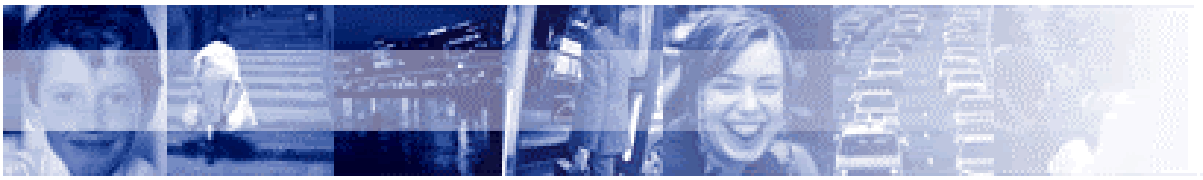
PRISE
privacy • security

Security Research

PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security Research



Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

Dansk rapport fra borgermøde om sikkerhedsteknologi og privatlivets fred

Due date of deliverable:
Actual submission date:

Start date of Activity: 1 February 2006 Duration: 28 month

Author(s):
Anders Jacobi, The Danish Board of Technology
Mikkel Holst, The Danish Board of Technology

Classification: PU

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment, Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Germany
Contact: Marit Hansen
prise@datenschutzzentrum.de
www.datenschutzzentrum.de

Indhold **side**

Indledning

Onsdag den 30. maj afholdt Teknologirådet et såkaldt borgermøde på DSB's konferencecenter på Østerport Station i København.

28 deltagere hørte foredrag, udfyldte et spørgeskema og debatterede nye sikkerhedsteknologier og disse teknologiers indgreb i privatlivets fred. I dagene efter blev lignende møder afholdt i Tyskland, Norge, Østrig, Spanien og Ungarn.

Rapportens formål

Borgermøder er et af de centrale elementer i PRISE – et forskningsprojekt finansieret af Europa-kommissionen. PRISE vil bidrage med retningslinier og støtte til udviklingen af sikkerhedsløsninger med særligt fokus på menneskerettigheder, menneskelig adfærd og opfattelse af sikkerhed og privatliv.

Nærværende rapport opsummerer holdninger og argumenter, der blev præsenteret på det danske borgermøde.

Udvælgelse af mødedeltagere

Deltagergruppen blev sammensat så differentieret som muligt. Først blev 2000 invitationer sendt ud til tilfældigt udvalgte personer i alderen 18-75 år, der makismalt boede tre kvarters kørsel fra Østerport. Af de positive tilbagemeldinger udvalgtes 36 personer på baggrund af køn, alder og uddannelsesniveau. Ikke alle, der havde tilmeldt sig, dukkede op til mødet, så selvom de udvalgte havde den tilstræbte fordeling på køn og alder, var der en underrepræsentation af kortere uddannelser og en tilsvarende overrepræsentation af mellemlange og lange uddannelser. En mere detaljeret gennemgang af gruppens sammensætning kan findes i bilag 1.

I den endelige gruppe kunne man møde folk med mange forskellige baggrunde; der var bl.a. en tidligere fængselsbetjent, en designer, en portør, studerende og civilingeniører.

Offentlig debat inden mødet

Der havde ikke været nogen særlig pressedækning eller offentlig debat om sikkerhedsteknologi i ugerne inden mødet. Størst omtale fik en undersøgelse foretaget af Epinion Capacent, der hævdede, at danskerne var særligt glade for tv-overvågning (se *Ritzau*: "Danskerne er vilde med overvågning" 10/5-07). Undersøgelsen blev debatteret i flere aviser, bl.a. i *Politiken* 25/5.
Et par emner relateret til mødet, som ikke tidligere havde været debatteret i medierne, fik en smule pressedækning – navnlig overvågning af private foretaget af private (f.eks. i *Urban* 16/5 og *Nyhedsavisen* 30/5) og øget offentligt ansvar for borgernes sikkerhed som følge af nye teknologiske muligheder (*Ritzau* 16/5).

Da ingen af de ovenstående emner medførte større offentlig debat, synes pressedækningen kun at have haft marginal indflydelse på de holdninger og argumenter, der blev præsenteret på mødet.

Sammenfatning

Hvad der betragtes som privat ændrer sig afhængigt af situationen. Privatlivets fred er tæt forbundet med tillid til brugen af og effekten af sikkerhedsteknologierne.

Mødedeltagerne faldt i to grupper: Et lille flertal følte sig ikke trygge ved nye sikkerhedsteknologier og prioriterede beskyttelse af privatlivet højt, mens et mindretal var langt mere positivt indstillet overfor de nye teknologier. Samtidig mente de fleste af deltagerne, at udviklingen af nye sikkerhedsteknologier er nødvendig, og de mente at teknologiernes er brugbare i forebyggelse og efterforskning af terror og anden kriminalitet.

Den kritiske majoritet af deltagerne stillede spørgsmålstegn ved den reelle effekt af de nye teknologier – de forventede, at kriminelle vil være i stand til at omgå eller misbruge teknologierne. De forventede også, at en række af teknologierne ikke vil nedbringe kriminalitet, men i stedet vil flytte den andre steder hen.

Spørgsmålet om teknologiernes effektivitet er også et spørgsmål om tillid til de institutioner, der forvalter teknologierne. En del af gruppen gav udtryk for, at sikkerhedsteknologier primært skal give borgerne en følelse af tryghed og derfor er politiske instrumenter uden reel effekt. Flertallet forventede desuden, at det offentlige vil misbruge teknologierne og udtrykte frygt for, at privatlivets fred vil blive krænket af de personer, der kontrollerer teknologierne i det daglige.

Det er interessant at bemærke, at et stort flertal i gruppen ikke er villige til at acceptere negative konsekvenser for folk, der enten ikke er i stand til eller ikke ønsker at benytte nye sikkerhedsteknologier. Hvis flertallet accepterer at sikkerhedsteknologierne skal være frivillige eller kan omgås, så forringes effekten af visse teknologier, så som registrering af data, lokaliserings- og skanningsteknologier.

