



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

**Annex to D. 5.3 Danish Report –
Interview Meeting About Security and Privacy**

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

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

TEKNOLOGI-RÅDET

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



Legal notice:

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of the following information.

© PRISE 2007. Reproduction is authorised provided the source is acknowledged.

Table of Contents		page
Annex 1	Participants' background	4
1.1	<i>Selection Bias in Participants in the Interview Meeting</i>	4
1.2	<i>Response and Selection</i>	4
1.3	<i>Conclusion</i>	5
Annex 2	Agenda for the interview meeting (in Danish)	6
Annex 3	Material sent to the participants (in Danish)	7
3.1	<i>Letter of invitation</i>	7
3.2	<i>Letter of confirmation</i>	10
3.3	<i>Letter of refusal</i>	12
3.4	<i>Directions</i>	13
3.5	<i>Scenarios</i>	14
Annex 4	Questionnaire and interview guide (in Danish)	27
4.1	<i>Spørgeskema om sikkerhedsteknologi og privatlivets fred</i>	27
4.2	<i>Interview guide</i>	56
Annex 5	Transcripts of group interviews (in Danish)	59
5.1	<i>Transcript of interview by BB</i>	59
5.2	<i>Transcript of interview by IL</i>	100
5.3	<i>Transcript of interview by MIH</i>	134
5.4	<i>Transcript of interview by UV</i>	158
Annex 6	Frequency tables	194
6.1	<i>Frequencies</i>	194
6.2	<i>Cross tables</i>	229
6.3	<i>Recoding</i>	276
6.4	<i>Syntax / SPSS</i>	278
Annex 7	Comments from the questionnaire (in Danish)	282

Annex 1 Participants' background

1.1 Selection Bias in Participants in the Interview Meeting

Selection of participants was based on three criteria, on which the participants should be equally distributed.

- Sex
- Age
- Level of Education

The potential participants was divided by age in three subgroups

- 18-35 years
- 36-54 years
- 56+

In accordance with highest education, they were further divided into three educational subgroups, based on the years of schooling and common perception of the Danish educational system.

- 10 years of education or less and vocational training was coded as "1"
- Longer secondary education e.g. highschool and short tertiary educations less than 3 years (not including 'professional-bachelors') was recoded into "2"
- Tertiary education of at least 3 years e.g. university diplomas, was recoded into "3"

1.2 Response and Selection

Out of 2000 invitations sent out, 58 (2.9%) responded. Out of these, we selected 37 participants. At the meeting 28 participants showed, 27 of these filled out a questionnaire.

The 58 original responses were distributed as follows:

	Male			Female		
Education	1	2	3	1	2	3
18-35	2	4	4	0	1	2
36-55	2	3	1	1	4	5
56+	5	4	5	3	9	3

Our aim was to have 2 in each space, cf. Interview Meeting Manual pp. 12f.

It is clear that the group of interested consisted of too many older people and lacked young women. We compensated for this in the final selection, but we could not take into account, which people would not show up at the meeting.

The final distribution of participants:

	Male			Female		
Education	1	2	3	1	2	3
18-35	1	2	4	0	1	2
36-55	1	2	0	1	3	1
56+	1	1	2	1	2	2

1.3 Conclusion

In the group we have too few participants with short education (5 preferable 9). Consequently we have too many with medium and long education.

The rest of the distribution satisfies our demands.

Annex 2 Agenda for the interview meeting (in Danish)

Program for PRISE borgermøde om privatliv og sikkerhedsteknologi, onsdag d. 30/5-2007 på DSB Kursuscenter Østerport

16:30-17:00	Adgang til kursuscenteret
17:00-17:15	Velkomst v. projektleder Anders Jacobi
17:15-17:50	Introduktion til sikkerhedsteknologi og privatliv v. Anders Albrechtslund
17:50-18:40	Udfyldning af spørgeskema
18:40-18:50	Gruppedannelse
18:50-19:50	Gruppedebat
19:50-20:00	Samling og afslutning

Annex 3 Material sent to the participants (in Danish)

3.1 Letter of invitation

Kære «Navn»

Vi har brug for din mening!

