykke personvernpolitikk på samme måte som før, enten gjennom skrevne avtaler eller ved en P3P policy. De pålegger likevel seg selv å garantere at data blir brukt som avtalt. Bakgrunnen for dette er at man potensielt kan miste markedsandeler dersom man ikke kan vise til at man behandler informasjon som avtalt. Dette blir spesielt viktig i store bedrifter som kanskje ikke vet nøyaktig hvilken eller hvordan informasjon blir lagret, ei heller hvorvidt kunder har gitt den nødvendige samtykke til bruk av data. E-P3P er altså designet for å bedre på denne situasjonen.

I artikkelen skriver de også at datasubjekter må tilbys maksimalt innsyn og kontroll over bruken og innhold i sine data, samt at en tredjepart bør overvåke at data blir oppbevart og behandlet på en riktig måte. De ser også på sikkerhet som en forutsetning for personvern,

men holder dette adskilt fra personverndiskusjonen.

Slik de uttrykker det, reflekterer en *Enterprise Privacy* politikk hvordan personlig identifiserbar informasjon (PII), kan flyte og bli brukt i en bedrift. Derfor er det nødvendig å gjøre en analyse av bedriften for å finne ut hvem som bruker innsamlede data, hvilke data de bruker, og hvilke operasjoner de gjør med disse data, altså hvordan de blir brukt. Dette er koordinert mot P3Ps mottakere, datagrupper og formål.

Videre defineres ulike roller innenfor et *Enterprise Privacy* system. **Datasubjekt** er den som data omhandler, for eksempel kunder, ansatte eller andre bedrifter. **Databrukere** utfører **oppgaver** ved hjelp av **applikasjoner**. Hvilke oppgaver som er tillatt, det vil si hvilke operasjoner som er tillatt gjort, med hvilket formål, og med hvilken databruker på hvilke typer datasubjekter defineres av en ***Privacy* Offiser**. *Privacy* offiseren er spesielt viktig ved innføringen av et slikt personvernsystem, fordi alle data som tidligere applikasjoner bruker må settes inn i dette systemet.

Denne rollen er skilt fra **Sikkerhetsoffiser**, som er ansvarlig for tilgangspolitikken, det vil si hvilke fysiske personer som blir tildelt ulike roller som databrukere i bedriften.

E-P3P forholder seg også til paradigmen om å lagre metadata, i dette tilfelle *privacy* politikk sammen med innsamlede data. Denne praksis kaller de *sticky policy* paradigmen. Dette innebærer å behandle data på en per-person og ned til en per-record basis. De valgene for *opt-in* og *opt-out* samt den politikken som gjaldt i det brukeren delte sin personlige informasjon med bedriften skal henge ved data så lenge de består, også om de blir delt med andre bedrifter.

Hver eneste datatuppel kan dermed inneholde betingelser som må evalueres ved forespørsler om data og når disse tas i bruk. Standard betingelser kan settes på grunnlag av formål, databruker og operasjoner, som må være en del av enhver forespørsel. I tillegg kan det være betingelser som ligger i data eller i gjeldende kontekst for om data kan brukes. Det kan være at eksplisitt samtykke må innhentes fra kunden, for eksempel at kunden må være over 18 år for at informasjonen skal kunne brukes til et gitt formål.

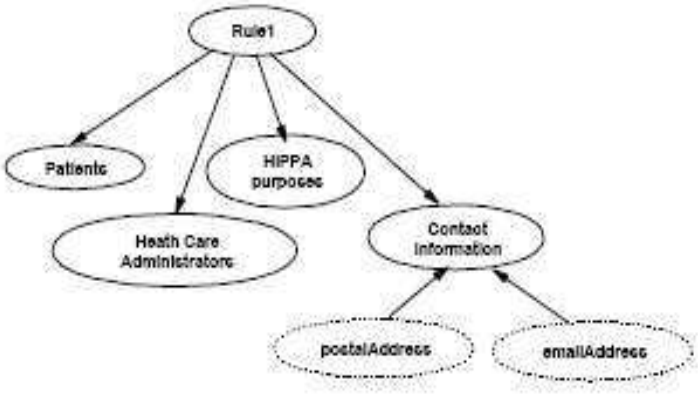
E-P3P har altså sitt eget språk, lignende P3P syntaksen, med tilleggselementer for å uttrykke den ekstra funksjonalitet som de tilbyr.

Alle applikasjoner som skal bruke data i bedriften må dermed innhente tillatelse til dette gjennom E-P3P maskinen. I noen tilfeller kan en operasjon autoriseres uten forbehold, i andre kan en operasjon bli autorisert, men med forpliktelser til den som mottar data. Evalueringsmotoren vil da lagre dette som en forpliktelse som vil bli utført når et sett betingelser er oppfylt. Dette kan for eksempel være at data kan beholdes i en uke uten at et datasubjekt har samtykket i bruk av disse. Etter dette blir de slettet, dersom kanselleringsbetingelsen for regelen ikke er oppfylt, altså at man har godtatt bruk av data.

4.3.5.1 Individualisert personvernbasert tilgangskontroll

Bohrer et.al., går i [20] lengre i å dekomponere *policies* mot de enkelte dataelementer og ulike brukere og deres roller. Dette er også et IBM prosjekt. Deres hovedanliggende er at mulighetene for *opt-in* og *opt-out* av personvernpolitkk som P3P og E-P3P gir muligheter til,

er en altfor dårlig modell for å gi brukere kontroll over sine data. De argumenterer for en modell med individuell personvernpolitikk istedet for eller i tillegg til at tjenestetilbyder definerer disse på tvers av hele sin bedrift.



Illustrasjon 4: Personvernregler lages ved at logiske grupperinger av data, brukere og formål dekomponeres. Illustrasjon fra Bohrer [20].

De vil oppnå dette ved å bygge opp regler slik at hver del av en regel kan deles av mange regler. For å få til dette bruker de designprinsipper fra objektorientert design, nærmere bestemt *Composite Design pattern* (Gamma et. al. [46]). På den måten kan man aggregere individuelle objekter eller grupperinger av objekter som igjen blir mål for en regel, eller en større gruppe av regler. Dette pattern bruker de så både for databrukere, datasubjekter og selve data. Se figur 4 for en illustrasjon.

Databrukere kan for eksempel ordnes som familie, ansatte, pålitelig bedriftforbindelse (bank?),eller andre forbindelser. Data kan ordnes som for eksempel medisinsk, finansiell, kontakt, kjøpsvaner, som i P3Ps data kategorier, eller på andre og mer eller mindre subjektive måter. For eksempel som svært sensitiv, noe sensitiv, kan frigjøres om påkrevet, offentlig. Ut fra slike logiske grupperinger kan man så definere hvilke personvernregler som skal gjelde.

Logiske grupperinger må selvsagt kobles til konkrete dataelementer, og denne dekomponeringen kan da komme til å granulere personvern enda mer drastisk enn å tillate politikk å være knyttet til en per person eller per *record*, som Karjoth et.al. [19]. gjorde.

Modellen tillater også datasubjekter å være uidentifiserbare, på den måten at en "*personna*" kan bestå av distinkte dataelementer, eller dataelementer som også tilhører andre. Et individ kan dermed ha mange brukeridentiteter, der ikke alle er identifiserbare som personen.

Bohrer et.al. mener at modellen de presenterer kan komme i tillegg til adgangskontroll, men den kan også erstatte slike systemer. De ser på sin modell som et supersett av tilgangskontroll. Tilgangskontroll kan implementeres i modellen ved at alle slags data, ikke bare de som er personlige data, blir definert i *dataview*. Dermed kan man lage regler som gjelder for alle eller ingen, og uautorisert aksess kan dermed ikke oppnås. Hele modellen baserer seg på tilgang til dynamiske views basert på dynamiske roller eller dynamiske formål, og dette kan også fungere som tilgangskontroll, mener de.

I det ene ytterpunkt kan individuelle brukere altså sette opp egne brukergrupper, hierarkier av dataressurser og formål, og dermed lage fullstendig individualiserte kontrakter. På den andre side kan bedrifter tilby en eneste personvernpolitikk, og datasubjekter kan *opt-in* ved å bli lagt til i data-subjekt listen for denne *policy*. I mellom disse to underpunkt har vi situasjoner der ulike logiske grupperinger av dataressurser, brukergrupper og formål kan deles og kontrolleres av ulike parter.

4.3.6 P3P kontrakter og personvernkrav

Konseptene med å inngå avtaler har hatt et visst innpass i miljøer innen utvikling av Internett og distribuerte bedriftsnettverk, noe P3P standarden fra W3C og eksempelvis IBMs systemer viser. For Internett gir P3P tjenestetilbydere en metode for aktiv formidling av hvordan de behandler informasjon, og slik aktiv formidling fører sannsynligvis til at brukere blir mer interessert i personvernspørsmål, slik Cranors [18] undersøkelse antydet.

P3P tilbyr også et brukbart utvalg av kategorier for innsamlingdata, bruksformål, og spredningsstrategier til at svært mange typer informasjon blir omfattet, samtidig som politikken kan uttrykkes og behandles automatisk. I forhold til *fair information practice* og *The Directive* har man oppfylt viktige punkter; Det er åpenhet om datainnsamlingen, og datainnsamling og bruk blir i prinsippet begrenset til formålet. Selv om P3P ikke gir noen referanse til noen kontrakt antar man at innsamleren er ansvarlig, og følger opp sin egen politikk, i beste fall gjennom systemer som E-P3P.

Med disse punktene oppfylt har brukeren kanskje en viss kontroll og tilbakemelding om hva som foregår, og et noe bedre utgangspunkt for aktivt å samtykke til datainnsamling.

Selv om P3P presenterer en av de få tekniske løsningene som er standardisert for personvern har oppslutningen likevel vært laber. Ingen nettlesere jeg har sett har per idag støtte for å lese og presentere valg basert på P3P *policies*, man er henvist til *plugin*-prototyper som *Privacy Bird*. Dette er kanskje en av grunnene til at tjenestetilbyderne ikke prioriterer å presentere sin politikk på P3P formen. En annen årsak kan kanskje være at de ikke *ønsker* å lære opp sine brukere i personvern. Ved å presentere sin politikk og gi brukeren valg risikerer man jo å få mindre og dårligere informasjon enn med dagens situasjon.

P3Ps muligheter for valg mellom flere *policies* er definert, men det finnes ingen klienter der brukerne kan å *gjøre* disse valgene. Man gir muligheter for *opt-in* og *opt-out* mekanismer, men dette medfører ganske store transaksjonskostnader for brukere å finne ut av; Man risikerer å stå ovenfor en ganske byråkratisk prosess. Bohrer [20] peker jo også på at disse mekanismene ikke gir noen særlig god kontroll, selv om dette kanskje var meningen. Løsningen Bohrer presenterer, med total dekomponering av politikk og brukergrupper gir en teknisk løsning på dette problemet, men som de også selv påpeker mot slutten av artikkelen skalerer den ikke særlig bra, og jeg er ikke overbevist om at den vil være så mye enklere for ikke-tekniske brukere å forstå heller. Den interne administrasjonen av systemet blir svært komplisert, og det samme tror jeg egentlig kan sies om E-P3P. Om slike løsninger skal brukes må det i alle fall nøye vurderes hvilket nivå dekomponeringen kan ligge på.

Et spørsmål blir om P3P bare tilbyr et skinn av brukerkontroll, mens den egentlige kontrollen og ansvaret fremdeles ligger hos tjenestetilbyder. Man må da stole på innsamleren, og eventuelt på tredjeparten som er oppnevnt som garantist for datainnsamleren. I beste fall benytter datainnsamler løsninger som E-P3P for å følge opp sin egen politikk.

Oftest vil man måtte samtykke i den politikken som tilbys om man vil benytte tjenesten. Kanskje er man med P3P noe mer opplyst om personvern enn før, men reelle valg finnes sjelden. Som ellers i Internett må man altså fremdeles ha stor innsikt dersom man virkelig skal kontrollere sine data.

4.4 Mulige løsningsmodeller for allestedsnærværende systemer

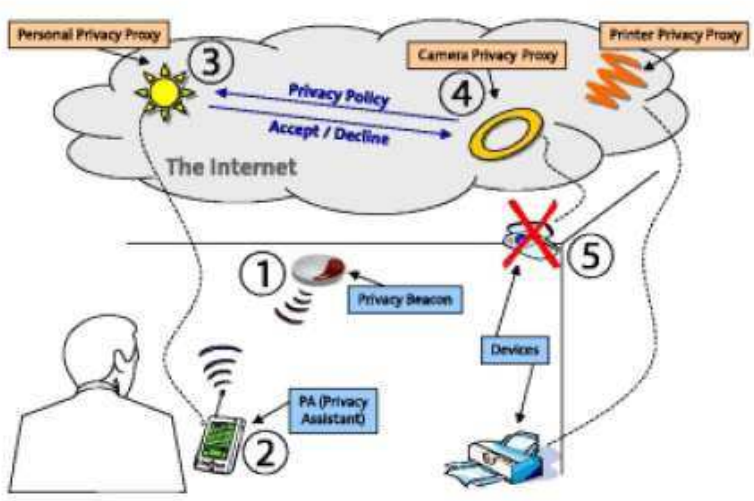
I de neste avsnittene vil jeg se på noen modeller basert på P3P som påstår å ha løsninger som kan fungere utenfor Internett, og med større muligheter for faktisk kontroll og feedback.

4.4.1 Privacy AWare System - PAWS

Langheinrich har i [17] beskrevet en prototype for et system som delvis støtter de personvern-prinsippene jeg refererte til i kap. 3.4.5.2. Han ser på prinsippene om sikkerhet, anonymitet/pseudoanonymitet som viktige deler av en infrastruktur for *pervasive* systemer, men ikke som selvstendige løsninger på problemet.

4.4.1.1 Annonsering av personvernpolitikk

Langheinrich har i sin prototype skilt mellom to typer annonsering/melding til brukere om at datainnsamling pågår: Implisitt annonsering, der en bruker aktivt søker etter tjenester ved hjelp av en service *discovery protocol* som lokaliserer tjenestene, og aktiv politikkannonsering ved bruk av et kortdistanse trådløst signal, et såkalt *privacy beacon*.



Illustrasjon 5: Slik ser Langheinrich for ser et Privacy Aware System. Se beskrivelse i avsnittet over. Illustrasjon fra Langheinrich[17]

Som et eksempel på hvordan han tenker seg sitt system har vi en situasjon der en person kommer inn i en sone der det finnes to tjenester, en printertjeneste og en sporingstjeneste med videokamera, se illustrasjon 5. Disse tjenestene og deres datainnsamlingspolitikk annonseres ved hjelp av et *privacy beacon* (1) som sender konstant med en kortdistanse trådløs kommunikasjonskanal som *bluetooth* eller *IrDA*. Brukerens *privacy assistant* (2) (PDA, mobiltelefon eller annet) oppfatter denne sendingen og delegerer informasjonen til en personlig *privacy proxy* (3) på Internett for å spare prosesserings-energi. Denne kontakter så de korresponderende tjenesteproxier for kamerasporingstjenesten og printertjenesten(4) som også finnes på Internett, og holder deres personvern politikk opp mot brukerens preferanser. Brukerens innstillinger tillater bruk av printertjenesten, men avviser kamerasporingstjenesten (5), noe som gjør at kameratjenesten slås av, eller ikke samler videre data om denne personen, eller i alle fall kan oppdages og holdes ansvarlig for at de overholder sin egen datainnsamlingspolitikk.