1.1 Privatsfærens grænser

Omfanget af privatsfæren bestemmes af mindst fire elementer: a) Den nøgne krop er privat og må ikke eksponeres. b) Folk føler ubehag ved teknologier, der indsamler data, der gør brugerne af teknologien i stand til genkende eller rekonstruere folks identitet og baggrund. c) Visse lokaliteter opfattes som mindre private og er derfor bedre egnet til nye sikkerhedsteknologier. d) Visse former for kriminalitet betragtes ikke som alvorlig, og bør ikke være mål for nye sikkerhedsteknologier. F.eks. var deltagerne meget skeptiske overfor automatisk hastighedskontrol.

1.2 Anbefalinger

Der var næsten konsensus om behovet for grundig demokratisk evaluering af nye sikkerhedsteknologier før de bliver implementeret. Menneskerettighedsorganisationer og til en hvis udstrækning udviklerne af teknologier bør deltage i debatten. Endelige beslutninger skal træffes af politikere.

Der bør blive lagt større vægt på at forske i teknologiernes effekt, og deres indflydelse på privatlivets fred og i udviklingen af lavteknologiske alternativer. Det er nødvendigt at regulere både udviklingen og brugen af nye sikkerhedsteknologier.

Kapitel 2 Generel holdning

2.1 Deltagernes generelle holdning

”Hvis man ikke har noget at skjule, behøver man heller ikke at være bekymret over de sikkerhedsteknologier, der krænker privatlivets fred”. Således lød et af de udsagn, som deltagerne blev konfronteret med i det uddelte spørgeskema. Responsen på dette udsagn viste sig at være særdeles sigende for deltagernes generelle holdning. Gruppen var delt i deres holdning – et lille flertal frygtede for privatlivets fred (ud af de 27 deltagere, var 11 helt eller delvist enige, 2 var hverken enige eller uenige og 14 var delvist eller helt uenige i udsagnet). Opdelingen i en mindre teknologi-optimistisk gruppe og i en større privatlivsbekymret gruppe prægede gennemgående debatten.

De teknologi-optimistiske deltagere havde ingen problemer med overvågning og registrering:

> *Jeg har undret mig over, at man går ud fra, at der er en mistillid til overvågningssamfundet. Det har jeg undret mig meget over. Ja, altså jeg føler mig rigtig godt tilpas, hvis der er overvågning.*

De bekymrede deltagere påpegede, at selvom man er en lovlydig borger, så kan øget overvågning og registrering på længere sig have konsekvenser, der er svære at tage højde for:

> *Jeg sidder her som lovlydig borger. Det er nemt for mig at sige; Jamen bare registrer det hele, ingen problemer i det. Men problemet er bare, at man kan ikke tænke sig hen til den situation hvor den registrering kunne gå hen og blive et problem for en. Også selvom det ikke er i et kriminelt øjemed.*

Deltagernes holdninger til sikkerhedsteknologi er til dels selvmodsigende. På den ene side synes flertallet af deltagerne at det er ubehageligt at blive overvåget, og at privatlivets fred ikke bør krænkes uden begrundet mistanke om forbryderisk fortsæt (omtrent 70% er delvist eller helt enige i disse to udsagn). På den anden side mener et flertal, at samfundets sikkerhed beror på udviklingen af nye sikkerhedsteknologier.

Deltagere uden børn viste sig at være mere kritiske overfor implementeringen af nye sikkerhedsteknologier og mere bekymrede for privatlivets fred. Den samme kritiske holdning og bekymring kunne oftere ses hos deltagere, der ikke havde videregående uddannelse – ingen i denne lille undergruppe følte sig tilpas under overvågning. De mandlige deltagere viste sig at være mere teknologiskeptiske end kvinderne, især når det kom til spørgsmål om ubehag som følge af overskridelse af privatsfæren – mindre end en tredjedel af mændene var helt eller delvist enige i udsagnet, der indledte dette afsnit, mens mere end halvdelen af kvinderne var uenige.

Deltagerne forholdte sig skeptisk overfor effekten af sikkerhedsteknologierne. Spørgeskemaerne viser, at størstedelen af deltagerne var overbevist om, at mange sikkerhedsteknologiske tiltag rent faktisk ikke har nogen effekt, men kun bliver iværksat for at give indtryk af, at der bliver gjort noget for at bekæmpe terrorisme. Dette kan ses både som en hård kritik af den terrorbekæmpelse der foregår i dag, og som en mistillidserklæring til det offentlige. Denne skepsis står i kontrast til at mere end halvdelen af deltagerne mente, at sikkerheden i samfundet kræver udvikling af nye sikkerhedsteknologier.

Under gruppediskussionerne kom deltagernes tvivl til udtryk:

> *Jeg synes i meget høj grad det giver en falsk tryghed. Jeg synes egentlig det er lidt bekymrende. Det er sådan lidt for at tækkes de gamle damer…*
>
> *Allerede nu er der jo masser af sikkerhedstjek I lufthavnen, og derfor er der jo stadigvæk folk der kaprer fly.*
>
> *Man skal vel også overveje om det er det værd. (…) Du kan jo vende den om og sige, at hvis man er terrorist, jamen så skal vi jo sikre alt. Al forsyning. Du kan jo hælde bakterier ned i vandet, der kan slå os alle sammen ihjel. Altså, der er jo masser af muligheder, og terrorister er jo heller ikke dumme. (…) Vi kan jo blive ved i en uendelighed.*

Deltagerne var også bekymrede for misbrug. Spørgeskemaerne viser, at mere end halvdelen var overbevist om, at sikkerhedsteknologier vil blive misbrugt af offentlige myndigheder, og næsten 90 % var overbevist om, at kriminelle vil misbruge dem. Under diskussionerne blev det klart, at deltagerne forventede, at kriminelle altid kan finde en måde at misbruge teknologien på. Deltagerne forventede også, at hvis en sikkerhedsteknologi bliver udviklet, så vil den blive taget i brug – også på måder, der oprindeligt ikke var tiltænkt. En deltager sammenlignede det med udviklingen af atombomben:

> *Det er ligesom at forhindre atom-bomben. Når først den er opfundet, så er det altså svært at blive ved med at forhindre den, ikke. En eller anden dag dukker den op på et sted hvor den ikke skulle være.*

Deltagerne fokuserede tilsvarende meget på, hvordan de personer, der kontrollerer teknologierne, kan misbruge dem. Der var udbredt bekymring for hvem, der har adgang til den information og de data der indsamles, og hvad det kan bruges til.