Teknologirådet inviterer dig til at dele dine holdninger om privatliv og sikkerhedsteknologi med os på et borgermøde

**Onsdag d. 30. maj 2007 klokken 17.00 – 20.00 på
DSB Kursuscenter Østerport
Folke Bernadottes Alle 7
2100 København Ø**

Hvilket privatliv og hvilke sikkerhedsteknologier?

Du er måske ikke klar over det, men information om din gøren og laden i forskellige situationer bliver i stadig større grad registreret og gemt – når du sender eller modtager en e-mail derhjemme, når du bliver filmet af et kamera på togstationen, og når du bruger dit kreditkort i en butik. Dette er konsekvensen af udviklingen indenfor sikkerhedsteknologi. Sikkerhedsteknologi kan få os til at føle os mere trygge ved at forhindre og bidrage til opklaring af kriminalitet og terrorisme, og kan også gøre hverdagslivet mere bekvemt.

Imidlertid kan udviklingen af sikkerhedsteknologi være problematisk – hvordan kan en tryk og bekvem dagligdag afbalanceres med den risiko for krænkelse af privatlivets fred, falske anklager og misbrug af personlig information, som sikkerhedsteknologi også rummer? Det er dette dilemma, vi ønsker, at du diskuterer med os.

Hvorfor dig?

Ny sikkerhedsteknologi vil have indflydelse på alle. Derfor er det vigtigt at inddrage dem, der skal leve med disse teknologier – det er dig. Sammen med andre i og omkring Københavnsområdet er du blevet tilfældigt udvalgt til at modtage dette brev. Den tilfældige udvælgelse hjælper os med at komme i kontakt med folk der har forskellige baggrunde og meninger. Det betyder at vi ikke forventer at du har nogen forudgående viden om sikkerhedsteknologi – bare du har lyst til at påvirke fremtiden.

Hvad er et borgermøde?

Mødet er et uformelt 'gå-hjem møde' og vil vare tre timer. Du vil møde omkring 30 andre deltagere med forskellig baggrund, ingen af dem vil have specialiseret viden om sikkerhedsteknologi. Først vil en ekspert introducere de relevante problemstillinger med tid afsat til spørgsmål. Derefter vil du blive bedt om at udfylde et spørgeskema. Til sidst vil du få muligheden for at debattere mulige fremtidsscenerier med de andre deltagere i mindre grupper. Under mødet vil der blive serveret mad og drikke.

Deltagelse i mødet er gratis. Teknologirådet dækker alle ekstraordinære udgifter til transport.

Hvorfor afholdes borgermødet?

Mødet er en del af EU-projektet PRISE (**P**rivacy enhancing shaping of **s**ecurity research and **t**echnology). Forskningsprojektet laves i samarbejde mellem institutioner i Danmark, Norge, Tyskland og Østrig, der alle har stor erfaring med at vurdere og evaluere ny teknologi. Der vil blive afholdt borgermøder i Danmark, Norge, Tyskland, Østrig, Spanien og Ungarn.

PRISE vil udvikle en række guidelines til den fremtidige udvikling af sikkerhedsteknologi i EU. De perspektiver, der fremkommer til møderne, vil være det centrale element i projektet.

Vi har vedlagt en kort præsentation af PRISE, og du kan klikke ind på hjemmesiden (engelsk) <http://prise.oeaw.ac.at/>, hvis du vil vide mere.

Hvordan kan jeg deltage?

Du kan enten tilmelde dig på <http://www.tekno.dk/prise2007> eller ved at udfylde og returner den vedlagte svarkupon i den tilhørende svarkuvert. Portoer er betalt.

Vi skal senest have din tilmelding den 14. maj. Du modtager svar på din tilmelding senest den 16. maj.

Deltagere vil modtage et detaljeret program for mødet og en kort introduktion til ny sikkerhedsteknologi. Hvis vi modtager mere en 30 tilmeldinger, vil vi udvælge folk, så deltagergruppen bliver så blandet som muligt.

Hvis du *ikke* ønsker at deltage, behøver du ikke at foretage dig noget. Bemærk venligst at vi **har** slettet dit navn og din adresse, så snart vi har sendt dette brev.