4.4.1.2 Maskinlesbar personvernpolitikk.

Langheinrich baserer seg på arbeidet gjort av P3P komiteen, samt at brukere skal presentere sine ønsker for personvern i preferansespråket APPEL. Egne programmer hjelper brukere å definere disse på en brukervennlig måte. Hovedprinsippet er brukeren skal ha ulike valg og gi samtykke til bruk av en av flere tilgjengelige politikker. Den politikken som passer med brukerens innstillinger, blir så automatisk valgt.

For å kunne dra nytte av syntaksen i P3P standarden vil Langheinrich bruke *EXTENSION* tagen. I eksempelet i tabell 4 angis en referanse til en RPC tjeneste for *remote access* til systemet, for oppdatering av passord. Langheinrich ser også for seg at *EXTENSION* tagen kan brukes til å sette opp regler for dataspredning i henhold til prinsippet om lokale data.

```
<ACCESS><all/>
  <EXTENSION optional="yes“ >
    <ACCESS−METHODS>
      <UPDATE rpc_uri="http://ww.example.org/soap/“ service_urn="access">
        <DATA ref="#user.login.password"/>
      </UPDATE>
    </ACCESS−METHODS>
  </EXTENSION>
<ACCESS/>
```

Tabell 4: Eksempel på bruk av P3Ps EXTENSION tag. Eksempel fra Langheinrich [17].

4.4.1.3 Personvernproxy og datatilgang

I sitt system tenker Langheinrich seg at enheter har sin egen *service-proxy*, eller at en *proxy* behandler alle enheter innenfor et miljø. På den andre side må hver bruker/enhet ha en korresponderende personlig *service-proxy*. Disse tjenestene må alltid være tilgjengelige for å svare på spørringer fra brukere og for å forhandle avtaler mellom bruker og tilbyder av tjenester. Denne personlige *proxy* skal ta seg av all utveksling av brukerdata og spørringer mot tjenestetilbyderen på vegne av brukeren.

Etter en interaksjon mellom bruker- og *service-proxy* opprettes det hos tjenestetilbyderen en avtale i form av et XML dokument som inneholder de dataelementer som er blitt utvekslet samt en referanse til hvilken personvernavtale som gjelder for disse data. En avtale-id returneres til brukerens personlige *proxy*, sammen med info om hvordan oppslag kan gjøres, og denne kan senere brukes for oppslag i den datautveksling som har foregått. Potensielt kan data også oppdateres gjennom en slik avtale-id, f.eks dersom personlige data blir endret.

Databasen lagrer innsamlede data og den inngåtte avtalen om bruk av disse sammen, og blir så ansvarlig for at data ikke brukes på en måte som er i strid med politikken som er avtalt. Det kan innebære avtaler om hvor lenge data skal lagres, bruk, og mottakere av data. Videre kan databasen holde en logg over når data faktisk er brukt. En bruker, eller en agent for brukeren, kan da kontrollere under hvilke omstendigheter personlige data om han har blitt brukt. Dermed oppfylles prinsippet om at den registrerte skal ha tilgang til informasjon om seg selv, og om bruken av denne informasjonen.

4.4.1.4 Anonymisering av informasjon

Langheinrich ser for seg at siden tjenestene befinner seg på Internett, kan disse plasseres bak

anonymiserings-*proxier*, som kan dermed kan dekoble *proxy* fra brukerens identitet, på samme måte som det ville foregå ved annen anonymisering av IP-adresser på Internett.

4.4.1.5 Trusted systems

Ideen om å lagre data sammen med metadata om bruken av data er ganske populær, f.eks for å implementere digital kopibeskyttelse. Denne slags system krever imidlertid alltid at alle ledd i distribusjonskjeden forholder seg lojale mot modellen, ellers er det egentlig ikke noen vanskelig sak å dele data fra metadata igjen, og dermed ødelegge modellen.

Modellen Langheinrich presenterer er et forsøk på å bygge et system som muliggjør lovlig bruk av data, det forhindrer ikke ulovlig bruk.

4.4.1.6 PAWS og personvernkrav

Langheinrich har i sin prototype av PAWS foreslått en del forbedringer i forhold til P3P standarden han selv har vært med å utvikle. Han forholder seg til likevel i stor grad til eksisterende infrastruktur og standarder, og prøver å innføre personvern i systemene uten å kreve for store endringer i disse. For P3P sin del benytter han for eksempel mulighetene for utvidelser som er innebygd i protokollen, og for nettverksdelen baserer man seg på å få sikkerhet og muligheter til anonymitet gjennom eksisterende strukturer.

Et punkt som bedrer brukernes kontroll med og tilbakemelding om innsamlede data er at han vil tilby referanser for inngåtte avtaler, slik at brukere senere kan bruke denne referansen og få informasjon om hvordan data har blitt brukt. Dette er et lignende system som er designet i IBM's E-P3P. Et slikt system krever at tjenestetilbyder lagrer kundens referanse og personvernkontrakten som er inngått sammen med innsamlede data om kunden. Dette medfører økte transaksjonskostnader og krav til sikkerhet hos tjenestetilbyder.

Hans eksempler tyder på at han har tenkt seg systemet først og fremst i nokså lukkede miljøer, som en bygning, der én datainnsamler har full kontroll. Han baserer seg på at systemet vil godta brukernes kanskje restriktive innstillinger for datainnsamling, noe som kan virke som en idealisert situasjon, og som fort kan komme i konflikt med systemets eget behov for sikkerhet. P3P baserer seg å tilby fornuftige valg fra tjenesteleverandørens side. I fysiske situasjoner vil det kanskje ikke være så enkelt å bare la være å benytte en tjeneste, dersom disse ikke tilbyr et valg man kan godta. Da må man kanskje implisitt godta politikken som tilbys likevel.

P3P er basert på XML, som hierarkisk strukturerer data og meta-informasjon om data. Det er designet for enklere å kunne utveksle informasjon mellom heterogene systemer, og virker dermed som et godt valg for Internett. Det krever imidlertid en del prosessering å hente ut og evaluere informasjonen i slike dokumenter. Jeg har nevnt at P3P tilbyr en *compact policies* versjon for å utveksle nøkkelpolitikk. Dette kan bedre situasjonen noe, men uttrykket må fremdeles evalueres, og man mister mye tilleggsinformasjon.

Langheinrich ser ut til å ha innsett at en P3P regel-evaluator sannsynligvis vil ha tungt for å kjøre på enkle terminaler. Oppgavene med å bli enige om en policy, og informasjonen som skal utveksles blir derfor delegert til tjenester på Internett. Disse tjenestene anses som *trusted* fra begge parters side. Dette skalerer på samme måte andre servere i Internett: Stort sett er

ikke trafikken større enn at nettet og serverne kan skaleres til å håndtere det. En slik sentralisering av informasjon vil imidlertid generere mye ekstra trafikk mellom de forskjellige *proxy*-servere på Internett, og man risikerer å blir utsatt for de samme sikkerhetsproblemer og angrep som finnes ellers på Internett. Et innbrudd på en server som holder mange personlige *proxier* vil dermed føre mye data på avveie.

Delegeringen medfører også at man baserer seg på automatiske valg basert på preferanser, man velger altså å stole på at systemet gjør riktige valg for en. Alternativet vil kanskje være at man konstant blir bombardert med spørsmål om å godta datainnsamling. Med automatiske valg blir kontrollen i innsamlingsøyeblikket altså overlatt til systemet.

4.4.2 Context Fabric arkitektur for allestedsnærværende systemer

Hong og Landay har i [36] presentert et mer omfattende konseptuelt rammerverk som de kaller Context fabric, eller Confab. Bakgrunnen for deres arbeid er en anerkjennelse av mye av det tidligere arbeid som har vært rettet mot anonymisering og sikkerhetssystemer for å ta vare på personlig informasjon. Deres fokus er imidlertid på de situasjonene der mennesker har behov for vil dele informasjon med arbeidskolleger, famile og venner. De refererer blant andre til Palen og Dourish[6], og de mener at i mange sammenhenger vil personvern ikke være snakk om å skjule identitet, men heller et ønske om å unngå uønskede eller flaue sosiale situasjoner.

Derfor har de fokus på å utvikle et teknisk system der valg og samtykke er viktige faktorer, slik at folk kan dele riktig informasjon til riktige personer og tjenester, i riktige situasjoner. De mener at personvern egentlig et spørsmål om feedback og kontroll for brukerene, og de samtykker med Palen og Dourish i at det vil være skalaer med ulike nivåer av pålitelighet og behov overfor ulike kommunikasjonspartnere.

Rammeverket er ikke ment å skulle tilby fullstendig og absolutt personvern, om noe slikt eksisterer: Confab er et forsøk på å lage et teknisk rammeverk for at utviklere skal kunne bygge applikasjoner for allestedsnærværende systemer, og for at bedriftene skal kunne tilby tjenester der de også kan oppnå tillit hos sine kunder.

Rammeverket de har designet er beregnet på miljøer med kontekstbevissthet. Det betyr altså at enheter kan være utstyrt med sensorer og andre datakilder som kan si noe om en brukers fysiske og sosiale miljø.

Forfatterne mener at et ikke ubetydelig subsett av systemer kan konstrueres på deres arkitektur. Forskning på nettverk har gått fra sentraliserte til distribuerte systemer, for eksempel lokasjons-sporing til lokasjons-støttede systemer (f.eks fra *Active Badge* [47] til *Cricket location system*[44]). Dette har skjedd for å kunne skalere systemene, og nettopp for å kunne støtte personvern, mener de. Dessuten er trenden at store subsett av mobile enheter, som mobiltelefoner og PDA-er og installerte systemer i for eksempel biler får så stor regnekraft at de med letthet kan kjøre og lagre det som før måtte delegeres til sentraliserte servere. Det er heller ikke vanskelig å se for seg at slike mobile enheter relativt billig kan utstyres med mange slags sensorer, for selv å skaffe seg kontekstinformasjon.

4.4.2.1 Brukerens behov

Et hovedtrekk i systemet er at brukerens tillit oppnås ved å være distribuert: Informasjon er innsamlet, lagret og behandlet på brukerens eget system i så stor grad som mulig. Det innebærer at sluttbrukeren vil stå fritt til å velge hvilken informasjon han vil skal deles med andre. Hong og Landay kommet frem til seks brukerkrav for hvordan informasjonsutveksling bør foregå:

- ***Innsamlingen må ha et klart formål og verdi***: Systemer som ikke gjør det helt klart hvilke fordeler systemet gir og hvilke data som derfor må samles inn er i fare for å bli boikottet eller lite brukt.
- ***Enkel og passende kontroll og feedback***: En del tidligere systemer har hatt avanserte kontrollsystemer- som har medført at folk ikke har brukt disse. I de fleste tilfeller er enkel adgangskontroll samt meldinger ved forespørsler tilstrekkelig. Det er også forskjell på hvordan øyeblikksinformasjon oppfattes kontra kontinuerlig oppdatering.
- ***Troverdig nektbarhet:*** Det må finnes en måte å oppnå utilgjengelighet, på samme måte som man kan la være å ta telefonen dersom det ikke passer eller ikke vil snakke med vedkommende som ringer. Å ikke ta telefonen kan for den som ringer tolkes som at den man vil nå ikke er hjemme eller har med seg telefonen, er utenfor rekkevidde, at telefonen er slått av, eller den egentlige grunnen, at man velger å ikke ta telefonen. De mener at det må være mulighet for "hvite løgner" for at systemer skal kunne godtas, og et visst nivå av slike muligheter må gis av systemet, og kanskje også være standard respons.
- ***Begrenset lagring av data***: Kombinering av data åpner opp for senere spredning av informasjon, og for datamining, noe som databehandlingslover regulerer ganske strengt. Ved begrenset lagring av data reduseres disse mulighetene.
- ***Distribuert kontroll***. Folk har en innebygget mistillit for sentraliserte sensitive data, fordi man har en følelse av at dersom rette vedkommende ønsker det, er det lite som kan hindre dem å bruke informasjon på måter som ikke var formålet. Det er også større konsekvenser dersom data skulle komme på avveie. Med desentralisert kontroll har man praktisk kontroll over egne data.
- ***Unntak for nødsituasjoner***: I nødsituasjoner vil behovet for hjelp være langt større enn behovet for kontroll over informasjon, og man tenker seg at en tredjepart man har tillit til kan håndtere lokasjonsinformasjon som kun kan frigis i nødstilfeller, dvs ved nødanrop.

4.4.2.2 Tjenestetilbyders og utvikleres behov

Hong og Landay har undersøkt systemkrav for en rekke ulike typer applikasjoner og tjenester, med spesiell vekt på utviklingen av lokasjonsbaserte tjenester. Systemene er av mange kategorier: Meldingssystemer, herunder mobiltelefoni, SMS, *Instant messenger*, og *smart homes*; *Finder* applikasjoner, som inkluderer søketjenester for personer, steder og objekter; gruppebevissthetssystemer, nettverksspill, situasjonsbasert sanntidsinformasjon (vær, trafikk), nødmeldingsystemer m.fl.

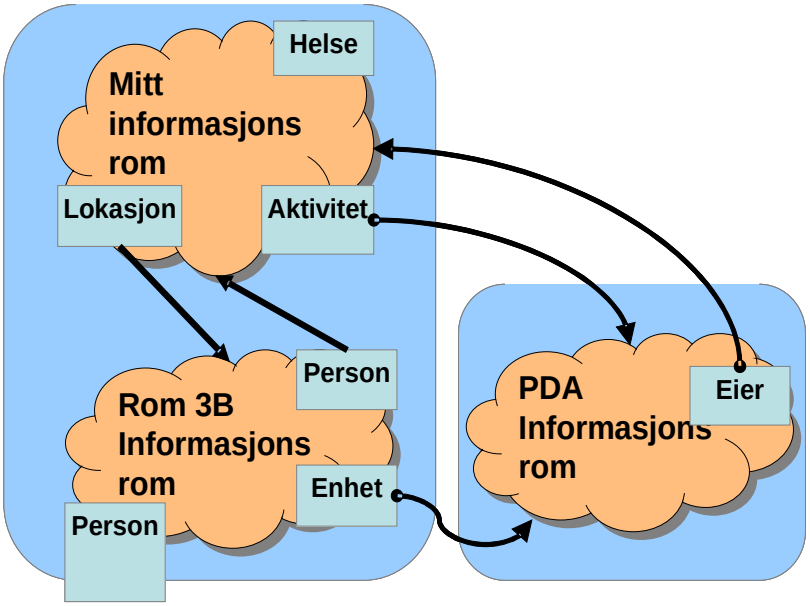
Ut fra alle disse systemenes krav har de prøvd å definere et felles multiplum for hva et system må kunne støtte for å ivareta personvern, oppsummert i fem punkter:

- ***Støtte for optimistisk, pessimistisk og mixed-initiativ applikasjoner***: Hong og Landay identifiserer tre basis interaksjonsmønstre i applikasjoner som tar personvernhensyn. I pessimistiske applikasjoner vil sluttbrukere sette opp strenge krav og preferanser for når personlig informasjon kan frigjøres til andre. I motsetning til dette finnes optimistiske applikasjoner, som gjør det enklere å frigjøre informasjon, og som heller tar problemer på etterskudd ved å vedlikeholde interaksjonslogger og gi meldinger ved bruk, for slik å kunne oppdage misbruk. Optimistiske applikasjoner er enklere å bruke, fordi det kan være vanskelig å forutse alle brukssituasjoner man kan komme opp i. For mixed-initiativ kontroll vil sluttbruker bli forespurt hver gang en person eller tjeneste spør etter personlig informasjon. Analogien vil være et spørsmål om å svare på en telefon når det ringer, eller la være.
- ***Støtte for tagging av personlig informasjon;*** Inkluderer preferanser for hvordan informasjonen skal behandles. Det kan være om den kan deles til andre og hvor lenge den kan lagres, og kan ses på som Digital Rights Management (DRM) for personlig informasjon.
- ***Mekanismer for å kunne kontrollere aksess, flyt og lagring av personlig informasjon***: Dette innebærer å kunne kontrollere hvor mye informasjon som deles. Det må kunne innføres aksessrestriksjoner basert på identitet, lokasjon og tid (for eksempel at bare personer i samme bygg kan se min lokasjon, og bare i arbeidstiden) samt at det må kunne være mulig å være usynlig i systemet.
- ***Mekanismer for å kontrollere kvaliteten på informasjonen som deles:*** Det vil si med ulik nøyaktighet, avhengig av hvem som spør. Det kan gjelde for all slags informasjon, identitet, lokasjon, identitet.
- ***Logging av informasjon, både for klienter og servere:*** For klienten er det viktig å se hvem som spør og får tilgang til hvilke data på en lettfattelig måte. For servere er det viktig å logge på en slik måte at sluttbrukerens informasjon blir behandlet lovlig og som avtalt, og for å kunne avdekke eventuell misbruk.