> *Der er jo bare den ene hale på det hele, og det er at det er mennesker der sidder på den anden side af teknologien og styrer det hele. Og alle ved hvad der sker, når mennesker får magt. Power corrupts!*

Deltagerne forudser, at private firmaer vil udnytte sikkerhedsteknologier til kommercielle formål. Både i forbindelse med reklamebaserede analyser af personlige indkøbsvaner og i forbindelse med forsikringsspørgsmål.

Nogle deltagere blev frastødt af tanken om privat overvågning af børn og ældre. En deltager refererer til det scenario, hvor Carla bliver overvåget af sin søn:

> *Den sidste del med Carla der bliver overvåget af sin søn uden at hun egentlig selv er bevidst om det. Det var nok også det der stødte mig mest sådan rent følelsesmæssigt. (…) Der tænkte jeg, det ville jeg virkelig føle mig krænket over.*

2.2 Konklusion

Hovedparten af deltagerne føler ubehag ved sikkerhedsteknologierne og vil beskytte deres privatliv. Yderligere fandtes der et stort flertal, der er overbevist, om at kriminelle, kommercielle interesser og offentlige institutioner alle vil misbruge teknologierne – især de personer, der direkte skal kontrollere teknologierne, er en kilde til bekymring.

På den anden side var der en tendens til, at deltagerne ønsker mere og bedre sikkerhedsteknologi for at garantere sikkerheden i samfundet. Udviklingen af ny, effektiv sikkerhedsteknologi, der kan øge sikkerheden, og som kun påvirker privatlivets fred i meget begrænset omfang, er en del af løsningen til at undgå konflikter. Men under mødet blev der fremsat holdninger, der lagde vægt på, at det er centralt at sikre tilliden til de institutioner, der skal implementere og kontrollere ny sikkerhedsteknologi.

Kapitel 3 Sikkerhedsteknologier

3.1 Sikkerhedsteknologier

Når vi retter blikket mod specifikke sikkerhedsteknologier, finder, vi at deltagernes holdninger og meninger er mere nuancerede og differentierede. I det følgende vil vi gennemgå deltagernes holdninger til en række specifikke sikkerhedsteknologier.

3.1.1 Biometri

Deltagerne faldt i to grupper, når de skulle tage stilling til brugen af biometri som adgangskontrol. Omtrent 40 % af deltagerne føler sig ikke tilpas ved at bruge nogen form for biometri. Resten accepterer at benytte sig af fingeraftryk, irisgenkendelse og i mindre omfang ansigtstræk.

Når teknologien blev knyttet til specifikke situationer og steder, blev den lettere at acceptere for deltagerne. Spørgeskemaerne afslører, at flertallet kan acceptere biometrisk adgangskontrol i lufthavne og ved grænseovergange (ca. 60 % af deltagerne). Kun omtrent en fjerdedel af deltagerne vil acceptere biometri i banker, på tog- og busstationer, ved sportsstævner og i butikker. Som en af de deltagere, der var positiv over for biometri udtrykte det:

> *Jeg kan klart se en fordel ved dem (biometri) når man flyver. Måske er det lidt overdrevet at bruge til bustransport. Lidt overkill (…) Men det er jo sikkerhed for os alle sammen. Så hvorfor ikke?*

Når deltagerne sammenlignede brugen af biometri med eksisterende sikkerhedsmæssige forholdsregler, fandt de at:

> *Det giver mere mening end at have tandpasta i en plasticpose.*

Selvom biometri accepteres i lufthavne og ved grænseovergange føler størstedelen af deltagerne sig utrygge ved at bruge biometriske pas, da de er nervøse for, at deres personlige data bliver stjålet.

Dette skal ses i lyset af, at mange deltagere var usikre på, hvor stor en risici biometriske rummer, hvad identitetstyveri er og hvilke farer, det indebærer.

En anden mulighed for at opklare kriminalitet, der bliver mulig med biometri, er central registrering af biometriske data. Deltagerne var delt i to næsten lige store grupper for og imod et sådan register. Diskussionerne viste, at mange ikke er klar over, at der allerede findes et DNA-register. Det var ikke et fremtrædende emne under diskussionerne, men en deltager sagde om DNA-registeret:

> *Så længe det kun bliver brugt i forbindelse med opklaring af forbrydelser. Det gør det meget nemt at udelukke folk (som mistænkte).*

3.1.2 Kameraovervågning

Kameraovervågning (CCTV) var en af de mest omdiskuterede teknologier i gruppediskussionerne – CCTV har været meget debatteret i medierne og er en teknologi

deltagerne var fortrolige med. Det er også den teknologi, deltagerne var mest positive overfor. Gruppediskussionerne viste, at deltagerne var overbevist om, at CCTV har potentiale til at forebygge kriminalitet og være en stor hjælp i efterforskningen af forbrydelse og terrorangreb.

Besvarelserne af spørgeskemaet understøtter denne opfattelse. Mere end fire femtedele synes enten, at der er et tilpas antal kameraer i samfundet, eller at der skal være flere (11 deltagere synes, der er tilpas mange og 11 ønsker flere). Alle deltagere kunne acceptere CCTV i lufthave og mere end 90 % vil acceptere det i banker og på bus- og togstationer. Tre fjerdedele vil acceptere CCTV ved sportsstævner og andre steder, hvor mange mennesker er samlet, og to tredjedele af deltagerne vil acceptere CCTV i butikker.

En deltager argumenterede:

> *Tv-overvågning i det offentlige rum, altså mere sådan, ikke på wc'er og omklædningsrum men andre steder, kan jeg ikke se noget galt i. Det kan hjælpe med at identificere kriminelle samtidig med at man normalt ikke ville foretage sig noget i det offentlige rum under alle omstændigheder, som man ikke ville lade andre se. Så det kan jeg ikke se noget galt i.*

Der er dog grænser – kun et fåtal ville acceptere at blive overvåget i *alle* offentlige rum og i prøverum for at forebygge tyveri. Den nøgne krop er *for* privat. En deltager formulerede det præcist:

> *Ikke indenfor min intimsfære!*

Samtidig var der delte meninger om, hvorvidt overvågning medfører en større følelse af tryghed. Gruppediskussionerne tog grundigt fat på dette emne – hovedtemaet var hvorvidt CCTV medførte mere sikkerhed eller mere mistillid mennesker imellem. Flere deltagere påpegede, at effekten af CCTV ikke er blevet klarlagt, især ikke den præventive effekt.