Kontakt

Kontakt os endeligt hvis du har spørgsmål eller kommentarer.

Vi glæder os til at høre fra dig!

Venlig hilsen

Mikkel Holst

Anders Jacobi

Projektmedarbejder

Projektleder

mih@tekno.dk

aj@tekno.dk

Direkte tel.: 33 45 53 72

Direkte tel.: 33 45 53 71

Tilmelding til borgermøde om privatliv og sikkerhedsteknologi, onsdag d. 30. maj 2007 kl. 17.00 – 20.00 på DSB Kursuscenter Østerport, Folke Bernadottes Alle 7, 2100 København Ø

Udfyld venligst alt markeret med *

*Navn:

*Vej og nr.:

.....

*By:

*Postnummer:

*Telefon:

*E-mail:

*Køn:

*Alder:

*Uddannelse:

Begrundelse for deltagelse / kommentarer:

.....

.....

.....

.....

.....

.....

3.2 Letter of confirmation

Kære «Navn»

Det er os en glæde at kunne meddele dig, at du er blevet udvalgt til at deltage i PRISE borgermøde om sikkerhedsteknologi og privatliv.

Vi minder dig om at mødet finder sted

**Onsdag d. 30. maj 2007 klokken 17.00 – 20.00 på
DSB Kursuscenter Østerport
Folke Bernadottes Alle 7
2100 København Ø**

Vi byder på mad og drikke *allerede en halv time før mødestart.*

Rutebeskrivelse er vedlagt.

Borgermødet

Borgermødet er en metode udviklet specielt til at opfange befolkningens perspektiver på komplekse problemstillinger. Det især, når det handler om problemstillinger, hvor forudgående viden om emnet er begrænset. Mødets vigtigste formål er at skabe forståelse for mangfoldigheden af holdninger og argumenter der knytter sig til emnet. Dette betyder at der ikke er nogen 'rigtige' og 'forkerte' svar på de spørgsmål der bliver stillet og debatteret. Tværtimod afhænger mødets succes af at stemningen er uformel, livlig og respektfuld og af at alle bliver hørt.

Mødet består af tre dele. Når alle har fået en plads og der er blevet budt velkommen, vil en oplægsholder med speciale i sikkerhedsteknologi og privatliv introducere emnet. Det skal sikre at alle har en god forståelse af de underlæggende problemer, der følger med udviklingen sikkerhedsteknologi. Der er afsat tid til uddybende spørgsmål.

Derefter vil I blive bedt om at udfylde et spørgeskema, der omhandler personlige holdninger til – og betragtninger om – nye sikkerhedsteknologier i forskellige situationer. Vi vil være der til at hjælpe jer igennem forløbet.

Efterfølgende vil deltagerne blive opdelt i mindre grupper med seks til ni personer, hvor I vil debattere problemstillingerne, med hjælp fra trænedede interviewere.

Til sidst samles alle igen, og der vil være tid til at stille de sidste spørgsmål og kommentere forløbet.

Vi gør dig opmærksom på, at gruppeinterviewene vil blive optaget på bånd, for at lette vores arbejde. *Alle bidrag vil blive anonymiseret i det efterfølgende arbejde.*

Program

16:30-17:00	Adgang til kursuscenteret
17:00-17:15	Velkomst v. projektleder Anders Jacobi
17:15-17:50	Introduktion til sikkerhedsteknologi og privatliv
17:50-18:40	Udfyldning af spørgeskema
18:40-18:50	Gruppedannelse
18:50-19:50	Gruppedebat
19:50-20:00	Samling og afslutning

Forberedelse

Vedlagt dette brev finder du nogle såkaldte *scenarier*, der behandler sikkerhedsteknologi og privatliv. Scenarierne er en måde at fremstille tænkelige udviklinger inden for sikkerhedsteknologi, de dilemmaer som medfølger og forskellige måder at anskue dilemmaerne på. Scenarierne beskriver en forholdsvis normal dag for to opdigtede personer og er lette at forholde sig til. Scenarierne indeholder også fakta om de forskellige teknologier, der optræder i historierne.