4.4.2.3 Confabs datamodell: Informasjonsrom

Alle personer, steder, tjenester og objekter som er interessante i en kontekst er tilegnet et informasjonsrom (*InfoSpace*), se illustrasjon 6. Dette vil være et nettverk-adresserbart logisk lagringsrom for kontekst data om den entiteten som informasjonsrommet tilhører. Hong og Landay bruker altså informasjonsrom om virtuelle informasjonsrom, i motsetning til O'Neill [7], som brukte begrepet om fysiske sosiale rom.

Rommet kan inneholde statisk informasjon, som navn og kontaktinformasjon, såvel som dynamisk informasjon, som aktivitet og lokasjon. Informasjonsrommet kan ses på som en lokal hjemmeside med informasjon om en entitet, og det er denne informasjonen vi kan dele og/eller beskytte.



Illustrasjon 6: Confabs datamodell

Informasjonsrom lagres på informasjonsservere (*InfoServers*), som kan kjøres distribuert på en persons personlige datamaskin, PDA, mobile enhet, eller på en sentral enhet, dersom det er ønskelig eller nødvendig.

Informasjonsrom inneholder kontekstuppler, også XML basert, med to typer informasjon: Indre kontekst (*Intrinsic*), som er attributter for den gjeldende enitet, og ytre kontekst (*extrinsic*), som er relasjoner til andre entiteter. Se eksempel på en *Context tuple* i tabell 5.

Tuplene inneholder metadata som kan fortelle noe om historien til data, og de kan også inneholde *Privacy tags*, som kan fortelle hvordan sluttbrukeren ønsker at data skal benyttes. Det kan være hvor lenge en tuppel skal få leve, regler for når den ellers skal slettes, og hvem som skal varsles ved bruk. En kontekstuppel inneholder også data som beskriver relasjonene til andre entiteter, og linker til disse ved hjelp av *enitity links*. Et informasjonsrom for et rom kan for eksempel inneholde flere lenker til personer som finnes i rommet.

Default svar på alle ulike datatyper er "*UNKNOWN*" uansett om en tuppel finnes eller ei. Dermed blir ingen data frigitt uten at den som eier informasjonsrommet har gitt andre eksplisitt tilgang til disse.

```
<ContextTuple dataformat="edu.school.building" datatype="location"
    description="location of an entity"
    entity-link="http://myhost.com/~jdoe"
    entity-name="John Doe"
    timestamp-created="2003.Feb.13 16:06 PST">
    <Values>
      <Value value="523" />
    </Values>
    <Sources>
      <Source datatype="location"
        link="http://localhost/map.jsp"
        source="Location Simulator"
        timestamp="2003.Feb.13 16:06 PST"
        value="523" />
    </Sources>
    <Privacytags>
        <Notify value="mailto:addr@mail.net" />
        <TimeToLive value="1 day" />
        <MaxNumSightings value="5" />
        <GarbageCollect>
            <Where requestor-location=
            "not edu.school.building" />
        </GarbageCollect>
    </Privacytags>
</ContextTuple>
```

Tabell 5: En Confab Context tuple. Eksempel fra Hong og Landay [36].

4.4.2.4 Confabs programmeringsmodell

Confab definerer to typer metoder *In* og *Out: In* metoder berører hvilke data som lagres i et informasjonsrom, og inneholder *add* og *remove*. *Out* metoder berører alle data som forlater et informasjonsrom, det vil si forespørsler(*query*), *subscribe*, *unsubscribe*, og *notify*,

For *In* metoder er det definert noen *In*-operatorer som blir kjørt på alle tupler som kommer inn i et informasjonsrom. Likeså er det definert *Out*-operatorer for all info som går ut. I tillegg har vi *On*-operatorer som kjøres periodisk for å rydde opp internt i systemet.

- Operator In:
  - Overhold tilgangspolitikk
  - Overhold *Privacy tags*
  - Send meldinger (notifikasjoner) ang. innkommende meldinger.
- Operator Out
  - Overhold tilgangspolitikk
  - Overhold *Privacy tags*
  - Send meldinger (notifikasjoner) ang utgående meldinger
  - Usynlig modus
  - Legg til *Privacy tag*
  - Interaktiv modus
- Operator On
  - *Garbage collect*
  - periodiske rapporter
  - koalesens

Noen detaljer om disse punktene:

Å overholde tilgangspolitikk innebærer å la brukere spesifisere tilgangsbetingelser for deres inormasjonsrom. Det kan være basert på hvem som spør om data, hvilke data som er forespurt, alder på data, tid og rom, eller IP-adresser. Dette gjelder både for inngående og utgående data.

Privacy tags skilles fra tilgangspolitkk. Å overholde *privacy tags* sørger for at data som ikke skal forlate informasjonsrommet ikke gjør det, samt at informasjon som ikke skal inn i et informasjonsrom ikke kommer inn. I et sett av informasjonsrom kan man jo tenke seg at noen brukere ikke behandler data på en forsvarlig måte. Dersom disse da prøver å dele disse data med andre parter som behandler data forsvarlig, vil disse kunne konkludere med at de har blitt tilsendt data i strid med det som er avtalt for informasjonen, og dermed at den andre parten ikke behandler data ordentlig. Dette kan vedkommende melde dette tilbake til avsender av informasjonen, opphavet av informasjonen, eller til en etterforskende myndighet. Med digital signering av data vil man også kunne oppdage at *privacytags* har blitt endret, og på den måten også oppdage mulige brudd på personvernet.

Sending av meldinger (notifikasjoner) angående innkommende meldinger er en del av designet for tilbakemelding: Brukeren skal ha beskjed når informasjon om han blir frigjort, når og til hvem, på en oversiktlig måte, dersom han ønsker det. *Om han ønsker det* er avhengig av om applikasjonen bruker er optimistisk, pessimistisk eller mix-initiativ skjema. I noen tilfeller kan det være snakk om oppsummeringer av delt informasjon til hvem og når, på

epost eller via øyeblikkelige meldinger.

Usynlig modus kan brukes for å fristille seg og ikke dele noen informasjon. Alle utgående meldinger blir blokkert, eller leverer verdien "*UNKNOWN*". Dette kan skje selv om man kan hente informasjon inn fra systemet. Dette gir mulighet for hvite løgner.

Interaktiv modus er ment for situasjoner der en person vil aktivt samtykke til alle utgående meldinger fra hans system, typisk i mix-initiativ applikasjoner.

Garbage collector fungerer i denne sammenheng for å slette informasjon som har *Privacy tags* som indikerer at de skal slettes, som at de har utløpt på avtalt oppbevaringstid, eller at en person befinner seg utenfor stedet der informasjonen var gyldig.

Periodiske rapporter kan sendes til eieren av et informasjonsrom for å oppsummere hvilken informasjon som har blitt frigjort til hvem over et visst lengre tidsrom.

Å opprettehold *koalesens* innebærer å slette duplikate tupler, for eksempel gjentatte tupler som indikerer at en person befinner seg på et og samme sted. Det vil være nok å beholde første og siste tuppel for når man fikk denne lokasjonen og når man forlot den.

Siden vi i dette systemet ikke har noen annen *trusted* part enn oss selv, kan vi ikke tvinge andre til å slette data, selv om vi skulle gjøre dette. *Privacy tags* er ønsker på hvordan vi vil at data skal behandles, ut over dette må man stole på sosiale, lovmessige og andre mekanismer for forhold mellom mennesker og forhold mellom kunder og bedrifter om at disse vil behandle data som det er forventet av dem.

4.4.2.5 Ulike nivåer av tjenester basert på frigivelse av informasjon

Confab har også definert sin egen måte for tjenestetilbydere å tilby ulike nivåer av tjenester, avhengig av hvor mye informasjon en bruker er villig til å gi fra seg. Et eksempel kan være en turguide som kan gi ulike grader av lokasjonsspesifikk guiding ettersom hvor nøyaktig informasjon de kan få. Det kan for eksempel være på bynivå, postnummernivå, eller svært nøyaktig med bruk av lengde- og breddegrader.

4.4.2.6 Confab og personvernkrav

I likhet med Langheinrichs PAWS er Confabs rammeverk et system som egentlig krever at alle datainnsamlere forholder seg til det for at systemet skal fungere. Egentlig er det ingen andre parter man stoler på enn seg selv, men på den andre er det innebygd en distribuert kontroll ved at systemer som mottar misbrukte data, men selv er "lovlydig", kan fortelle om dette til den som informasjonen gjelder. I tillegg til tilliten man eventuelt viser parten man deler informasjon med, kan man også få tilbakemelding fra andre parter som respekterer systemet. Dette er kanskje en forbedring i forhold til bare å måtte stole på mottaker og hans eventuelle garantister.

Confab bygger på teoriene der det er brukeren selv som kontrollerer med informasjonen, og kan regulere hvordan den skal deles, holdes tilbake når det er behov for det. De refererer blant annet til Palen og Dourish personvernakser for hvordan slik regulering foregår, og disse tankene er med i brukerkravene som blir presentert. Dette er gode prinsipper, men igjen, de vil kreve innsikt og interesse i å sette seg inn i systemet for å forstå dem.

Confab er inspirert av P3P standarden, men presenterer sitt eget hierarkiske system og syntaks for hvordan personvernpolitkk skal følge med data i det de blir delt. Og i sin programmeringsmodell har de fått med seg mange av Langheinrichs prinsipper for hva slags krav man kan sette til data. For eksempel prinsippet om lokale data og nærhet, og om at man skal motta rapporter ved bruk. Igjen er vi imidlertid avhengig av at de som mottar data praktiserer Confab-rammeverket, og strengt følger reglene som er lagt ved data, og virkelig fjerner data når de er ute av sin kontekst, eller andre vilkår for å beholde data har løpt ut.

Ellers skalerer jo systemet godt i og med at all informasjon og prosessering er distribuert. På den andre side gjelder det samme som for P3P når det gjelder regel-evaluering og administrasjon, det kan blir for tungt for enklere enheter.

4.4.3 Lokasjonsbaserte tjenester

Et annet system for kontroll av personlige data er presentert av Einar Snekkenes i [35]. Hans konsepter er designet for mobilnettverk, og hans konsept er at brukere skal kunne justere nøyaktigheten av lokasjon, identitet, fart og tid som eventuelt deles med andre. Han forutsetter at mobiltelefonnettverket kan sees på som et *trusted* nettverk og tjenestetilbyder, i prinsippet adskilt fra andre nettverk.

Snekkenes baserer sine konsepter på arbeidet som er gjort av P3P komiteen, men differensierer seg fra P3P ved at han lager et system som setter en bruker i stand til å gjøre andre valg enn å bare godta eller avvise en P3P politkk.

Konseptet er at mens P3P overlater ansvaret for å overholde personvernpolitikk til tjenestetilbyder etter at man har godtatt en avtale, skal brukeren kunne beholde mer av kontrollen ved å minske nøyaktigheten på informasjonen som eventuelt deles.

Se illustrasjon 7 på side 90 for et eksempel på en forespørsel i Snekkenes` system.

4.4.3.1 Identifikasjonsstiger

Identifikasjon og lokasjon omtales i artikkelen som to ulike stiger, eller *lattice,* definert som et "delvis ordnet sett med en unik topp og bunn". Stigene kan på mange måter sammenlignes med Palen og Dourish identitetsakse.

En person vil i den ene enden av en identitets-stige være uidentifiserbar (I form av ikke mulig å skille fra en mengde andre objekter), til i den andre enden å være unikt identifisert. Eksempler på delvis identifikasjon på en slik skala kan være å avsløre f.eks. kjønn eller arbeidsgiver.

Den andre stigen er lokasjon. Denne observasjonen har dynamiske bestanddeler av både tredimensjonal posisjonering i et visst område, et tidspunkt for denne observasjonen, samt en hastighet for objektet, basert på en eller flere observasjoner over tid. Også på denne stigen er det nivåer, fra ikke å gi noen informasjon om posisjon i det hele tatt, til nøyaktig posisjon, fart og/eller tid. I mellom disse finnes det mindre og mindre geografiske områder, tidspunkt og hastighetsområder man kan referere et objekt til.

Snekkenes har ved hjelp av logisk notasjon beskrevet disse konseptene der objekter er med i sub-sett av identifikasjonsnivåer i stigene. På den måten presenterer han altså et språk for hvordan man kan minske nøyaktigheten av rådata, og levere tilpassede data til tjenestetilbydere, alt etter brukerens innstillinger.

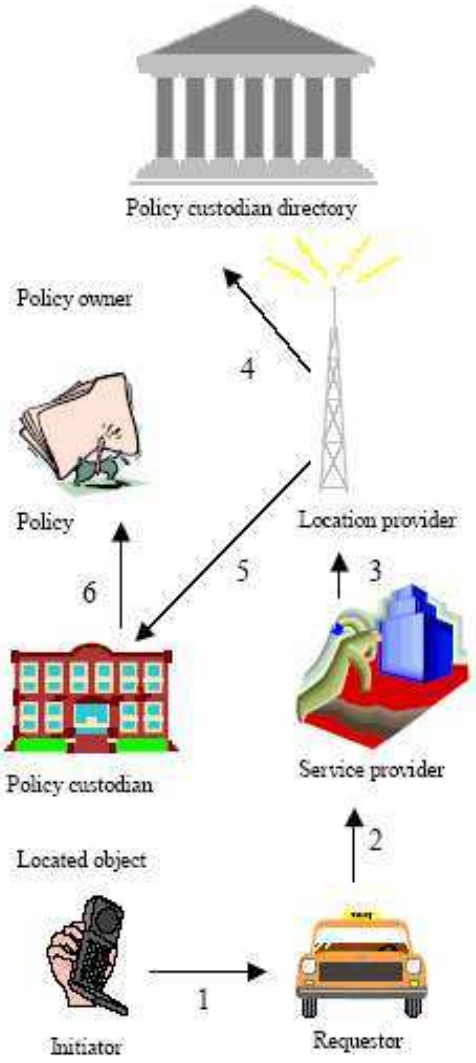
4.4.3.2 Håndtering av forespørsler

Det er stort sett to typer forespørsler man kan stille i forhold til lokasjon. Den ene er av typen; "Hvor er du?" Den andre er av typen: "Er du ved X? ". På det første spørsmålet kan en lokasjonsbestemmelse av typen beskrevet over være på sin plass, på den andre er det nok med et enkelt JA/NEI. Likevel må det i begge tilfeller defineres og beregnes hva det vil si å være "ved" et sted, så tankemåten kan være nyttig uansett. Begge typer spørsmål kan potensielt avsløre sensitiv informasjon, den første nok oftere enn den siste, som medfører mer kvalifisert gjetning.