Det er meget vigtigt for deltagerne at skelne mellem aktiv og passiv kameraovervågning. Diskussionerne i grupperne viste, at størstedelen af deltagerne ønsker, at optagelser med passive kameraer kun bliver set igennem i forbindelse med bestemte hændelser. Men de var usikre på om det rent faktisk ville være sådan:

> *Hvis du altid er helt sikker på at den oplysning, den lille kamera bid og den lille ting der er registreret her aldrig nogensinde bliver misbrugt, og altid kun blev brugt til at fange the bad guy (…) så kan det godt være. Problemet er bare at det kan du bare aldrig nogensinde være sikker på.*

Aktive kameraer overskrider for langt de flestes vedkommende privatlivets grænser, sandsynligvis fordi den aktive kameraovervågning betyder, at handlinger og handlingsmønstre konstant evalueres.

3.1.3 Skanning

Det er primært i lufthavne, at deltagerne vil acceptere forskellige skanningsteknologier – deltagerne mener, at skanning er et acceptabelt værktøj til at forebygge terrorisme. De fleste kan også acceptere at deres bagage bliver røntgenfotograferet, selv at blive skannet for metalgenstande samt at blive skannet, hvor billeder af genstande på kroppen projiceres på en virtuel mannequin.

Det var kun i forbindelse med den såkaldte *nøgenmaskine*, at der var modstand mod skanning i lufthavne. Her meldte stort set alle deltagere pas. Det er tydeligt at denne teknologi overskrider de mest private grænser.

3.1.4 Lokaliserings-teknologi

At politiet lokaliserer mobiltelefoner og biler var ikke kontroversielt for deltagerne, så længe teknologien kun tages i brug på baggrund af en dommerkendelse, hvis der har været en ulykke, eller hvis en bil er blevet stjålet. Alle tre forhold er vigtige for omtrent tre fjerdedele af deltagerne. Så længe lokalisering bliver benyttet til disse tre formål, så mener deltagerne, at eCall og lokalisering af mobiltelefoner er gode måder at benytte sikkerhedsteknologi på.

Derimod er det kontroversielt at bruge eCall til at håndhæve fartgrænser og til at give fartbøder. På den ene side mente deltagerne, at det kan forbedre trafiksikkerheden. På den anden side betragtedes det også som en fundamental indtrængen i privatsfæren. Spørgeskemaet viste, at kun lidt mere end en tredjedel af deltagerne vil acceptere denne brug (10 ud af 27). Størstedelen af deltagerne mente, at installationen af eCall skal være frivillig, eller at eCall nemt skal kunne slås fra. Dette er særligt interessant, da det viser, at der findes en offentlig accept af visse former for forbrydelser, såsom at køre for stærkt. I situationer, hvor nye sikkerhedsteknologier skal indføres, kan det være afgørende præcist at definere hvilke forbrydelser, teknologien er rettet imod, og hvilken den ikke er, for at sikre befolkningens accept.

Størstedelen af deltagerne fandt på én gang at muligheden for at lokalisere biler og mobiltelefoner er en overskridelse af privatlivets fred og at det er et godt værktøj for politiets forebyggelse og efterforskning af forbrydelser og terrorisme. Dommerkendelsen var den afgørende faktor, der gjorde at deltagerne kunne acceptere lokaliseringsteknologierne.

3.1.5 Registrering af data

Registrering og skanning af data og sammenkørsel af registre kan bruges både til forebyggelse og efterforskning af forbrydelser og terrorisme. Spørgeskemaerne indikerer at registrering, skanning og sammenkørsel er accepterede metoder for størstedelen af deltagerne (mere end tre fjerdedele), så længe der er tale om, at teknologierne kun bruges til efterforskning af bestemte terrorangreb eller forbrydelser, der har fundet sted. Kun en fjerdedel vil acceptere, at gemte data bliver brugt i forbindelse med forebyggelse.

Samtidig fandt de fleste deltagere, at registrering af data potentielt overskrider privatsfæren. De mente f.eks. ikke at trafikdata fra kommunikation skal gemmes længere end hvad der er brug for til regninger, modsat hvad det bliver i øjeblikket. Modstanden mod registrering af data har sine rødder i angsten for, at registreret data bliver brugt til andet, end det oprindeligt var tiltænkt, et såkaldt *funktionsskred*. Op til 80 % af deltagerne i undersøgelsen mente at funktionsskred udgør et alvorligt problem for privatlivets fred. I gruppediskussionerne udtrykte deltagerne bekymring for, at en personlig profil kan blive skabt på baggrund af personlige data i forskellige databaser. En deltager brugte personnummeret som illustration af funktionsskred – det bliver i dag brugt til flere ting, end da det blev introduceret. En anden deltager sagde:

> *Du tager udgangspunkt i den lille bitte information, som egentlig på daværende tidspunkt, da den blev registreret, kunne være nok så uinteressant. Men fordi man lige pludselig identificerer den som værende interessant, så kan du lige pludselig gå*

> *tilbage og stykke alle mulige andre irrelevante informationer sammen og koble det op på en person.*

Registrering af data virker som en teknologi, der er svær at forstå. Den del af gruppen, der dagligt benytter e-mail eller Internet er betydeligt mindre bekymrede for registreringen. Det tyder på, at jævnlig brug af en given teknologi gør folk mere trygge, hvilket kan medtænkes når nye sikkerhedsteknologier skal implementeres.

Selvom de var bekymrede, mente omtrent halvdelen af deltagerne at skanning af data og sammenkørsel af registre er gode værktøjer for politiet til at forebygge terrorisme. Nogle påpegede dog, at mængden af data kan være så stor, at værktøjerne bliver ubrugelige.

Det er værd at bemærke, at 4 ud af 27 deltagere *aldrig* vil kunne acceptere skanning og sammenkørsel af databaser med personlige oplysninger. Størstedelen vil ikke acceptere, at offentlige institutioner af sikkerhedsmæssige årsager opbevarer alle de data, de finder nødvendigt. Registrering af data synes at være i direkte konflikt med beskyttelse af privatlivets fred. Dette billede tegnede sig også i gruppediskussionerne. Nogle deltagere påpegede et problem med adgangen til data:

> *Det største dilemma er hvem der skal have adgang til de her data om mig og borgerne…*

Imidlertid syntes andre deltagere at denne bekymring var overdrevet. De stillede i stedet spørgsmålstegn ved at andre på nogen måde skulle have interesse i at gennemgå data fra almindelige mennesker.