Vi opfordrer dig til at læse og reflektere over disse scenarier inden mødet, da de fleste spørgsmål og meget af debatten vil tage udgangspunkt i de dilemmaer, som bliver præsenteret heri.

Hvis du har spørgsmål eller kommentarer kontakt os endelig.

Venlig hilsen

Mikkel Holst

Projektmedarbejder

mih@tekno.dk

Direkte tel.: 33 45 53 72

Anders Jacobi

Projektleder

aj@tekno.dk

Direkte tel.: 33 45 53 71

3.3 Letter of refusal

Kære «Navn»

Det er med beklagelse, at vi må meddele dig, at du *ikke* er blevet udvalgt til at deltage i PRISE borgermøde om sikkerhedsteknologi og privatliv.

Der har været så stor interesse for projektet, at vi har været tvunget til at prioritere tilmeldingerne. I udvælgelsen har det været vores mål at sikre at vi fik sammensat en gruppe, der indeholder folk med så forskellige baggrunde som muligt.

Vi er virkelig glade for din interesse i PRISE, og håber at du vil udvise samme interesse for lignende projekter i fremtiden.

Du kan følge udviklingen af PRISE på den officielle hjemmeside <http://prise.oeaw.ac.at/>, og du er selvfølgelig også velkomne til at kontakte Teknologirådet om udviklingen.

Hvis du har spørgsmål eller kommentarer kontakt os endelig.

Venlig hilsen

Mikkel Holst

Projektmedarbejder

mih@tekno.dk

Direkte tel.: 33 45 53 72

Anders Jacobi

Projektleder

aj@tekno.dk

Direkte tel.: 33 45 53 71

3.4 Directions

Kursuscenter Østerport ligger midt i København, der er gode forbindelser hertil med både tog, bus, cykel og bil.

Østerport station ligger blot 2. min gang fra Kursuscenteret og er du i bil eller på cykel kan du parkere umiddelbart ved kursuscenteret, her nedenfor kan du læse hvad du særligt skal være opmærksom på ved ankomsten.

NÅR DU KOMMER MED TOG ELLER BUS

Der er forbindelse fra såvel S-tog og Kystbane til Østerport station, desuden BUS forbindelse til Oslo Plads. Du kan finde yderligere oplysninger om tog og busafgange på www.dsb.dk.

NÅR DU KOMMER I BIL - PARKERING

Du kan parkere ved bagsiden af kursuscenteret. P-pladsen er overvåget og der kræves P-billet på alle pladser. Parkeringspladserne er markeret på gule skilte med DK-parkering.

Du kan afhente P-tilladelse i kursuscenterets reception. Indgang til denne sker ved den store flagstang modsat P-arealet eller via terrassen ved P-areal og så brug døren som er markeret med bagindgang til reception. Sidstnævnte er klart den hurtigste.

HVIS DU FÅR BRUG FOR AT BLIVE KONTAKTET MENS DU ER HER

Du kan modtage opkald på kursuscenterets telefon og telefax. Vi beder dig derfor venligst checke ind ved kursuscenterets reception ved ankomst så vi er opmærksomme på at du evt. venter opkald eller andet



3.5 Scenarios

Forord

PRISE projektet stiler mod at bidrage til en sikker fremtid i EU, som stemmer overens med europæernes borgerrettigheder – herunder specielt beskyttelse af privatlivets fred – og deres præferencer.

Projektet vil:

- udvikle kriterier og retningslinjer for sikkerhedsforskning og teknologiudvikling som tager hensyn til privatlivsbeskyttelse
- udvikle scenarier for sikkerhedsteknologier og sikkerhedstiltag
- afprøve scenarierne gennem en borgerinddragelsesproces i forskellige europæiske lande for at få et indtryk af hvordan sikkerhed og privatlivsbeskyttelse opleves i offentligheden, og hvilke præferencer europæiske borgere har på området
- videreudvikle kriterier og retningslinjer gennem direkte involvering af leverandører af sikkerhedsteknologi, private og offentlige brugere og udviklere, institutioner og organer som former politikker og love, samt organisationer som repræsenterer (potentielt) modstridende interesser
- formidle resultaterne til aktører som er relevante i udformningen af teknologi og politikker på området.