Snekkenes har så begynt å definere et språk i BNF syntaks som en bruker (eller et brukerprogram) kan bruke til å definere en politikk for identifikasjon og lokasjonsbestemmelse. Språket bruker XML i sin syntaks, og bygger videre på P3P standarden. Definisjonen inneholder også et utkast til hvordan responsen fra en forespørsel vil se ut: Det vil bli en observasjon av en bestemt nøyaktighetsgrad, tilpasset i henhold til brukerens innstillinger.

For brukerens del vil en policy bestå av en *default* respons som skal leveres dersom ingen andre preferanser slår til. Denne responsen vil være svært begrenset, nærmest anonymitet.

Videre kan brukeren sette opp g*uards*, altså betingelser som må være oppfylt for at andre typer svar skal kunne gis. Det kan være at man vil at et vaktselskap skal kunne spore farten og posisjon på en persons bil dersom eieren *ikke*



Illustrasjon 7: En tjenestetilbyder(requestor) som ønsker lokasjon og identifikasjons opplysninger om et eller flere objekter, f.eks. en mobiltelefon(1), sender en forespørsel til tjenestetilbyder(2) om å få vite mest mulig. I sin forespørsel må han inkludere formålet, sin egen identitet, og videre hva slags policy tjenestetilbyderen har for videre bruk av data, som i P3P. Leverandøren av mobiltjenesten vil også gjerne fungerer som en lokasjonstilbyder(3). Snekkenes ser for seg at det bør finnes et offentlig register, et Policy Custodian directory(4) lik en DNS tjeneste, som lokasjonstilbydere kan slå opp i for å finne en Policy Custodian(5), der mobilbrukerens personvernpreferanser (6) ligger lagret. Lokasjonstilbyderen deler så tilstrekkelig nøyaktig informasjon ut fra brukerens preferanser. Illustrasjon fra Snekkenes [35].

kjører bilen selv. Det kan også for eksempel settes opp betingelser om at en forespørsel må komme fra en viss tjenestetilbyder, og at tjenesten må være av den bekreftende typen, som bare leverer ja/nei svar. Eller det kan være at vi vil gi fra oss posisjon, men ikke identitet, for eksempel til en taxitjeneste.

4.4.3.3 Lokasjonsbaserte tjenester og personvernkrav

Snekkenes modell gir den enkelte bruker kontroll til å sette opp regler som kan kontrollere hvordan informasjon skal deles med ulike parter. Han krever ikke at andre systemer skal implementere det samme systemet, men verner bare egen informasjon.

Systemet krever et nettverk som anses som *trusted* for å kontrollere innstillinger og levere informasjon, ikke egentlig så ulikt Langheinrichs *privacy proxy*. Forskjellen er at Snekkenes fokuserer på mobiltelefonsystemer, der det meste av informasjonen om lokasjon og identitet, og kanskje aktivitet faktisk allerede ligger i nettverket, og ikke hos personen selv.

Han forventer at tjenestetilbyder skal kunne presentere hvordan han skal bruke data, for eksempel ved hjelp av P3P, og tilpasser så nøyaktigheten i data han deler i forhold til dette. Denne inndelingen i personvernstiger kan korrespondere til Palen og Dourish akser om sosial kontroll. I motsetning til andre forventer han egentlig ingen tilbakemelding og tilgang ut over dette.

Transaksjonskostnaden for kunden ligger i å konfigurere sine personverninnstillnger, altså hvilke avtaler man er villig til å godta og med hvilken nøyaktighet man i så fall vil dele data. Beslutninger om deling skjer så automatisk i innsamlingsøyeblikket, basert på disse personverninnstillingene.

4.4.4 Oppsummering

Jeg har i dette kapitlet presentert metoder som er i bruk i eksisterende teknologier og foreslått i løsningsmodeller for å beskytte personlig identifiserbar informasjon fra de ulike trusler om observasjon, uautorisert førstehåndstilgang, og deling med tredjeparter gjennom annenhåndsinformasjon eller datamining. Beskyttelsesstrategier mot observasjon og uautorisert adgang fokuserer ofte omkring å kryptere informasjon og kommunikasjon, og sikring av dataintegritet. For de andre truslene baserer løsningene seg på ulike grader av kontroll og tilbakemelding om egne data og bruken av disse, samt inngåelse av fysiske eller virtuelle avtaler, eller sosial regulering der man gjennom gjensidig tillitsbygging stoler på at andre parter ikke vil bruke og dele informasjon på andre måter enn avtalt.

Gjennom presentasjonen har jeg også sett på utfordringer løsningene presenterer i forhold til å få gjennomført transaksjoner. For brukerne innebærer dette varierende vanskelighetsgrad og behov for innsikt i systemet, for systemet innebærer det utfordringer med krav til prosessering og skalering.

I det neste kapitlet vil jeg prøve å ordne resultatene jeg har kommet fram til, både i forhold til at disse personvernkrav har kommet ut fra mitt scenario med Sporveiens elektroniske billettsystem, og for de mer generelle implikasjoner for allestedsnærværende systemer.

5 Diskusjon

I dette kapitlet vil jeg først diskutere mine resultater i forhold til de teorier og systemer jeg har gjennomgått. Jeg vil presentere en modell for hvordan tillit må oppnås som en prekondisjon for informasjonsdeling, før jeg foreslår noen løsninger i eksempelet med Sporveiens billettsystem. Jeg vil så diskutere noen generaliseringer av resultatene med mulige implikasjoner på teorien. Jeg vil så se på hvordan metoden jeg har brukt kan ha påvirket mine resultater, før jeg til slutt gir noen føringer for videre arbeid.

5.1 Resultater i forhold til andres arbeid

I tabell 6 har jeg forsøkt å ordne hvordan noen av de systemene jeg har diskutert forholder

System / **Avsløring**	**Elektronisk Billettsystem (for Sporveien)**	**Internett**	**Awareness systemer**	**Instant Messenger/ Chat**	**Mobil**
Sosial bruk i systemet (informasjonsrom , utvidet til også å gjelde virtuelle rom)	Ingen. Bruk er kun relatert til gjennomføring av kollektivtransport.	Offentlig rom En-til-mange, men ofte sosial/privat bruk der man adresserer noen få. Kjente og ukjente mottakere	Sosialt rom En-til-en eller flere. Tillit til mottaker, ikke alltid kjent	Sosialt rom En-til-en eller flere - kjent mottaker	Privat rom En-til-en Mulig lydforurensing av offentlige rom?
Brukers forhold til det tekniske systemet (forhold til teknisk interaksjonsrom)	*Trusted system* Primært automatisk kommunikasjon til systemet.	Offentlig kanal, med varierende datainnsamling. Brukere har varierende systemkunnskap.	Internt nettverk, alle "interne" er potensielle brukere. Ofte stor innsikt i systemet.	Offentlig kanal, IM systemer har datainnsamling. Varierende systemkunnskap	*Trusted system* Identifikasjon i systemet nødvendig for teknologi og transaksjon
Rekonstruksjon over tid (tidsaksen)	Rekonstruksjon av reisemønster per billett.	Søkemotorer lagrer info over tid. Delvis info lagret på mange steder. Ingen total rekonstruksjon.	Rekonstruksjon av arbeidets framdrift, og all sanntids-informasjon	Samtalepartner kan lagre informasjon over tid. Kanskje også system?	Rekonstruksjon for fakturering, og andre formål.
Personlig identifiserbar informasjon (PII) (identitetsaksen, informasjonssfærer)	Tidspunkt og lokasjon m.m. ved all bruk per billett Identitet (ved kundeavtale)	All bruk logges av webservere. IP-adresser kan lokaliseres og identifiseres. PII legges implisitt og eksplisitt igjen på egne eller andres websteder	Identitet, mange nivåer og typer av aktivitet, lokasjon, delt informasjon. Arbeidsrelatert kommunikasjon	Oftest identitet, tilstedeværelse/ aktivitet. Kan bruke pseudonym. Sosial/privat kommunikasjon Ellers som Internett.	Identitet, tidspunkt, lokasjon , samtalelengde, m.m., logges sentralt. Kommunikasjon i privat sfære.
Totalt Spredningspotensiale	Reisemønster i billettsystemet og partnere. Internett via kundekanal. Anonym for de fleste andre.	I prinsippet høy og og global, spredning av del-informasjon. Ingen kontroll med delt informasjon.	Detaljert info, men begrenset til arbeidsmiljø Anonym for alle utenfor systemet	Anonym ? for alle utenom systemet, men potensielt som i Internett.	I mobilsystemet og samarbeids partnere. Internett via kundekanal. Anonym for de fleste andre.

Tabell 6: Systemegenskaper i forhold til ulike avsløringsaspekter.

seg til noen sosiale egenskaper, basert på Palen og Dourish akser og O'Neills ulike rom.

Jeg har ikke fulgt deres Palen &Dourish og O'Neills kategorisering slavisk, men refererer til deres begreper i parentes der jeg mener det er relevant.

5.1.1 Avsløringsapekter

I kap. 3.2.9 stilte jeg spørsmål ved om *avsløring/disclosure* kan ses på som en egen dimensjon, slik som Palen & Dourish gjør det med Altmans teorier, eller om avsløring egentlig består av andre aspekter. Jeg har prøvd å sette dette i system i tabell 6. Ulike egenskaper ved hvordan systemet blir brukt og hvordan datainnsamlingen skjer kan føre til ulike grader av avsløring av informasjon om brukerne.

5.1.1.1 Spredning i et system vs. sosial spredning

Det er etter mitt syn to viktige dimensjoner for når informasjon kan bli spredd; Gjennom den sosiale bruken, og gjennom systemets bruk av innsamlet informasjon. I tabellen har jeg derfor skilt mellom avsløring i forhold til sosial bruk og i forhold til systemet. Med sosial bruk mener jeg informasjon som går fra en person til en annen, ikke nødvendigvis i sanntid, men uavhengig av annen senere bruk i systemet. Med systemets bruk mener jeg hvordan systemet behandler informasjon som har blitt meddelt det, enten direkte som part i en kommunikasjon, eller fordi systemet har blitt brukt som en kanal i en sosial kommunikasjon.

En slik oppdeling ligger ikke så langt unna Görlachs [4] oppdeling av de ulike trusler, omtalt flere steder, først i kap. 1.3.1. Lekkasje av informasjon i allestedsnærværende systemer handler om å få tak i førstehåndsinformasjon eller annenhåndsinformasjon: den første refererer til situasjonen der en bruker selv deler informasjon om seg selv, mens den andre handler om at systemet deler eller selv finner informasjon.

For Internett er det slik at den faktiske bruken som regel er privat (man sitter alene ved skjermen), informasjonen man aktivt deler blir offentlig (hjemmesider, nyhetsgrupper), mens informasjon om bruken og eventuelle registreringer blir lagret i servere man kommuniserer med. I disse to siste mister man i de fleste tilfeller kontroll over videre bruk.

For mobiltelefoner er bruken i utgangpunktet sosial, og jeg har referert til Palen og Dourish sin undersøkelse om bruk av mobiltelefon i det offentlige rom, kap. 4.2.2. Det hender selvsagt at private opplysninger slik kommer ut i det offentlige rom, men spredningen er begrenset. Kanskje er ikke sosial mobilbruk som dette egentlig et spørsmål om personvern, men heller et spørsmål om lydforurensing og tilvenning til mobiltelefoni/mangel på sosiale antenner.

Men informasjonen om bruken logges alltid av mobiltjenesteleverandøren, og kan i verste fall avlyttes. Vi anser leverandøren som et *trusted system*, men vi har egentlig lite kontroll og tilbakemelding på hva som skjer videre med informasjonen inne i systemet. Jeg har antydet i 4.2.4 at innføringen av forskjellige *awareness* systemer for mobiltelefoni kanskje vil endre på den tilliten vi har til våre leverandører, fordi informasjonen de innehar da faktisk blir delt med andre.

På den andre side finnes *Awareness* miljøene, som i utgangspunktet ser på all innsamling som sosial. Ofte har man muligheter til innsikt og kontroll av hva man deler med systemet og

hva som finnes der fra før. Grensen mellom den sosiale bruken av systemet og systemets bruk av informasjon er dermed nesten borte. Man antar at man allerede er beskyttet mot uautorisert bruk ved at dette er interne systemer. Terskelen for hva som er akseptabelt å dele av informasjon kan derfor være mye lavere.

5.1.1.2 Personlig identifiserbar informasjon, tidsaksen og spredningspotensiale

Det er forskjeller på sensitiviteten i informasjon som blir samlet inn. Derfor var det naturlig at et av avsløringsaspektene i tabellen er personlig identifiserbar informasjon.

For *awareness*-systemer er deling av identitet, lokasjon, og aktivitet og eventuell rekonstruksjon av disse en akseptert del av helheten i systemet. Tilliten er stor, basert på sosiale normer, og innsikt og kontroll i systemet. Dessuten er man bare en del av systemet i jobbsammenheng, eller når man ellers velger å være det. Det samme er tilfelle med *Instant Messenger*. Man har valget om ikke å bruke applikasjonen, og begrense hva man deler. Sosiale mekanismer vil som oftest regulere hvordan personer som konverserer eventuelt bruker informasjon som er lagret.

Palen og Dourish peker på tidsaksen, altså at informasjon blir lagret og kan rekonstruere informasjon, som et av problemene i dagens personvernsituasjon, noe jeg tror de har rett i. Et av avsløringsaspektene i tabellen omhandler også muligheter for rekonstruksjon av aktivitet over tid. Palen og Dourish synes å mene at informasjonen i tidsaksen også kan reguleres gjennom den "dialektiske og dynamiske" prosessen. Dette stemmer kanskje i de eksemplene som de gir, der man har flere kanaler tilgjengelig. I Internett er informasjon om hva man har foretatt seg spredd ut over alle de steder man har kommunisert, surfet, og publisert informasjon, og det er dermed mulig å balansere den informasjonen som finnes.

I Internett legger vi fra oss spor mange steder, men noen total rekonstruksjon av alt vi har foretatt oss er vanskelig å få til. Den største risikoen er etter mitt syn ikke hvilket inntrykk av en person som kan dannes gjennom søk i søkemotorer, selv om dette *er* en risiko, som Palen og Dourish nevner. Som mye annet i denne oppgaven handler det mer om hva den enkelte datainnsamler gjør med de data de har samlet inn, hvem de deler disse med, og hva de bruker dem til.

5.1.1.3 Ingen sosial dynamisk prosess?

For billettsystemer og mobilsystemer er det slik at systemet automatisk samler inn informasjon over tid, etter sigende fordi de trenger informasjonen for at systemene skal fungere, og for å sikre økonomisk integritet. Tilliten til slik automatisk innsamling er basert på at brukeren oppfatter innsamlingen som viktig for å kunne oppnå et eller flere formål: For mobilsystemer er dette for det første å kunne tilby dem mobiltjenesten, og for det andre å kunne dokumentere riktig fakturering. For billettsystemet er formålet kanskje å tilby en enklere og mer pålitelig reise, samt økonomisk integritet i de elektroniske transaksjonene. Når kunden har "godkjent" formålet , implisitt eller eksplisitt, bryr han seg sjelden om detaljene i hvordan innsamlingen skjer, eller hvordan informasjonen videre blir behandlet, ut over at man har tillit til at datainnsamlerne behandler informasjonen ordentlig.

Jeg antydet i 3.3.5.2 at automatisk innsamling av informasjon i slike situasjoner ikke passer

særlig bra inn i modellene til hverken Palen & Dourish eller O'Neill. Palen og Dourish mener at alle grensespenningene i tid, identitet og avsløring foregår i en sosial, "dialektisk og dynamisk prosess" mellom individet og de andre. De forutsetter altså at individet har en interesse i å regulere informasjonen som samles inn og finnes i systemet.