3.1.6 Aflytning

Ligesom det forholder sig med lokaliseringsteknologier, så er det dommerkendelsen, der er afgørende for, hvorvidt deltagerne kan acceptere aflytning. Spørgeskemaerne viser, at over 80 % af deltagerne accepterer aflytning som middel til at forebygge og efterforske kriminalitet og terrorangreb, men kun så længe, der foreligger en dommerkendelse. Kun en fjerdedel kunne acceptere aflytning uden dommerkendelse.

> *Det gør en kæmpe forskel om politiet, uanset hvad de gør overfor mig, om de har fået en dommerkendelse først. Så kan det godt være at der indimellem sidder nogle dommere der siger ja til alt, det har man jo så nogle gange en fornemmelse af, men alligevel så har det været forbi en dommer, og så kan jeg ligesom mærke magtens tredeling, og så bliver jeg mere rolig.*

Som med andre teknologier, opfattede deltagerne aflytning som et godt værktøj for politiet, men også som et værktøj, der krænker privatsfæren.

3.1.7 Teknologier til beskyttelse af personlig information

Størstedelen af deltagerne mente, at teknologier til beskyttelse af personlig information (PET) er nødvendige for at sikre privatlivets fred i dag (17 ud af 27 deltager erklærede sig enige i dette udsagn i spørgeskemaet). Når de blev spurgt om hvilke konkrete teknologier, der skal være tilgængelige, svarede mere end en tredjedel ”ved ikke”. Det tyder på, at der er megen usikkerhed om, hvad PET er, og på at deltagerne ikke har nok viden om disse teknologier – hvordan de virker, og hvilke konsekvenser de har. Deltagerne foretrak krypteringsprogrammer

(14 deltagere), mens kun et mindretal mente at det skal være lovligt at benytte anonyme taletidskort og identitetsstyringsprogrammer (henholdsvis 6 og 8 ud af 27).

3.2 Konklusion

Den mest diskuterede sikkerhedsteknologi til mødet var kameraovervågning. Kameraer bliver i høj grad accepteret, så længe de er passive og ikke aktive.

Overordnet accepterer deltagerne teknologier til adgangskontrol i særligt definerede områder, især i lufthavne. Det samme gælder for skanningsteknologier. De steder, hvor deltagerne accepterer disse teknologier, er steder, der opfattes som særligt farlige og steder, hvor det er belejligt. Eksempelvis er sikkerhedskontrol på steder, hvor deltagerne kun færdes uden for dagligdagen, såsom lufthavne og grænseovergange, ikke så stort et problem, som sikkerhedskontrol på den daglige bustur. Endeligt er kroppen for langt de fleste deltagere en uoverskridelig grænse for privatsfæren, der ikke bør eksponeres af sikkerhedsteknologier.

Mange af teknologierne vækker ambivalente følelser hos deltagerne (lokaliseringsteknologi, registrering af data og aflytning). På den ene side kan deltagerne se, at disse teknologierne er gode værktøjer i politiets arbejde med forebyggelse og efterforskning. På den anden side føler de, at disse teknologier krænker privatlivets fred. Dette skaber et åbenlyst dilemma, som mange af deltagerne forsøger at håndtere ved kun at ville acceptere brugen af disse teknologier, hvis der foreligger en dommerkendelse. Dilemmaet understreger vigtigheden af at sikre tilliden til de institutioner, der skal varetage og kontrollere brugen af sikkerhedsteknologien.

Det er ikke overraskende at observere en positiv sammenhæng mellem deltagernes kendskab til teknologierne og deres accept af samme. Yderligere finder vi, at deltagerne i højere grad er villige til at acceptere nye teknologier, når de bliver installeret steder, der i forvejen benytter andre sikkerhedstiltag. Begge dele tyder på, at accepten af nye sikkerhedsteknologier i høj grad er afhængig af, at folk lærer teknologierne at kende og bliver vant til dem.

Kapitel 4 Dilemmaer

4.1 Dilemmaer omkring brugen af sikkerhedsteknologi

Deltagerne blev i spørgeskemaet bedt om at tage stilling til en række dilemmaer. Visse dilemmaer blev også debatteret i grupperne.

4.1.1 Bekvemmelige rejser

Deltagerne blev bedt om at tage stilling til i hvilken grad, de er villige til at afgive personlige oplysninger, for at få mere bekvemmelige rejser. Det viste sig, at de fleste deltagere ikke er villige til at kompromittere privatlivets fred for at få nemmere ved at betale i offentlig transport, såsom metroen. Nogle deltagere vil dog acceptere at bruge f.eks. fingeraftryk som betalingsmiddel, men kun hvis det er valgfrit og ikke er den eneste form for betaling. Øget bekvemmelighed i forbindelse med rejser i offentlig transport er ikke grund nok til at opgive privatlivets fred.

Deltagerne er anderledes villige til at opgive dele af privatlivets fred for øget bekvemmelighed, når det gælder flyrejser. Kun en tredjedel af deltagerne vil ikke acceptere at opgive private data i bytte for nemmere check-in i lufthavnen. Resten af deltagerne er villige til at opgive private oplysninger så de kan benytte sikkerhedsteknologier, der kan gøre flyrejser nemmere. Dette kunne være at gennemgå et grundigt personligt baggrundscheck, at blive registreret i en sikkerhedsdatabase i lufthavnen og efterfølgende bruge biometri til identifikation. Det kunne også være at benytte 'nøgenmaskinen' og at få målt transpiration, kropstemperatur og puls. Folk der flyver ofte er mere tilbøjelige til ville bruge disse teknologier, hvilket indikerer, at fortrolighed med situationerne og teknologierne er en vigtigt faktor for accept.

At folk i højere grad støtter nye sikkerhedsteknologier i lufthavne end i metro, bus og tog, skyldes sandsynligvis, at folk er vant til at gå på kompromis med privatlivets fred i lufthavne, og at der er større tidsmæssig gevinst at opnå, da sikkerhedskontrollen normalt tager lang tid. Der er mindre privatliv at afgive og højere grad af bekvemmelighed at vinde i lufthavne end i resten af den offentlige transport.