Det samme er tilfelle med O'Neills teorier. Han har studert systemer for offentlig kommunikasjon på offentlige steder, og presenterer nettopp et system for å ordne hvordan vi forholder oss til deling av informasjon i ulike sosiale situasjoner. Han forholder seg ikke til at hensyn for å ordne sosiale rom i den teknologiske verden er lite verdt dersom systemet vi kommuniserer med eller gjennom, interaksjonssfæren, benytter informasjonen på andre måter enn den sosiale situasjonen tilsier.

Begge forutsetter altså at det finnes en sosial prosess, der vi er i stand til, og ikke minst interessert i å gjøre valg, gi samtykke, kontrollere og motta tilbakemeldinger fra systemet. Det er mange systemer som praktiserer slik automatisk innsamling uten egentlig å gi noen reelle valg for datainnsamling, eller i å kunne velge å bruke systemet. Slike systemer faller etter mitt syn utenfor aksene som er foreslått for å "pakke ut" personvernhensyn. Jeg mener det kan være grunn til å spørre om disse systemene er glemt i teorien, og om det kan være andre mekanismer som gjør av vi godtar informasjonsinnsamling og stoler på datainnsamlerne.

5.1.1.4 Total spredningsfare

Alle avsløringsaspektene oppsummeres grovt i det jeg har kalt for total spredningsfare i tabellen. Den verste spredningsfaren finnes i Internett, men denne minskes noe fordi informasjonen gjerne er stykkevis. Spredning i *awareness* systemer er stort sett begrenset til arbeidsmiljøet. Spredning ut over dette kan være forretningskritisk ugunstig for bedriften, men sjeldnere for den enkelte, i og med at informasjonen som spres oftest er jobbrelatert.

Dersom vi har et tillitsforhold med systemet er informasjonen vi gir fra oss gjerne mer kritisk, knyttet til privat informasjon. For den enkelte vil det være verre om slik informasjon ble spredd. Oftest fungerer nok dette tilfredsstillende, ved at informasjonen holder seg innenfor systemet, men dette har brukeren som regel ikke annet enn en antagelse om i forhold til informasjonssjangeren (Palen & Dourish [6]) , eller den implisitte avtalen.

5.1.1.5 Oppsummering om avsløringsaspekter

For allestedsnærværende systemer må man skille den sosiale bruken mellom mennesker i systemet fra systemets bruk av informasjonen. Selvfølgelig er det i mange tilfeller mennesker bak systemene også, men disse vil opptre som representanter for systemet selv, industri, myndigheter eller andre som har til hensikt å bruke data på et vis.

I mange systemer der informasjonen er mest privat blir informasjon automatisk samlet inn uten at det blir gitt valg. Det eksisterer ingen sosial prosess for å regulere hvordan informasjonen oppfattes eller brukes. Disse situasjonene ser ikke ut til å passe inn i teorien jeg har beskrevet for regulering av personvern. Spredning av denne informasjonen vil være mer kritisk enn spredning i andre domener, men her er vi altså overlatt til å stole på systemet.

5.1.2 Personvernkrav i de ulike systemer og løsningsmodeller

I tabell 7 har jeg satt opp en sammenligning av noen av de systemene jeg har presentert i forhold til personvernkrav for sporveien. Personvernkravene jeg har analysert etter kom fram fra designet og dokumentasjonen jeg hadde tilgjengelig for Sporveiens billettsystem, og er de kravene jeg har satt teori og løsningsmodeller opp mot. Sammenligningen er satt opp for å vise hva de ulike konseptene kan tilby for å støtte kravene jeg mener de reisende på Sporveien kan stille til billettsystemet.

Personvernkrav/ System	**Kontroll**	**Melding/ tilbakemelding**	**Avtaler**	**Transaksjons-kostnader**	**Sikkerhet**	**Note**
(Sporveiens) Elektroniske billettsystemer	*Kan velge å kjøpe anonym billett? Kundeprofil på web*	*Validert/ stemplet billett? Kundeprofil på web?*	*Eventuell kunde-/ reise-/ personvern-avtale ?*	*Må være enkelt ? MANGE transaksjoner-begrenset prosessering?*	*Trusted system? Sikkerhet arvet fra konvergende systemer?*	-
Internett	Ansvar for å verne seg ligger hos bruker. (Virus,*cookies*, brannmurer)	-	Eventuelle Privacy policies implisitt godtatt ved bruk.	-	Mulighet for adgangskontroll kryptering, anonymisering	-
Mobiltelefoni	Av/på	Faktura	Abonnements-avtale	Enkelt for bruker	*Trusted system*	-
Awareness systemer	Relativt detaljert kontroll over egen status	Melding ved andres søk, gjensidig awareness.	Sosiale relasjoner	Krever høy innsikt i systemet for bruker	-	-
Instant Messenger	Kan endre egen status	Melding kun ved aktiv kontakt.	Sosiale relasjoner	Relativt enkelt for bruker	-	-
Smartcard	-	-	-	Enkelt for bruker. Krever avanserte systemterminaler	Kort rekkevidde Adgangskontroll Kryptering	-
P3P1.0	Skal prinsipielt ha valg mellom avtaler. Avtale kan kreve anonymitet. *Opt-in opt-out.*	Forhåndsmeldning om bruk.	Maskinlesbare privacy policies	Bruker må forstå personvernspørsmål Evaluering av XML *policies* krever prosessering	Kan lage regler som bare godtar anonym innsamling av data	Standardisert, men få har implementert.
E-P3P	*Opt-in opt-out*. Evt. ytterligere dekomponering av rettigheter og data	All bruk blir logget, tilbakemelding kan gis	Referanse til lagres sammen med data	Bruker må forstå personvernspørsmål Tungvint intern datatilgangsprosess	*Trusted system* Regler for nærhet /lokale data	Intern overholdelse av *Privacy policies*
PAWS	Kontroll for å sette opp *policy*. Senere ansvar delegert til *proxy*. Antar at man kan bli enig om *policy*	All bruk blir logget, på server, Bruker logger deling, og får referanse for tilgang til sine avtaler/data/ bruk av disse	Avtaleinfo lagres sammen med data	Bruker må forstå personvernspørsmål og sette opp sin egen *policy*. Intern prosessering for å følges opp avtalt bruk.	Som P3P1.0 Regler for nærhet /lokale data	Kun prototype Krever at alle bruker rammerverket
Confab	Detaljer kontroll for frigivelse av informasjon/nekt barhet hos hos brukeren	Logging av deling og bruk i alle informasjonrom. System for tilbakemelding og periodiske rapporter. Kan få melding om uautorisert databruk	Avtaleinfo lagres sammen med data DRM for informasjon	Brukeren må forstå systemet, awarenss av andre enheter, personvernspørsmål Intern prosessering for å følges opp avtalt bruk.	Digital signering gir integritet. *UNKNOWN* svar for nektbarhet/ anonymitet Regler for nærhet /lokale data	Kun prototype Krever at alle bruker rammerverket
LBS	Setter opp sine egne policies. Kan ha streng/ anonym *policy.*	-	Maskinlesbare *privacy policies*	Må sette opp egne policies/ regler for granularisert identifikasjon	Stoler på *trusted system* hos mobiltjeneste-leverandør	Kun prototype

Tabell 7: Personvernkrav vs. løsningsmodeller og ulike systemer.

5.1.2.1 Kontroll og tilbakemelding

For design av personvern har jeg referert til arbeidet som er gjort av W3C komiteen, spesielt de prinsippene Langheinrich har skissert (kap.3.4.5.2) , basert på f*air information practice* og *The Directive,* samt innspill fra *Awareness* miljøet, spesifikt Bellotti og Sellen i kap. 3.4.2. I løsningsmodellene presenterte Hong og Landay et sett av brukerbehov og utviklerbehov i kap. 4.4.2.1 som korresponderer godt med arbeidet til Bellotti og Langheinrich. Samtlige av disse har fokusert på valg, kontroll, samtykke og ulike versjoner av melding for at brukeren skal ha tillit til informasjonsdelingen og kontroll med egne data.

I 3.4.4.3 diskuterte jeg om valg og kontroll egentlig var noe som var ønsket i et system som billettsystemer. Jeg konkluderte med at den reisende sannsynligvis er lite interessert i kontrollfunksjoner i systemet, fordi systemet systemet ikke gir dem noe, annet enn et bevis på at de har betalt for transporten. Fraværet av den sosiale prosessen med systemet gjør altså at systemet i utgangspunktet blir lite interessant å ha en interaksjon med, ut over det aller mest nødvendige.

Nå er det slik at billettsystemet likevel kommer til å samle inn informasjon. Kan noen av de konvergerende systemer eller løsningsmodeller bidra med noen form for løsning for å omgå problemet? Eller er det mulig å tilby et tilstrekkelig enkelt nivå av kontroll, tilbakemelding, valg og samtykke for datainnsamling, som reisende/brukere kan godta?

Awareness løsninger går ut fra at all informasjon kan samles inn dersom man ikke selv har gjort innstillinger som sier noe annet. Det må gå an å gi brukere bedre valg enn som så? I Internett er all kontroll overlatt til brukeren, eventuelt til programmer som kontrollerer deling av informasjon på vegne av brukeren. P3P og variasjoner av denne gjør det mulig å sette politikk som gjør at man krever å være anonym, eller andre nivåer av identifikasjone. Det samme også med løsningsmodellene Confab, LBS, PAWS.

Kanskje er dette en mulighet, men det forutsetter at tjenestetilbyder er villig til å tilby nivåer av identifikasjon, som igjen innebærer at han ikke får samlet inn all den informasjonen han kanskje ønsker i alle tilfeller. Det forutsetter også at brukeren blir stilt enkle spørsmål så han virkelig kan samtykke i datainnsamling, og kanskje forstå noen av de hensyn til personvern som ligger bak. Slikt samtykke kan ikke skje ved hver transaksjon/reise, men det er kanskje mulig å henlede oppmerksomheten på slike spørsmål i det en kundeavtale/abonnement blir inngått eller i enda enklere form når "vanlige" billetter blir kjøpt?

5.1.2.2 Avtaler

Mennesker liker at avtaler blir inngått og holdt, og avtaler og kontrakter er med på å skape tillit mellom parter. Vi praktiserer også ofte implisitte avtaler bare ved hjelp av forventninger til hvordan en handling skal foregå.

De færreste liker å lese avtaletekster. Så langt har dette likevel vært den eneste måten avtaler i forhold til systemers bruk av innsamlede data er blitt formidlet. Resultatet er at de færreste antagelig leser avtalene de implisitt inngår ved å fortsette å bruke systemet. Dette er tvilsomt i forhold til *fair information practice* og *The Directive* (kap. 3.1), som krever opplysning, samtykke og ansvarlighet fra datainnsamler.

En del av løsningsmodellene, som P3P,PAWS og LBS, mener at slike avtaler kan formidles og "inngås" automatisk, basert på brukerens innstillinger. Eventuelt kan avtalene presenteres i en lettfattelig form. Dette må til for å gjøre systemene brukelige i forhold til at det kan komme svært mange forespørsler som brukeren må gi sitt samtykke til.

Jeg har forståelse for argumentet om brukbarhet, men på den andre side fungerer avtaler som har med å opprette tillit best når det er gitt et *samtykke,* som også *The Directive* krever. Automatiske avtaler bør derfor etter min mening bare gis når det er snakk om total avvising, altså der man samtykker om ikke å gi fra seg identifiserbar informasjon i det hele tatt. Man kan jo spørre om det er nødvendig å inngå avtaler i slike tilfeller, men en avtale om *ikke* å samle inn informasjon kan være juridisk nyttig å ha dersom det skulle vise seg at datainnsamler likevel har samlet inn identifiserbar informasjon.

Avtaler og valg/kontroll henger tett sammen. I mange tilfeller vil en datainnsamler sannsynligvis bare gi en bruker valg i forhold til de svar han ønsker, vridd i en retning. Datainnsamler skal etter reglene ha en god grunn for datainnsamlingen, men det er ofte lett å finne en grunn. Dersom man "svarer feil" i forhold til det som er ønsket eller påkrevet kan man altså risikere å ikke kunne bruke tjenesten. I fysiske situasjoner som kollektivtrafikk kan dette by på problemer. *Faktiske* valg i forhold til avtaler og at datainnsamlere respekterer disse valg er altså svært viktig. Spørsmålet er om tjenestetilbydere er villige til å tilby dette.

Automatisk formidling av avtaler kan fungere, og vil kanskje bli nødvendig etterhvert som vi får allestedsnærværende systemer. Samtykket i datainnsamling bør imidlertid ikke bli automatisk, men heller fremheves i mye større grad enn i dag. Jeg tror ikke man kan bygge opp tillit til datainnsamlere ved å overlate til andre datasystemer å gi samtykke.

Dette krever selvfølgelig igjen at brukere blir lært opp til å forstå personvernspørsmål i forhold til datainnsamlingen man blir presentert. Det er en hårfin linje mellom å gi brukere mulighet til valg og kontroll, og å være irriterende ved konstant å be om samtykke.

5.1.2.3 Transaksjonskostnader

I gjennomgangen av design og løsningsalternativer har jeg ofte kommet fram til at løsningene byr på store transaksjonskostnader, både i form av vanskelighetsgrad og krav til opplæring av brukere, og til skaleringskrav i datainnsamlerens system. I forhold til elektroniske billettsystemer må brukere forstå personvernspørsmål fra et system de ikke forventer å få slike spørsmål fra. Det kan hende at dette kan bedre seg dersom de i andre sammenhenger blir vant til å få de samme spørsmålene og eventuell muligheter for kontroll og tilbakemelding, og dermed blir "opplært" i konseptene. Dette var jo for eksempel erfaringen ved bruk av *Privacy bird*, kap 4.3.4.3, og er også egen erfaring ved bruk av denne applikasjonen over en viss tid.

For alle løsningsmodellene, P3P, E-P3P, Confab, Paws og delvis LBS krever innføring av interne datasystemer for å håndtere avtaler/metadata minst like store transaksjonskostnader som innføring av sikkerhetsystemer for kryptering og adgangskontroll tidligere har gjort. Systemene som er presentert medfører ganske kraftige endringer i hvordan datainnsamlere kan benytte de data de har. Man har jo også tidligere vært prinsipielt bundet av slike prinsipper gjennom at man forholder seg til lovverk, som f.eks. Personopplysningsloven, og

sine egne *privacy policies.* Med systemer som E-P3P blir databehandlingen mye strengere *bundet* til disse avtalene, og avvik vil bli registrert. Vil bedriftene være interessert i slike endringer?

Transaksjonskostnader er et viktig punkt. Systemer må være enkle å bruke, i alle fall for kunden, for å bli akseptert og brukt.

5.1.2.4 Sikkerhet

Sikkerhet er viktig først og fremst for å verne førstehåndsinformasjon fra å komme på avveie. Dette punktet har tatt for seg hvordan de ulike domenene ser på sikkerhet som en bestanddel for personvern. En del systemer ser på sikkerhet som det som sikrer personvern, ved at de ser på og presenterer seg selv som et *trusted system.* Dette er tilfellet for mobiltelefoni, og jeg har i kap. 4.2.5 presentert likheter mellom mobiltelefonisystem og elektroniske billettsystemer, og peker på at Sporveien ønsker lignende forhold i sitt system. Mange av likhetene gikk på sikkerhetsaspekter i forhold til å kunne være et *trusted system.*

I *Awareness* miljøet oppfatter jeg det som at sikkerhet er en totalt annen dimensjon enn det som har med personvern å gjøre: Man forutsetter at sikkerhet eksisterer som en ramme rundt systemet som kontrolleres og tilbyr awareness.

Andre, som E-P3P bygger inn avanserte adgangskontrollsystemer basert på brukerroller, oppgitt formål ved bruk av data, samt inngåtte avtaler som evalueres og bestemmer om tilgang til data kan gis.

En del miljøer ser på mulighetene for å anonymisere sendere, mottakere, og informasjonen de sender som et viktig sikkerhetaspekt. I kap. 3.4.5.2 har jeg referert til Langheinrich, som diskuterer anonymitet som en løsning for å omgå problemer med å innhente samtykke, blant annet gjennom å bruke anonymiseringsproxy, eller ved å bare samle inn data som vanskelig kan identifiseres. Andre løsninger er diskutert for anonymisering av informasjon i rutere ved bruk av *mix-net* og *onion-routing* i kap. 4.1.2, spesielt som vern av førstehåndsinformasjon. En del av disse løsningene har imidlertid enorme transaksjonskostnader i systemet i form av prosessering for kryptering, kringkasting, og generering av data.

Andre forhold som spiller en rolle for sikkerheten er mulighetene for fysisk spredning, basert på prinsippet om lokale data. Begrenset fysisk rekkevidde i RFID brikker/kontaktløse smartkort begrenser mulighetene for spredning. PAWS,E-P3P og Confab forsøker også å bruke disse prinsippene ved å etablere personvernregler i avtalene som inngås for sletting av data når de kommer ut av området de er ment for. Her er man imidlertid igjen avhengig av at datainnsamlere er tilpasset slike rammerverk, og ikke beholder informasjon på tross av reglene.

5.1.2.5 Oppsummering om personvernkrav og løsningsmodeller

Jeg har analysert en rekke løsningsmodeller med bakgrunn i personvernkrav om kontroll/tilbakemelding, bruk av avtaler, transmisjonskostnader og sikkerhet. Disse har gitt god informasjon om de ulike systemene. I avsnitt 5.1.1 om avsløringsaspekter kom jeg fram til at den sosiale reguleringsprosessen er så godt som fraværende i automatiske datainnsamlingssystemer som Sporveiens. Mange av løsningsmodellene baserer seg på en

slik aktiv holdning fra bruker, og det er usikkert om prosessene for kontroll, meldinger, valg, og samtykke vil fungere særlig godt. Kanskje er det likevel nødvendig med innføring av varianter av noen av disse løsningene for å oppnå tillit hos brukere og få den lovpålagte samtykke til innsamling av data.

5.2 Autoritet, legitimitet og tillit

Sporveiens elektroniske system kommer til å bli brukt, og om det teknisk fungerer tilfredsstillende vil det sannsynligvis bli godt mottatt av de reisende. Dette vil skje, som i mange andre områder, uten at brukerne er spesielt bekymret over sine personlige opplysninger. Ut fra min forståelse av teorien har jeg kommet fram til at jeg kan kategorisere avsløring/deling av informasjon som en funksjon av mange andre aspekter som man kan finne i varierende grad i i de ulike systemene, som jeg har gjort i tabell 6. For å vurdere om avsløring kan foregå har jeg så diskutert mine fire personvernkrav i forbindelse med tabell 7. Disse tabellene og modellene er ganske omfattende . Vil det være mulig å re-konseptualisere hvordan brukere forholder seg til deling av informasjon på en ny og mer presis måte?

5.2.1 Hvordan oppstår tillit?

Deling av informasjon vil i de fleste tilfeller ha en forutsetning om tillit til den andre part. I sosiale prosesser "regulerer" vi denne tilliten i form av menneskelige relasjoner. I tekniske systemer velger vi på et tidspunkt å stole på systemet, og anse det som *trusted,* som i tilfellet med mobiltelefonsystemer, men også med tjenester på internett som vi velger å bruke, og sannsynligvis også med billettsystemer. Hvordan består denne tilliten av?

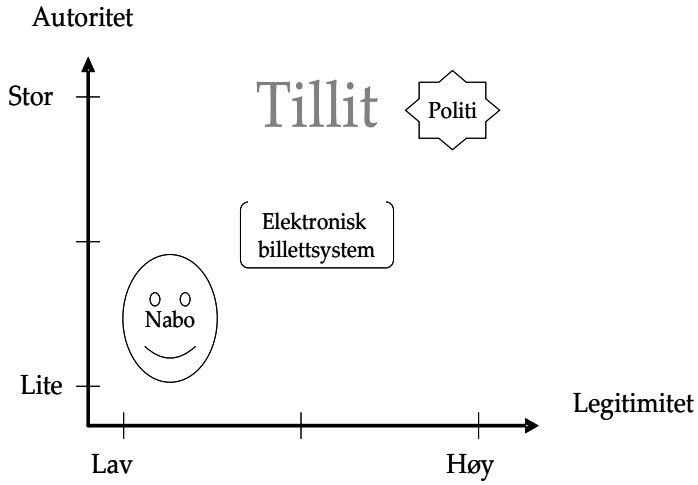
Kanskje er det mulig å dele tillit opp i to bestanddeler: ***autoritet*** og ***legitimitet.***

For å oppnå *autoritet* må en person eller et system være gitt et ansvar i forholdet til en person. Dette ansvaret kan være gitt av brukeren selv, av myndigheter, eller av andre institusjoner. I noen tilfeller vil ansvaret bestå i "å ta vare på " den enkelte, i form av å foreta seg handlinger som er til beste for oss. I sosiale relasjoner kan autoritet komme av et arbeidsforhold, slekt eller venner som man hører på, eller sosiale forventninger av hvem som har autoriteten i ulike situasjoner.

Handlingene som en stor eller liten autoritet foretar seg må imidlertid ha *legitimitet*, de må være forståelige i forhold til å oppnå et rettmessig formål. Legitimiteten kan også komme av at noen representerer oss på en god måte.

I illustrasjon 8 har jeg skissert noen eksempler på tillitsforhold som jeg vil forklare.

Samfunnet har opprettet institusjoner som for eksempel politi, som for



Illustrasjon 8: Tillit oppnås gjennom autoritet og legitimitet.

eksempel er gitt ansvar for å drive trafikkovervåking. Politiet har stor autoritet, ved at representerer "samfunnet", og formålet med trafikkovervåkingen er å begrense og redusere antall ulykker som skjer på grunn av råkjøring, samt sikre god framkommelighet. Vi liker ikke å bli tatt i radarkontroll, men er stort sett enige at handlingen er legitim, fordi formålet er godt. Det samme er som regel tilfelle ved telefonavlytting fra politiets side: Formålet er å fange kriminelle, til beste for samfunnet, altså oss alle, og politiet har høy tillit, og de fleste er villige til å svare på det meste politiet spør om.

I den andre enden av en slik skala finner vi kanskje naboen, som setter opp et overvåkingskamera i vinduet sitt for å finne ut om en person røyker i sin egen leilighet, eller i oppgangen. Et søkt eksempel, naturligvis, men det er åpenbart at naboen ikke har blitt gitt noe ansvar og autoritet for å kontrollere dette, og omtrent like lite har han et godt formål og legitimitet. Naboen får liten tillit om han gjør dette, og vi vil motsette oss denne overvåkingen.

Hva så i kommersielle situasjoner med automatisk datainnsamling? Mange av systemene vi i dag ser på som *trusted* kan passe inn under slike akser. I det fleste tilfeller vil vårt forhold til kommersielle aktører være preget av at disse selger noe vi vil ha, og dersom vi på en eller annen måte kan verifisere at varene finnes, kan aktøren gis autoritet som vare- eller tjenesteleverandør. I slike tilfeller er det også legitimt at vi får det vi betaler for, og fra aktørens side er det legitimt å kreve å få betaling. Tillit kan oppnås når begge har fått det de forventer. For mobiltelefonsystemer er det derfor legitimt at leverandøren samler inn informasjon om alle samtaler, nettopp for å vise at vi betaler for det vi skal. For brukeren er det sekundært at innsamling også må til for at tjenesten skal fungere. Tilliten eksisterer fordi tjenesteleverandøren leverer det han har lovet.

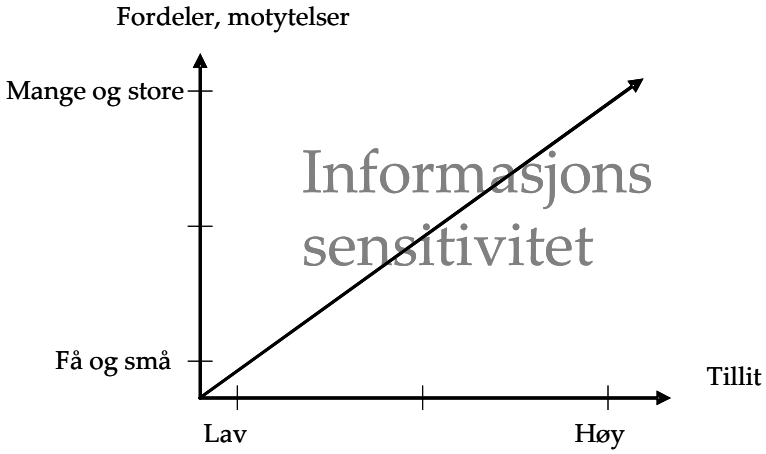
Kan man kan få tillit i forhold til innhenting av informasjon dersom man bare har autoritet eller bare legitimitet? Jeg tror at en tilstrekkelig autoritær aktør vil kunne få all slags informasjon, uten å måtte legitimere datainnsamlingen, og det er kanskje også grunnen til at *fair information practice* presiserer at informasjon bare kan samles inn for det formål det er tiltenkt i innsamlingsøyeblikket. På den andre side tror mange etterhvert vil gjennomskue og miste tillit til en autoritær aktør som samler inn unødvendig informasjon, da dette nettopp har preg av overvåking. Når det gjelder legitimitet tror jeg det er vanskelig å oppnå dette uten å først ha opparbeidet seg en viss autoritet.

Det finnes grader av tillit. Det er ikke alle man vil dele sine innerste tanker med, ei heller fødselsnummer og pin-koden til kredittkortet. Det kreves mindre tillit å få navn og adresse, vi anser dette i stor grad som offentlig informasjon. I mellom disse finnes mange nivåer, som inkluderer alt fra generell og uidentifiserbar informasjon til personlig identifiserbar informasjon om identitet, aktivitet og lokasjon. Vi gjør konstant vurderinger om hvilke opplysninger som kan deles, avhengig av autoritets- og legitimitetsforhold.

Naturligvis er det rom for tillitsbrudd i alle steder, og det er jo akkurat det at tilliten blir brutt ved å bruke informasjon annerledes enn forventet som skaper problemer for personvernet.

5.2.2 Informasjonsvaluta

For elektroniske billettsystemer bygger autoriteten på at man ønsker å transportere kunden trygt og effektivt fra et sted til et annet, og fordi dette er et offentlig samfunnsgode. Det er legitimt å ta betalt for tjenesten. Tilliten til dette systemet er sannsynligvis stor nok til at de fleste kunder også vil gi fra seg informasjon når de blir spurt om det.



Illustrasjon 9: Er villighet til å dele sensitiv informasjon avhengig av egne fordeler og tilliten til datainnsamleren?

Når tillit er tilstede er man villig til å utveksle informasjon, og gjerne mot motytelser. Kanskje kan man se på slik informasjonshandel med egen informasjon som deltagelse på en markedsplass, der man *er* villig til å gi fra seg mye informasjon, bare tilliten er stor nok, og motytelsene store nok. I en slik sammenheng stiller man med en *informasjonsvaluta*, i form av idenifiserbar og ikke identifiserbar informasjon, som kan brukes til å kjøpe og selge motytelser. Bellotti og Sellen(kap. 3.4.2) peker også på dette, men da mer fra et systemstandpunkt, der *awareness* systemet samler inn og overvåker alt og alle, så lenge fordelene for fellesskapet er store nok. De frykter sosiale sammenbrudd på bakgrunn av dette og gir derfor den enkelte kontroll i systemet. På en markedsplass tenker man imidlertid mest på seg selv. Jeg sier ikke at dette er uproblematisk, men dersom tillit er oppnådd gjennom at man føler at den andre parten vil "ta vare" på oss, representere oss, eller tilby gode tjenester og varer, vil vi også være villige til å handle med informasjon om oss selv. Vi føler at vi ikke har noe å frykte, fordi vi har tillit til systemet, og har derfor bare en sjelden gang behov for kontroll og tilbakemeldinger fra systemet. Jeg har prøvd å illustrere dette i illustrasjon 9.

På en markedsplass er det naturligvis mulig å bli lurt, og kjøpe en dårlig vare, ved at man ikke får det man betaler for, eller at man betaler mer enn den forventede prisen. I denne sammenheng kan dette være at informasjon blir spredt på en måte som ikke var forventet.

Brukere vil ta imot et elektronisk billettsystem, fordi slik billettering gjør reisen enklere for dem, og gir i alle fall følelsen av at alle må betale for seg, noe som er legitimt. Tilliten er kanskje også stor nok til å opprette et kundeforhold med Sporveien, de fleste mener de ikke har noe å skjule, og man vil få motytelser, kanskje i form av enda enklere reiser, mulighet for etterbetaling, automatisk oppdatering, og muligheter for å bruke billetten over et større geografisk område. Dette vil oppleves som *fordeler*, ikke som trussel mot personvernet.

5.2.3 Representasjon og tid

I forhold til min tabell 6 på side 93 tror jeg at informasjonsdeling i forhold til både sosiale forhold og i forhold til systemer kan passe inn i denne modellen. Om deling kan foregå avgjøres av om det foreligger et tillitsforhold, og hvilken informasjon som kan deles avhenger

av hvor stor tilliten er og hvilke motytelser det gis for å dele informasjon. Spredning ut over det som er intuitivt forventet eller eksplisitt oppgitt kan oppfattes som tillitsbrudd.

Hva så med tidsaspektet og mulighet for rekonstruksjon over tid? Dersom tillitsforholdet ikke endrer seg er rekonstruksjon ikke et problem, fordi deling av gammel og ny informasjon er en del av tillitsforholdet. Dette kan gjelde i sosiale relasjoner, så vel som i ensidige systemer der systemet er den eneste datainnsamleren. Så lenge en part opptrer som en representant for meg og vil mitt beste, og jeg har tillit til dette, deler jeg også informasjon med denne. Problemer kan oppstå dersom tillitsforholdet ender, og den andre parten etterpå sitter med detaljert informasjon. Det er ingen tvil om at dette kan være problematisk. På den andre side er dette gammel informasjon som oftest bare representerer bruddstykker av informasjon om et liv. Kanskje er ikke slik at gammel informasjon nødvendigvis så mye verdt lenger?

5.2.4 Teknologi og tillit

Hvilken rolle har så egentlig teknologi i denne modellen? For informasjonsdeling i datasystemer er sikkerhet og adgangskontroll svært viktig for at tillit til et system skal opprettholdes. Aktører som viser dårlig informasjonssikkerhet og dermed gir mulighet for uautorisert adgang til sine systemer kan risikere å miste autoritet, og dermed tillit, fordi man ikke tar vare på sine brukere på den forventede måte.

Teknologi brukes til å samle inn og lagre informasjon, men kan også brukes til å begrense hvilken informasjon som blir delt og lagret. Jeg har nevnt prinsippene om anonymitet og lokale data som eksempler på å unngå å bygge infrastrukturer som kan brukes til overvåking. Teknologi kan tilpasses til å anonymisere data som ellers kunne være identifiserbare, når man ikke har legitim grunn for å samle inn personlig identifiserbar informasjon. Ved å formidle dette kan man forbedre tilliten til aktøren og systemet, og brukeren vil gladelig dele informasjon der det er påkrevd.