4.1.2 Terrorforebyggelse

Et komplekst dilemma opstår i valget mellem forebyggelse af terrorangreb og sikring af privatlivets fred. Aktiv kameraovervågning og automatisk ansigtsgenkendelse (AFR) i lufthavne og på tog- og busstationer kan muligvis forebygge terrorangreb, men kan også medføre at uskyldige fejlagtigt bliver antaget for at være eftersøgte og bliver afhørt. Deltagerne var delte: 25 % synes ikke at aktiv kameraovervågning og AFR skal benyttes nogen steder – ca. 40 % synes kun at disse teknologier skal tages i brug, hvis *ingen* uskyldige bliver forvekslet med terrorister og omkring 30 % kan kun acceptere disse teknologier, hvis fejlraten er meget lille. Derudover påpegede størstedelen af de folk, der kan acceptere denne form for overvågning, at teknologien kun bør blive brugt steder, der er specielt eksponeret for terrorangreb, eller hvor der er meget kriminalitet.

Nogle deltagere påpegede, at det vil have store omkostninger, hvis alle passagerer på travle stationer skal gennemgå sikkerhedskontrol.

> *Det er jo helt uoverskuelige konsekvenser, hvis man skulle til at sikkerhedstjekke alle de pendlere der skal på arbejde, der skal skifte tog på hovedbanegården.*

En anden teknologi, der kan bruges i terrorbekæmpelse, er skanning af persondata og sammenkørsel af registre, med formål at lokalisere individer med mistænkelige profiler. Her er der ikke så stor splittelse i gruppen: 19 % eller 5 ud af 27 deltagere kan acceptere at politiet bruger disse teknologier, 5 andre kan aldrig acceptere det og de 17 tilbageværende kan acceptere, at politiet bruger teknologierne, men kun hvis data er anonymiseret og identiteten kun kan blive afsløret på baggrund af en dommerkendelse. Deltagerne fandt teknologien skræmmende, hvis data ikke anonymiseres. Som en deltager beskrev det:

> *Det kan proppes sammen i en eller anden database og så ligger der bare en eller anden totalprofil på mig. Det synes jeg er skræmmende, og det bliver jeg endnu mere utryg over end at en eller anden terrorist kommer med en bombe.*

De fleste deltagere fandt, at registrering af data og sammenkørsel af registre i høj grad overskrider privatlivets fred. De lægger vægt på, at området bør være stærkt reguleret.

4.1.3 Lokalisering af biler

eCall kan installeres i alle biler, således at deres færden kan registreres. Data kan bruges til forskellige formål, der i forskellig grad bryder privatlivets fred. Der var bred enighed blandt deltagerne om, at den oprindelige ide med eCall – automatisk positionsangivelse i forbindelse med ulykker – er rigtig god.

Men politiet kan bruge eCall til to andre formål: Den ene mulighed er at aktivere eCall for at lokalisere en bil for at forhindre eller efterforske en forbrydelse eller et terrorangreb. Den anden er automatisk udstedelse af fartbøder. Selvom trafikken og især fart er skyld i flere dødsfald end terrorangreb, var deltagerne i langt højere grad klar til at lade politiet overvåge biler for at forebygge terrorangreb end for at udstede fartbøder. Det virker som om at 'retten' til at køre for stærkt har en særlig status, og at deltagerne mente at det er en stor overskridelse af privatlivets fred ikke at være i stand til at kunne køre for stærkt uden at få en bøde. Dette understreger vigtigheden af klart at definere og garantere hvilke lovovertrædelser, sikkerhedsteknologierne rettes imod, og undgå at bruge dem til at bekæmpe mindre betydningsfulde lovovertrædelser.

4.1.4 Beskyttelse af personlig information for alle

Teknologier til beskyttelse af personlig information kan benyttes af almindelige mennesker til at værne om deres privatliv, f.eks. når de går på Internettet, eller når de taler i mobiltelefon. Men disse teknologier kan også blive brugt af kriminelle og terrorister og dermed besværliggøre politiets forebyggende arbejde og efterforskning. Størstedelen af deltagerne er villige til at acceptere lovlig brug af krypteringsprogrammer, også selvom det vanskeliggør politiets arbejde. Med hensyn til anonyme taletidskort og Internet-anonymitet er deltagerne ikke så enige. Mindre end halvdelen kan acceptere, at disse teknologier er lovlige, hvis de vanskeliggør politiets arbejde. Når teknologierne knyttes sammen med specifikke former for kriminalitet, kan de accepteres af endnu færre deltagere. Hvis konsekvensen er, at en person, der leder efter bombe-opskrifter på nettet, ikke kan spores af politiet, så er det kun omtrent en tredjedel af deltagerne, der kan acceptere Internet-anonymitet. Kun en femtedel kan acceptere Internet-anonymitet, hvis konsekvensen er, at en person, der leder efter børnepornografi, ikke kan spores af politiet.

Flertallet af deltagerne fandt beskyttelse af personlige informationer vigtig. De er villige til at acceptere at politiets forebyggelse og efterforskning besværliggøres, men nogle konsekvenser er sværere at sluge end andre (f.eks. børnepornografi, der er et meget sensitivt emne). Det virker ikke som om Internet-anonymitet er lige så vigtig som anonymitet ved telefonsamtaler. Det tyder på, at telefonen opfattes som et mere privat 'sted' end Internettet.

4.1.5 Konsekvenser for andre

Det sidste dilemma deltagerne blev konfronteret med, adresserede hvilke konsekvenser, deltagerne var villige til at acceptere for folk, der enten ikke *kunne* eller ikke *ville* bruge teknologierne, såfremt teknologierne kunne medføre øget sikkerhed eller gøre hverdagen nemmere. Konsekvenserne kan være udelukkelse fra offentlige services eller problemer med at benytte offentlig transport.