Dessuten tror jeg som tidligere nevnt at avtaleinngåelse, gjennom personvernpolitikk og standarder som P3P, kan være med å ytterligere øke autoriteten og legitimiteten til datainnsamleren. Ved å fortelle hva man har tenkt å gjøre og hva man ikke har tenkt å gjøre med informasjonen øker man sin egen autoritet i forhold til at man ønsker å ta vare på brukeren, samt at man har mulighet til eksplisitt å legitimere den datainnsamlingen man gjør. De mulighetene som ligger for å tilby ulike valg av politikk og ikke minst samtykke, som *The Directive* [11] krever, kan også passe inn med at personer er villige til å avgi mer informasjon dersom de får motytelser, for eksempel i form av bedre tjenester.

5.3 Forslag til løsninger for Sporveien

Så langt har jeg presentert mine resultater fra gjennomgangen av teorier og teknologier, samt en egen modell for hvordan deling av informasjon foregår. Hva kan så Sporveiens billettsystem gjøre for å bedre situasjonen for sine reisende?

5.3.1 Tillitsbygging

Sporveien må bygge tillit ved å vise at de vil ta vare på sine kunder. De bør vise at de bare samler inn informasjon de trenger, og tilby motytelser for ekstra informasjonen de samler inn.

5.3.2 Pseudoanonymisering av reiser

Er det nødvendig å samle inn detaljert informasjon om alle reiser knyttet til hver enkelt billett og da også potensielt hver enkelt kunde? Hovedproblemet med systemet er såvidt jeg kan se *serieummeret* som blir registrert ved hver eneste reise. Det er denne som gjør systemet i stand til å rekonstruere reisemønster, samt å knytte kunden til en et serienummer på en billett. Langheinrich foreslår i sine personvernprinsipper å utvide bruken av anonymitet, eller pseudoanonymitet, ved hjelp av midlertidige identiteter (kap. 3.4.5.5). Spørsmålet er om det er mulig å få den nødvendige økonomiske integriteten ved å bruke pseudonym i transaksjonene, slik at det ikke var mulig å sette reiser i en billett sammen til et mønster, iallefall ikke uten å kunne lese loggen fra den fysiske billetten. I så tilfelle vil jo kunden ha full kontroll på denne informasjonen, på samme måte som ved "gammeldagse" papirbilletter, og det uten spesiell innsats fra kundens side i forhold til å måtte kontrollere informasjon.

5.3.3 Lokale data

Et annen mulighet er om det er mulig å anvende prinsippet om nærhet og lokale data. Hong og Landay har i sine brukerbehov , kap. 4.4.2.1, pekt på at begrenset lagring og replikering av data minsker mulighetene for å lage overvåkingssystemer. En måte å gjøre dette på er å la informasjon om billetter som ble registrert /validert på en stasjon/transportmiddel *bli værende* på dette stedet. Ansvar for eventuell kontroll av økonomiske transaksjoner kan gjøres lokalt, og eventuelle uoverenstemmelser på oppklares lokalt. Aggregerte data kan så formidles videre til det sentrale systemet, som fremdeles burde få tilstrekkelig data til å føre sine regnskap og planlegge trafikk gjennom denne informasjonen. Systemet ville også skalere bedre, da mindre informasjon trenger å bli kommunisert, og prosesseringen blir distribuert.

5.3.4 Opplæring i personvern. Inngåelse av personvernavtaler

I tillegg kunne man gjøre en innsats for å lære opp de reisende i personvern, ved å presentere oppslag og eventuelt dialoger om hvilke valg de faktisk har for de ulike billetter, og gjøre dette til en naturlig del av kjøpsprosessen. Dette vil være tillitsbyggende, og det vil være i tråd med *The Directive* å informere kundene om hva de samtykker til. Kanskje kunne man også benytte seg av systemer som P3P og kanskje en variant av PAWS, og gi kundene en referanse i sine billetter for hvilken personvernavtale de var registrert med. Denne kunne de kontrollere ved de distribuerte stasjonene. I tillegg kunne korte meldinger som fortalte hvilke typer informasjon som ble registrert gis som tilbakemelding ved validatorene. Ikke nødvendigvis fordi det er så nyttig, men for å opplyse om hva som skjer i systemet.

5.3.5 Internkontroll

Sist, men ikke minst må Sporveien ha et system for internkontroll for hvordan data blir brukt og delt i systemet, i tråd med kundenes avtaler og tilliten kundene har gitt dem. Dette gjelder spesielt for informasjonen som er knyttet til kundeavtaler, samt betalingsinformasjon av alle slag. Dette har naturligvis innvirkning på transaksjonskostnadene, men sensitiv informasjon må behandles ansvarlig, og dette må man forsikre kundene, seg selv, og myndigheter om.

5.4 Teoretiske følger

Som jeg har påpekt kan det se ut som om sosiale teorier for "utpakking" av personvern må utvikles videre for situasjoner der man bare forholder seg til systemer, og det ikke finnes noen sosial prosess. Det kan se ut som teorien er underspesifisert på dette området. Det kan også se ut som designprinsipper utviklet spesielt innenfor *awareness*- miljøer passer best nettopp innenfor slike systemer, men egner seg mindre godt i andre systemer.

Jeg har presentert en modell som kan brukes for å belyse hvordan mennesker oppnår tillitsforhold, også med systemer som driver ensidig automatisk datainnsamling. Kanskje kan denne modellen brukes for å utvikle teorier for hvordan den videre "utpakking" av personvern kan skje for nye, allestedsnærværende infrastrukturer som vil dukke opp.

5.5 Generaliseringer av resultat

Er det mulig å si mer overordnet om resultatene jeg så langt har kommet fram til omkring teknologi og personvern? Som jeg nevnte alt i kap. 1.3.2 er det mulig at vi så langt har lett etter teknologiske løsninger på noe som ikke egentlig er et teknisk problem. Vår skepsis og mangel på tillit til systemer blir vel egentlig ikke mindre av å innføre *mer* teknologi som skal forholde seg til det samme systemet?

5.5.1 Teori omkring tillit og informasjonsvaluta

I min diskusjon i kap. 5.2 diskuterte jeg hvordan man for all deling av informasjon er avhengig av tillit. Ved liten tillit deles ingen eller lite informasjon. Jeg har argumentert for at tillit bygges gjennom å oppnå eller få autoritet i forhold til en bruker, samtidig som man har legitimitet i sin innsamling av informasjon, blant annet ved å bare samle inn det man trenger av informasjon, og ikke mye mer. Det kan også se ut som store fordeler og motytelser kan kompensere for liten tillit, men da med øket risiko. Den enkelte gjør konstant slike vurderinger om man har tillit til den andre part, og hvilke fordeler man kan hente ut fra å dele informasjon.

Jeg har beskrevet denne modellen generelt, som et forsøk på å beskrive hvordan jeg tror informasjonsdeling faktisk foregår, istedet for hvordan den burde foregå. Jeg tror imidlertid at modellen kan være til hjelp for nye systemer som vil oppnå tillit, og dermed akseptans og bruk. Jeg tror også at brukere kan komme til å kreve mer av sin *informasjonsvaluta,* i form av bedre motytelser for å gi fra seg informasjon. Problemene vi allerede har omkring uønsket spredning av informasjon kan også føre til at brukere vil være mer forsiktig med hva de sprer av informasjon. Å oppnå tillit vil derfor være essensielt for den som vil samle inn informasjon.

5.5.2 Opplæring om personvern og innføring av reelle valg

Hva kan man så gjøre for å oppnå tillit? Jeg tror at *informasjonst*eknologi kan fungere som *opplæring* for tema innen personvern. Personvernpraksis i systemer er fremdeles ofte godt skjult for oss, enten i form av vanskelig tilgjengelig informasjon, vanskelig juridisk språk, eller ignorering av problemet fra både bruker og datainnsamlerens side. Da kan det være at

en automatisering og standardisering i presentasjon kan være med på å framstille hvilken informasjon som samles inn og hvordan denne brukes på en god og forståelig måte. Det må imidlertid fremdeles være brukers ansvar å samtykke. Jeg har pekt på at slik kontraktinngåelse er med å skape tillit. Ytterligere tillit kan skapes ved at brukeren får litt av kontrollen gjennom å gis reelle valg for datainnsamlingen, og dermed settes i en viss forhandlingsposisjon i forhold til legitimiteten til datainnsamlingen, og hvilke motytelser han kan vente seg.

5.5.3 Kommersielle behov

I mange situasjoner vil flere interesser i forhold til datainnsamlingen stå mot hverandre. I noen tilfeller kan det være næringslivets behov for å drive markedsføring som står opp mot kundenes behov for selv å bestemme om man er interessert i slik kontakt. Slik det fungerer i mange systemer i dag, eksempelvis telefonsalg i Norge, er man interessert så lenge man ikke eksplisitt har meldt fra til Brønnøysund om at man ikke er interessert. Vil vi fortsette å finne oss i slike ordninger?

Jeg tror at en av årsakene til at standarder for å formidle personvernpolitikk (P3P) har fått så liten utbredelse er at mange bedrifter, også seriøse, ikke *ønsker* å presentere hvilken informasjonspraksis de faktisk har. Dette betyr nemlig at de åpent må detaljere dette på en slik måte at kunden enkelt kan få oversikt, og bedriften kan bli gjort ansvarlige for avvik. Ei heller ønsker de å tilby politikk som medfører at man risikerer å samle inn *mindre* informasjon enn dagens situasjon gir dem. De satser altså på å bygge tillit på andre måter, uten å gi kunden mulighet for å forvalte son informasjonsvaluta. Kanskje vil en slik utvikling først skje når/dersom det blir et kundekrav om å få vite hva som skjer med informasjon om dem, eller de ønsker å å få mer igjen for informasjonen de deler. For at det igjen skal kunne skje må man kanskje plage brukere litt for å lære dem opp i hvilke valgmuligheter de bør ha i forhold til personvern.

5.5.4 Samfunnets behov

Andre interessekonflikter når det gjelder valg for datainnsamling er at samfunnets behov kan komme opp mot brukerens behov. I mange tilfeller vil det være ønskelig for mennesker med uærlige hensikter å unngå å bli registrert i de elektroniske transaksjoner de gjør, mens samfunnets interesser er å kunne spore dette i ettertid. Derfor er det ikke mulig å alltid kunne gi anonyme alternativer der ingen informasjon blir lagret i systemet. Likevel er det et spørsmål om vi ønsker flere infrastrukturer der det er mulig å gjøre slik sporing. Man kan anta at jo flere infrastrukturer som holder detaljert informasjon, jo flere muligheter er det for også andre enn myndighetene å spore personer uten at de vet om det, med eller uten rettslige kjennelser. Igjen er det derfor viktig at brukerne har den nødvendige tillit til systemet, og at systemet forholder seg til oppgavene de legitimt kan gjøre til beste for individet og samfunnet.

Hong og Landay (kap. 4.4.2.1) argumenterer for et brukerbehov som krever færre muligheter for misbruk. Å tilby anonymisering og å begrense sentralisering av informasjon som kan muliggjøre kryss-søk, er mulige løsninger på dette problemet.

Jeg har påpekt at den sosiale kontrollen og tilbakemeldingen som finnes i for eksempel *awareness* systemer er fraværende i mange andre systemer for automatisk innsamling. Mange slike systemer fungerer som en forenkling eller gir brukeren fordeler i forhold til en annen tjeneste, og det er disse tjenestene man er interessert i, ikke datainnsamlingssystemet. Dette er for eksempel tilfellet med billettsystemer, der formålet er en enklere og mer pålitelig reise, ikke sosial deling av informasjon. Brukeren er ofte interessert i å stole på systemet, og vil mest sannsynlig ikke være interessert i direkte innsikt og kontroll eller særlige mengder av tilbakemeldinger fra innsamlingssystemet. Datainnsamleren vil heller ikke ha særlig interesse av dette, selv om datainnsamleren er påbudt å gi brukere tilgang til egen informasjon. I de fleste situasjoner vil han være best tjent med at brukeren har tillit til ham, og han burde av den grunn ikke misbruke denne tilliten. Avtaleinngåelser kan bli *spesielt* viktig i slike systemer. Gjennom avtaler kan man gi brukere visse valg og ikke minst en juridisk middel for represalier dersom brudd på avtalen finner sted.

5.5.5 Standardisering og innovasjon

Transaksjonskostnadene ved slike kontroll- og avtale-systemer gjerne kan bli store, og jeg tror ikke vi enda har sett noen teknologi som virkelig lar seg operasjonalisere. På dette punktet står arbeidet med å standardisere opp mot ønsker om innovasjon. Confab systemet er et eksempel i så måte, ved at man presenterer et system som forbedrer konseptene som også er brukt i P3P standarden, men uten å forholde seg til for eksempel syntaks, selv om innholdet er mye av det samme. En del av løsningsforslagene som baserer seg på avtaler og regler bærer preg av å være prototyper, og forutsetter at de fleste eller alle forholder seg til deres rammeverk, eller at det alltid er mulig å komme til enighet om en politikk.

Etter mitt syn er det er lite trolig at slike rammeverk vil få noen særlig utbredelse. Først og fremst tror jeg dette fordi personvern ikke er et spesielt teknologisk spørsmål, men et spørsmål om tillit. Dersom tilliten ikke er til stede, eller en datainnsamler ikke er tilliten verdig, vil det heller ikke fungere med rammeverk som krever at man strengt følger et rammeverk som implementerer personvernregler.

Rammeverkene setter også krav til en kontroll og innsikt som de færreste er i stand til eller er interessert i å administrere. Noen av tankene og konseptene er likevel gode, og kan kanskje brukes i noen domener.

I forhold til standardisering har P3P sine helt klare svakheter, spesielt i måten man presenterer ulike valg, og gir mulighet for *opt-in* og *opt-out* , som virker tungvint, og er åpenbart mest tilpasset innsamlernes ønsker om å samle inn mest mulig informasjon. Dessuten er denne standarden like hierarkisk som alle andre XML dokumenter, og dette setter begrensninger for hvor denne kan evalueres i form av prosesseringskrav. Likevel er utbredelse og opplæring innen avtaler, valg og samtykke avhengig av at standarder som P3P opprettes og brukes. De kan selvsagt også utvides etterhvert.

5.5.6 Konvergens

Et annet spørsmål er også om det virkelig er en konvergens av teknologier som finner sted. Både når det gjelder avsløringsaspekter (tabell 6) og i forhold til personvernkrav (tabell 7) ser

det ut som flere av teknologiene fremdeles er svært ulike. Det finnes en del fellestrekk, men kanskje er tendensen heller at ulike teknologier *integreres* i de samme tekniske enheter, som så benyttes på flere forskjellige måter, altså ikke på en konvergent måte. En telefonsamtale vil fremdeles være noe annet enn betaling av kollektivbillett, selv om billetten skulle være innebygd i SIM-kortet.

5.5.7 Kan eksisterende konsepter og systemer for personvern fortsatt brukes?

Mitt formål med denne oppgaven var å finne ut om "de eksisterende konsepter og systemer for personvern fortsatt kan brukes når det ser ut som teknologiene konvergerer"

Mitt svar på dette spørsmålet er at konseptene og systemene ser ut til å fungere best i de domenene der de ble utviklet. Selv om en del av konseptene er gode, vil de ofte ikke kunne brukes, fordi den nye teknologien har en ny, eller kanskje manglende sosial bruk i forhold til situasjonen der konseptene og systemene ble utviklet.

Noen teknikker, som sikkerhetsalgoritmer, lar seg bruke i mange domener, men kommer ofte i konflikt med begrensede ressurser i mange nye enheter. Dessuten vil sikkerhetskrav for dataintegritet av og til komme i konflikt med krav om anonymitet.

Det ser ut som nye personvernkonsepter, hovedsaklig basert på tillit, må utvikles når nye infrastrukturer utvikles. Brukere vil kanskje ønske å få mer ut av sin *informasjonsvaluta* i form av motytelser for å gi fra seg informasjon.

5.6 Resultater i forhold til metode

Som nevnt i metodekapittelet 1.5 gjorde jeg først en *survey* av teorien og noen av løsningsmodellene som jeg har presentert i denne oppgaven.