Hovedparten af deltagerne er ikke villige til at acceptere nogen form for konsekvenser, hverken for personer, der ikke er i stand til at bruge sikkerhedsteknologierne eller personer, der vælger ikke at bruge sikkerhedsteknologierne. Det mindretal, der er villige til at acceptere en eller anden form for konsekvenser, er mest tilbøjelige til at acceptere konsekvenser for dem, der selv vælger ikke at benytte teknologierne. Kun lige over 10 % kan acceptere konsekvenser for personer, der ikke er i stand til at benytte teknologierne. Dette demonstrerer en stor følelse af solidaritet med både dem, der ikke kan, og dem, der ikke vil benytte sikkerhedsteknologierne. Det er sandsynligt, at deltagerne har lettere ved at forestille sig konsekvenserne af at blive afskåret fra offentlige services end konsekvenserne af et terrorangreb. Holdningerne kan komplicere implementeringen af ny sikkerhedsteknologi på nogle områder. Vi har eksempelvis tidligere påpeget at der findes en gruppe af deltagere, der ikke vil acceptere at deres personlige data bliver registreret. Hvis de bliver tvunget til registrering, vil det være i konflikt med flertallets overbevisning, men hvis det er lovligt at undlade at lade sig registrere, vil effekten af teknologierne i værste fald være betydningsløs.

4.2 Konklusion

De dilemmaer, der følger af ny sikkerhedsteknologi er komplekse. Ét er at kigge på de teknologiske muligheder, noget andet er at kigge på den faktiske brug af teknologier og hvilke konsekvenser det medfører.

Mere bekvemmelige rejser på bekostning af privatlivets fred er kun acceptabelt for flertallet, når det gælder rejser med fly, ikke andre former for offentlige transportmidler. Når det kommer til forebyggelse af terrorangreb, kan deltagerne acceptere nogle former for sikkerhedsteknologier, men kræver dommerkendelser, hvis teknologierne i for høj grad griber ind i privatsfæren. Generelt set er der ikke stor tilslutning til teknologier, der beskytter private informationer, hvis det er på bekostning af politiets arbejde. Der er størst opbakning til krypteringsprogrammer. Endeligt skal det fremhæves, at langt størstedelen af deltagerne ikke kan acceptere, at personer, der enten ikke kan eller ikke vil bruge sikkerhedsteknologierne, skal opleve nogen form for konsekvenser.

Kapitel 5 Demokratiske spørgsmål

5.1 Demokrati og deltagelse

Beslutninger om udvikling og implementering af ny sikkerhedsteknologi kan potentielt have meget stor indflydelse på borgernes hverdagsliv. Beslutningerne bør derfor træffes på et demokratisk grundlag. Spørgsmålet er hvordan: Hvem skal involveres i overvejelserne, i hvilke beslutninger og på hvilken måde? Deltagerne blev bedt om at tage stilling til disse spørgsmål.

Deltagerne udviste stor tillid til det etablerede repræsentative demokrati. De mener at det bør være de folkevalgte politikere, der træffer de endelige beslutninger om implementeringen af ny sikkerhedsteknologi. Men de mener også, at offentlig debat og offentlige høringer bør være en del af den demokratiske proces, når disse valg skal træffes. Kun få deltagere erklærede sig enige i udsagnet om, at spørgsmål om privatlivets fred og sikkerhedsteknologier er for komplicerede til at den brede offentlighed skal involveres. Den udbredte holdning gengives i dette citat fra gruppediskussionerne:

> *Efter en bred debat kunne det være rimeligt at politikerne traf beslutningerne. Det er jo vores demokrati.*

Visse deltagere ønsker dog mere indflydelse på de endelige beslutninger og foreslog en form for folkeafstemning, når det gælder vigtige sikkerheds- og privatlivsspørgsmål. Alle deltagere er enige om, at borgerinddragelse er meget vigtig og efter nogen diskussion opstod der i gruppediskussionerne konsensus om, at det vil være bedst at fokusere på at skabe offentlig debat, der kan tilkendegive den offentlige holdning overfor politikerne, før de træffer beslutninger.

> *Så kunne man få borgerne til at give en indikation af hvilken retning det er vi skal gå i. Men så tror jeg også man skal sige: Det var så det. Så er der et hold af eksperter eller et udvalg eller et eller andet, der sætter sig ned og finpudser det her. Man kan ikke lægge det ud til offentligheden.*

En anden ting der er vigtig for deltagerne, er, at politikerne skal høre personer med særlig viden om teknologierne og deres potentielle konsekvenser:

> *Fordi politikere de gør det jo kun ud fra deres politiske synsvinkel.*

Med hensyn til involvering af andre parter i forløbet er stort set alle deltagerne enige om at menneskerettighedsorganisationer bør deltage i beslutningsprocesser om sikkerhedsteknologi og privatliv. Dette indikerer, at deltagerne betragter menneskerettighedsorganisationer som talsmænd for beskyttelse af privatlivets fred.

På trods af at deltagergruppen er mere delt, når det gælder om at involvere udviklere af sikkerhedsteknologi i beslutningsprocessen, så er et lille flertal (15 ud af 27 deltagere) enige om, at de bør være med. Det blev begrundet med, at disse udviklere besiddelser af særlig ekspert-viden.

Det er bemærkelsesværdigt, at stort set alle deltagere finder det meget vigtigt, at debatten også inddrager alternative løsninger på de sikkerhedsmæssige problemer.

5.2 Forslag

Spørgeskemaet blev rundet af med fire konkrete forslag til hvordan sikkerhedsteknologier kan tages i brug samtidig med, at privatlivets fred sikres bedst muligt. Deltagerne blev bedt om at vurdere disse forslag. Resultaterne er præsenteret i følgende tabel:

Forslag	Stor betyd.	Vis betyd.	Begræn set betyd.	Ingen betyd.	Ved ikke
Indsamling af personlige data fra personer, som ikke er under mistanke, skal foregå anonymiseret, indtil en dommerkendelse har bemyndiget en identificering	20	3	2	0	2
Kun autoriseret personale må få adgang til de registrerede personlige data	25	2	0	0	0
Før de implementeres, skal de nye sikkerhedsteknologier altid kontrolleres for deres mulige konsekvenser for privatlivets fred	19	7	1	0	0
Finansieringen af forskning i nye sikkerhedsteknologier bør afhænge af grundig analyse for privatlivets fred	12	6	5	2	2

De to første forslag sigter mod at regulere brugen af sikkerhedsteknologier. Vi har tidligere i rapporten set, at registrering af personlige data synes at være et særdeles sensitivt emne for deltagerne. Forslaget om at kun autoriseret personel skal have adgang til disse data, er det forslag, som flest deltagere mener har stor betydning. Derefter følger forslaget om bevarelse af anonymitet med mindre der forligger en dommerkendelse, der også bliver evalueret meget positivt af deltagerne.

De to andre forslag sigter mod regulering af beslutningsprocessen om implementeringen af ny sikkerhedsteknologi. Forslaget om at indvirkningen på privatlivets fred skal vurderes, før teknologien implementeres, synes at være rimelig vigtigt. Forslaget om at finansiering af forskning i sikkerhedsteknologi skal afhænge af grundig analyse, er ikke lige så vigtigt for gruppen, som de tre andre forslag. Dette kan skyldes, at deltagerne ikke mener at det rent faktisk er muligt at styre udviklingen af ny sikkerhedsteknologi, en holdning der kom til udtryk i debatten:

> *Hvis der er nogen der vil købe, så er der også nogen der vil fremstille. Sådan fungerer markedet.*

Andre udtrykte dog uenighed i dette synspunkt og finder i stedet at regulering af udviklingen var både vigtigt og muligt.

5.2.1 Deltagernes egne forslag

Deltagerne kom selv med forslag til hvordan privatlivets fred kan sikres i udviklingen af nye sikkerhedsteknologier.

Udviklingen skal reguleres:

> *Ligesom man forsøger at regulere at virksomheder for eksempel ikke må forurene. (…) må man jo også kunne stille nogle krav til virksomheder, der fremstiller sikkerhedsteknologi.*

Magten, som de personerne, der kontrollerer teknologierne, er i besiddelse af, skal begrænses:

> *Man må jo prøve at gardere sig så vidt man kan, så den enkelte lille person har så lidt magt som muligt i de systemer.*

Der skal laves lovgivning, der begrænser brugen af sikkerhedsteknologi:

> *Man skal have nogle regler til, hvor man må bruge den teknologi.*

5.3 Konklusion

Deltagerne udviser tillid til det repræsentative demokrati og mener at det er politikerne, der bør tage beslutningerne om hvilke sikkerhedsteknologier, der skal implementeres og hvordan. De finder det dog vigtigt, at borgerne bliver involveret i den offentlige debat omkring emnet. De ønsker også at menneskerettighedsorganisationer og i mindre omfang udviklere af sikkerhedsteknologi skal høres inden beslutningerne træffes.

Det er også vigtigt at bemærke, at deltagerne ønsker, at der tænkes i alternative løsninger, når ny sikkerhedsteknologi debatteres.

De fire forslag i spørgeskemaet, som deltagerne skulle tage stilling til, blev alle vurderet til at have stor betydning og deltagerne bidrog med deres egne forslag under gruppediskussionerne – forslag om hvordan udviklingen og brugen af sikkerhedsteknologi kan reguleres.

Kapitel 6 Yderligere pointer

6.1 Fokuser ikke for meget på teknologien

Emnet for mødet var de muligheder for øget sikkerhed og de farer for krænkelse af privatlivets fred, der følger med ny sikkerhedsteknologi. Imidlertid blev det under gruppediskussionerne flere gange nævnt, at man ikke bør fokusere snævert på teknologi og antage at teknologi er den eneste måde at bekæmpe kriminalitet og terrorisme på. Nogle deltagere understregede behovet for at forske i ikke- eller lavteknologiske løsninger, såsom bedre gadebelysninger eller andre alternativer til mere kameraovervågning:

> *Altså hvis bare man havde noget patruljering af to politimænd, der gik og fløjtede, ikke. Jamen det giver ti gange mere end at der er et videokamera.*

Andre argumenterede for, at der skal fokuseres mere på de mulige negative konsekvenser, især mulighederne for misbrug, inden teknologierne tages i brug.

> *Det er ikke hvad teknologien kan, det er hvordan den kan misbruges.*

6.2 Deltagernes holdning efter mødet

Som afslutning på gruppediskussionerne og i slutningen af spørgeskemaet, blev deltagerne spurgt om, hvorvidt de havde ændret holdning efter deres deltagelse i borgermødet. Flertallet havde ikke ændret holdning efter at have udfyldt spørgeskemaet, mens 6 ud af de 27 deltagere var blevet mere bekymrede og én enkelt var blevet mere positivt indstillet overfor ny sikkerhedsteknologi. Nogle deltagere bemærkede, at de var kommet for at give deres mening til kende, ikke for at ændre den.

På den anden side tilkendegav mange deltagere, at de både havde lært en masse og fået større interesse i emnet i kraft af deres deltagelse. Deltagelsen havde for langt de fleste været en positiv oplevelse og flere deltagere ønskede flere lignende møder.

> *Det har fået mig til at tænke mere på sikkerhedsproblematikken.*

> *Det har ikke ændret min holdning, men jeg kan da godt se at der udviklet noget nyt som jeg ikke lige var klar over. Der er i hvert fald mere end jeg måske havde forestillet mig. Der er også meget jeg godt kunne tænke mig at sætte mig lidt mere ind i.*

6.3 Den danske kontekst

Resultaterne er selvfølgelig præget af den danske kontekst. Danmark har deltaget i Irak-krigen, og er derfor et mål for terrorangreb ligesom sagen om Muhammed-tegningerne har forværret sikkerhedssituationen. Imidlertid har der ikke været terrorangreb i Danmark i mere end 15 år, og landet har aldrig oplevet et stort angreb. Det er muligt, at dette gør danskerne mere kritiske over for effekten af sikkerhedsteknologier end borgere i lande, der har oplevet større angreb fornyeligt.

Det er også værd at bemærke, at Danmark har et gammelt og sundt demokrati, hvor politikere og især offentlige autoriteter nyder stor tillid fra borgerne. Det er sandsynligt at danskerne på

denne baggrund udviser tilsvarende større tillid til dem, der skal kontrollere ny sikkerhedsteknologi.

Kapitel 7 Bilag

7.1 Oversigt over bilag

- Bilag 1 – Deltagernes baggrund
- Bilag 2 – Program for borgermødet
- Bilag 3 – Materiale sendt til deltagerne
- Bilag 4 – Spørgeskema og interviewguide på dansk
- Bilag 5 – Transskriptioner af gruppeinterviewene på dansk
- Bilag 6 – Frekvenstabeller
- Bilag 7 – Kommentarer fra spørgeskemaerne