Under arbeidet med å hente inn forskningsbakgrunnen om Sporveiens Elektroniske billettsystem tok jeg utgangspunkt i Bellotti og Sellens designspørsmål fra kap. 3.4.2 for å stille spørsmål om billettsystemet.

Min erfaring med disse spørsmålene er at de avdekker viktige personvernaspekt ved systemet. Min kontaktperson gjorde seg flid med å svare på spørsmålene i en ellers travel hverdag, og en av årsakene kan være at spørsmålene var fokuserte og gode.

For noen av spørsmålene fikk jeg som svar at disse spørsmålene var "ikke avklart". Dette var spesielt spørsmålene som gikk på intern bruk av informasjonen sentralt i Sporveiens system. Det kan være at svarene var slik fordi spørsmålene var tidkrevende ¨svare på, eller fordi systemet er langt unna ferdigstillelse, selv om det etter årsmeldingen fra 2003 skal innføres i løpet av 2005. Uten å spekulere for mye i dette kan det også være at intern bruk ikke har vært et prioritert tema. Det burde det kanskje være. Det at jeg ikke fikk svar på disse områder antyder kanskje at man ikke er svært bekymret for hvordan den interne bruken vil påvirke de reisendes tillit til systemet.

Ut fra den teoretiske bakgrunn og scenario definerte jeg fire personvernkrav som jeg brukte til å strukturere og analysere teori og løsningsforslag på nytt. Det første kravet var mulighet for kontroll og tilbakemelding inkludert mulighet for å gjøre ulike valg og i å gi samtykke. Det andre var om det ble inngått implisitte eller eksplisitte avtaler. Det tredje gikk på

transaksjonskostnader for brukeren i form av vanskelighetsgrad og behov for innsikt i systemet, og på den andre side hvilke behov for prosessering og muligheter for skalering løsningene har i tjenestetilbyders system. Det fjerde og siste punktet var hvordan modellene forholdt seg til ulike sikkerhetsaspekter som en del av sine modeller for personvern.

Med et annet scenario og med annen teori kunne denne fremgangsmåten og kravene naturligvis blitt annerledes, men jeg vil påstå at det å belyse teoriene og løsninger med disse kravene har fungert. Et av aspektene kom direkte ut fra Bellotti og Sellens [5] designprinsipper, med forventning om at siden spørsmålene var gode, var kanskje også løsningene deres gode. Mine resultater er imidlertid at kontroll og tilbakemelding ikke fungerer særlig godt å bruke på en stor gruppe automatiske datainnsamlingssystemer.

Som jeg nevnte i metodekapittelet er det mange systemer som på mange måter ligner på billettsystemer. Systemene vi "tradisjonelt" ser på som *trusted* er ikke så mange: Bank, forsikring, ligningsmyndigheter, telefon og kanskje noen få andre. Jeg mener det er mening i å spørre om vi automatisk skal få tillit til alle andre som utfører automatisk innsamling? (Som parkeringsselskaper, flyselskaper, biblioteker, bonussystemer, bomringsystemer, RFID tags i klær, i tillegg til billettsystemer).Det kan være at disse må fortjene tillit på andre måter.

Jeg har presentert en teoretisk modell for hvordan tillit oppnås som et resultat av et system eller en persons autoritet og legitimitet i forhold til innsamlingen eller overvåking han foretar seg. Dersom det foreligger tillit vil personer dele informasjon, og kanskje også *mer* informasjon, dersom det gis motytelser.

Jeg tror derfor at for at nye systemer skal bli brukt må de oppnå tilstrekkelig og rettmessig tillit hos sine brukere, samtidig som de tilbyr store nok fordeler for brukeren selv. Om det virkelig er slik har det ikke vært metodisk mulig å undersøke innenfor oppgavens omfang, og dette må eventuelt overlates til videre forskning.

5.7 Videre arbeid

Av videre arbeid bør man kontrollere om mine resultater i forhold til mangelen på en sosial prosess og forholdet til personvernkravene stemmer også for andre automatiske datainnsamlere enn Sporveiens Elektroniske billettsystem.

Spesielt bør man også finne ut om det er fruktbart å definere tillit som et resultat av systemers og personers autoritet og legitimitet i andre mulige sosiale- og system-relasjoner.

Det bør utvikles en metodikk for å lære brukere opp i sine personvernkrav, slik at disse kan presenteres, velges og kontrolleres på en enkel måte. For P3P sin del bør bedre mekanismer for valg enn *opt-in* og *opt-out* mekanismer utvikles. Dessuten bør selvfølgelig klientprogramvare støtte personvernpolitikk på en slik måte at brukere blir opptatt av dette. Man bør også se om det er mulig å utvikle enklere systemer for kontroll av at personvern-avtaler blir overholdt, for dermed å tilby akseptable transaksjonskostnader for datainnsamler.

Konkret for billettsystemer må man finne ut om det er mulig å tilby økonomisk transaksjonsintegritet ved å bruke pseudoidentifikasjon i stedet for serienummer i billetten. I denne sammenheng bør det også undersøkes om en slik anonymisering kan bedre tilliten også til andre systemer, og om anonymisering kan få en mer fremtredende rolle, for eksempel som et gyldig alternativ i forhold til avtaleinngåelser.

6 Konklusjon

Vi har i denne oppgaven sett at utviklingen av strukturer for allestedsnærværende automatisk datainnsamling setter nytt fokus på hvordan vi forholder oss til eksisterende systemer som gjør dette. Ulike teorier og designmodeller eksisterer for hvordan informasjonsutveksling foregår. De fleste av disse baserer seg på at det eksisterer en sosial prosess der man ønsker og er i stand til å regulere hvilken personlig informasjon som deles.

Jeg har analysert eksisterende systemer i forhold til fire personvernkrav jeg har satt opp ut fra teorien og mitt scenario: kontroll og tilbakemelding, avtaler, lave transaksjonskostnader og sikkerhet. Gjennom denne analysen har jeg kommet fram til at den sosiale prosessen for regulering av hvilken informasjon som avsløres for enkeltbrukere *ikke* er til stede i mange av systemene med automatisk datainnsamling. Jeg har derfor kommet fram til at det må være andre mekanismer som gjør at vi likevel er mer enn villige til å dele informasjon med mange slike systemer.

Jeg har presentert en modell som går ut på at all informasjonsutveksling baserer seg på tillitsforhold, som oppnås gjennom autoritet og legitimitet i forhold til datainnsamlingen i de enkelte situasjoner. Tilliten bygger på at systemene tilbyr noe vi vil ha, enten i form av varer og tjenester, eller i form av være en autoritativ representant, der datainnsamlingen er legitim i forhold til formålet. Vi er villige til å dele informasjon, og spesielt dersom vi kan få motytelser, men et visst nivå av tillit er nødvendig for at dette skal kunne skje.

I denne modellen ligger også at personvern ikke er et utpreget teknisk problem. Teknologi kan imidlertid hjelpe til ved å tilby sikkerhet for informasjonsutvekslingen, som er med på å bygge opp tilliten. Nye tekniske standarder for å formidle personvernpolitikk kan være med å legitimere datainnsamlingen som blir gjort, og gi datainnsamler autoritet. Datainnsamler blir dermed gjort ansvarlig for å behandle informasjonen slik han har lovet. På den andre siden kan brukeren bli mer oppmerksom på hvilke motytelser han kan og bør kreve for å dele av sin *informasjonsvaluta*.

Bibliografi

1: Auto-ID Center - USMassachusetts Institute of Technology, 'AutoID RFID Technology Guide', AutoID Center, http://archive.epcglobalinc.org/new_media/brochures/Technology_Guide.pdf, sett nov 2004
2: S. E. Sarma, S. A. Weis, and D.W. Engels., 'RFID Systems and Security and Privacy Implications', Cryptographic Hardware and Embedded Systems - CHES 2002: 4th International Workshop Redwood Shores, 454 - 469, Springer-Verlag, LNCS no. 2523, 2002
3: Finkenzeller, K, 'RFID-Handbook, 2nd Edition',Wiley & Sons LTD,2003
4: Andreas Görlach, Andreas Heinemann, and Wesley W. Terpstra, 'Survey on Location Privacy in Pervasive Computing', Proceedings of Conference of SPCC, Springerlink, LNCS, 2004
5: Bellotti, V & Sellen, A, 'Design for Privacy in ubiquitous computing environments', Proceedings of the 3rd European Conference of CSCW - ECSCW'93, 77-92, Dordrecht:Kluwer, 1993
6: Palen,Leysia;Dourish,Paul, 'Unpacking "privacy" for a networked world', Proceedings on Human factors in comp. systems, 129 - 136, ACM Press, 2003
7: O'Neill,Eamonn ; Woodgate, Dawn ; Kostakos, Vassilis, 'Easing the wait in the emergency room:Building a theory of public info.syst', Proceedings of Conference of DIS2004, 17-25, ACM Press, 2004
8: Liechti, Olivier, 'Awareness and the WWW: An Overview', ACM SIGGROUP Bulletin, 3-12, ACM Press, 2000
9: Gutwin,Carl; Greenberg,Saul, 'A descriptive framework of workspace awareness for real-time groupware', 411-446, Kluwer Academic Publishers, 2002
10: , 'Fair Information practices. Sett nov 2004', http://www3.ftc.gov/reports/privacy3/fairinfo.htm, 1974
11: The European Parliament And Of The Council, 'The Data Protection Directive, sett nov 2004', http://www.dataprivacy.ie/6aii.htm, 1995
12: Norges Lover, 'Personopplsningsloven', Lovdata, http://www.lovdata.no/all/hl-20000414-031.html,
13: Datatilsynet, 'Datatilsynets hjemmesider', Datatilsynet, http://www.datatilsynet.no/
14: L. Cranor,M. Langheinrich, M. Marchiori,M. Presler-Marshall, and J. Reagle, 'The Platform for Privacy Preferences 1.0 (P3P1.0) Specifcation', W3C, http://www.w3.org/TR/P3P/, April 2002
15: L. Cranor,M. Langheinrich, M. Marchiori,M. Presler-Marshall,M. Marchiori, 'A P3P reference exchange language 1.0 (APPEL 1.0)', W3C, http:\\www.w3c.org/TR/P3P-preferences, April 2002
16: Langheinrich, M, 'Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems', Lecture Notes in Computer Science, 273-291, Springer, 2001
17: Langheinrich, M, 'A Privacy Awareness System for Ubiquitous Computing Environments', Lecture Notes in Computer Science, 237-245, Springer, 2002
18: Cranor, Lorrie F; Arjula, Manjula; Guduru, Praveen, 'Use of a P3P User Agent by early adopters', Workshop on Privacy in the Electronic Society, ACM, 2002
19: Karjoth, Günter; Schunter, Matthias; Waidner, Michael, 'Platform for E-P3P:Privacy-Enabled Management of Customer Data', Lecture Notes in Computer Science, 69-84, Springer-Verlag, 2003
20: Bohrer, Kathy; Levy, Stephen, Liu, Xuan, Schonberg, Edith, 'Individualized privacy policy based access control', Proceedings of the 6th International Conference in Electronic Commerce Research,

IBM, 2003
21: Couloris, George; Dollimore Jean; Kindberg, Tim, Security, 'Distributes systems, Concepts and design, 3rd edition',Addison Wesley,2001
22: Kong, J; Hong, X, 'ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-Hoc networks', Proceedings of the 4th ACM interna-tional symposium on Mobile ad hoc networking & computing, 291-302, ACM Press, 2003
23: M. Gruteser and D. Grunwald., 'Anonymous Usage of Location-Based ServicesThrough Spatial and Temporal Cloaking', MobiSys, USENIX, 31-42, 2003
24: Chaum,D, 'Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms', Communications of the ACM, 24,84-88,1981
25: Federrath,H; Jerichow,A; Pfitzmann.A, MIXes in Mobile CommunicationSystems: Location Management with Privacy, 'Information Hiding', 121-135,, 1996
26: H. Federrath and J. Thees., 'Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern', Datenschutz und Datensicherung, 338-348, Verlag Vieweg, 1995
27: A. R. Beresford and F. Stajano, 'Location Privacy in Pervasive Computing', PERVASIVE computing, IEEE CS and IEEE Communications Society, 46-55, 2003
28: A. Juels, R. L. Rivest, and M. Szydlo, 'The Blocker Tag: Selective Blocking of RFIDTags for Consumer Privacy', V. Atluri, ed. 8th ACM Conference on Computerand Communications Security, 103-111, ACM Press,
29: S. E. Sarma, S. A. Weis, and D.W. Engels, 'RFIDsystems, security and privacy implications. TechnicalReport MIT-AUTOID-WH-014', AutoID Center, MIT,2002
30: Katherine M. Shelfer; J. Drew Procaccino, 'Smart card evolution', Communications of the ACM, vol 45, issue 7, 83-88, 2002
31: Tisal, Joachim, 'The GSM Network. GPRS Evolution: One Step Towards UMTS. Second Edition', Wiley,2001
32: Palen,L Salzman, M and Youngs, E, 'Going Wireless: Behaviour & Practice of new mobile phone users', Proceedings of Conference on CSCW(Philadelphia Dec 2-6), 201-210, ACM Press, 2000
33: Ljungstrand, Peter, 'Context awareness and Mobile Phones', Proceedings on Conference in Personal and Ubquitous Computing, 5:58-61, Springer-Verlag, 2001
34: Stuart J. Barnes; Sid L. Huff, 'Rising sun: iMode and the wireless Internet', Communications of the ACM vol 46, issue 11, 78-84, ACM Press, 2003
35: Snekkenes,Einar, 'Concepts for Location Privacy Policies', Proceedings of the 3rd ACM Conference in Electronical Commerce, 48-57, ACM Press, 2001
36: Hong, Jason I.; Landay, James A., 'An Architecture for Privacy Sensitive ubiquitous computing', Proceedings of Conference ofMobiSys'04, 177-189, ACM, 2004
37: NSB, 'NSB Årsrapport 2003', http://ar2003.nsb.no/konsern/viktige_hendelser/, 2003
38: Vegdirektoratet, 'Elektronisk Billettering 206-1', Statens Vegvesen, http://www.vegvesen.no/fakta/publikasjoner/pdf/elektroniskbillettering/, 2004
39: AS Oslo Sporveien, 'Sporveiens årsrapport for 2003', www.sporveien.no, http://www2.oslosporveier.no/arsrapporten-2003/, 2003
40: Dourish, P. and S. Bly., 'Portholes: Supporting Awareness in a Distributed Work Group.', proceedingsof the ACM SIGCHI Conference on Human Factors inComputing Systems (CHI'92), , ACM Press., 1992
41: Grinter, Rebecca E; Palen, Leysia, 'Instant Messaging in Teen Life', Proceedings of Conference of

CSCW 2002, 21-30, ACM, 2002
42: Reynolds, Carson; Picard,Rosalind, 'Affective sensors, privacy and ethical contracts', Proceedings of Conference in Computer Human Interactions 2004, 1103-1106, ACM, 2004
43: I. A. Getting., 'The Global Positioning System.', EEE Spectrum, 30(12),36-47, 1993
44: N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, 'The Cricket Location-Support System', Mobile Computing and Networking,32-43,2000
45: Internet Mail Consortium, 'vCard-The Electronic business Card Version 2.1', Sept. 18. 1996
46: Gamma, Helm, Johnson, Vlissides; 'Composite pattern', i 'Design Patterns: Elements of reusable object-oriented design', 163-173, Addison-Wesley, 1995
47: R. Want, A. Hopper, V. Falcao, and J. Gibbons., 'The Active Badge Location System', ACM Transactions on Information Systems, 91-102, 1992

Tabeller

Illustrasjoner