Dette dokument er en præsentation af de scenarier, der er udviklet som en del af projektet. Scenarierne søger at give lægfolk indsigt i forskellige sikkerhedsteknologier og hvorledes de kan anvendes i dagligdagssituationer i en nær fremtid. Vi forsøger at adressere forskellige tilgange til teknologierne, både fra brugernes synsvinkler og i samfundet.

Introduktion

Dette dokument vil introducere dig til nogle scenarier, der viser, hvordan sikkerhedsteknologier og overvågning kan anvendes i dagligdagssituationer i en nær fremtid.

Hvad er sikkerhedsteknologi?

Sikkerhed kan defineres som fravær af fare – det vil sige en tilstand, hvor det ønskede status quo ikke på nogen måde er truet eller forstyrret. I **PRISE** projektets kontekst forstås sikkerhed som samfundets sikkerhed – eller mere præcist – sikkerhed, som omfatter de borgere, der udgør samfundet.

Udtrykket *sikkerhedsteknologi* kan dække alt fra private alarmsystemer og PC virus beskyttelsessystemer til grænsekontrollsystemer og internationalt politisamarbejde. I vore scenarier fokuserer vi hovedsageligt på teknologier eller midler (systemer, lovgivning etc.) som har til formål at forbedre samfundets sikkerhed med hensyn til trusler fra individer, eller grupper af individer (ikke fra stater). Dette omfatter kriminalitetsbekæmpelse, antiterror aktiviteter, grænsekontrol aktiviteter etc.

I scenarie-teksten finder du også fakta om de forskellige teknologier, som kan hjælpe dig med at forstå deres fremtidige potentiale og hvordan de fungerer i dag.

Hvad er privatlivets fred?

Privatlivets fred er generelt forbundet med beskyttelse af individets integritet og autonomi.. Grundlæggende omhandler det menneskers ret til at vælge, hvordan de ønsker at leve deres liv og hvilke aspekter, de ønsker skal være private anliggender. Privatlivets fred anses for at være en grundlæggende menneskeret og den første regel der omhandler privatlivets fred er artikel 12 i den universelle menneskerettighedserklæring.

Privatlivets beskyttelse vanskeliggøres af det faktum, at privatlivets fred næsten altid konkurrerer med andre samfundsgoder såsom mobilitet, effektivitet, sikkerhed eller bekvemmelighed. For eksempel: Selvom vi ved, at vores opholdssted kan spores, når vi medbringer en tændt mobiltelefon, ville de fleste af os ikke drømme om at lade telefonen blive hjemme! Og hovedparten af os foretrækker at have en RFID chip i vores bil, frem for at vente i kø for at betale (anonymt) med kontanter, når vi betaler vejafgift.

Forskning viser, at mange mennesker ikke bekymrer sig om teknologi, der overskrider privatlivets grænser, fordi de føler, at de ikke har noget at skjule. Eksperter frygter, at dette vil resultere i, at samfundsborgerne mister dele af deres privatliv, som det kan blive vanskeligt at genvinde, når de først en gang er gået tabt. Selv den mest loyldige borger kan befinde sig i en situation, hvor han ikke ønsker at blive iagttaget eller sporet.

Kritikere af sikkerhedsteknologi og overvågning hævder, at mange af de tiltag, som implementeres, ikke egner sig til terrorbekæmpelse, men kun til at forsikre offentligheden om, at ”der gøres noget”. Grunden er, at disse tiltag kan omgås, eller fordi den trussel, som de adresserer, er for usandsynlig til at retfærdiggøre den handling, som rettes imod den. Et meget anvendt eksempel herpå er forbudet mod anonyme telefonkort i mange lande. Kritikere af dette forbud hævder, at det kun forhindrer opkald fra almindelige mennesker, som gerne vil være

anonyme. De kriminelle kan på forskellig måde omgå denne lov ved at registrere sig med en falsk identitet eller ved at anvende stjalne mobiltelefoner.

Nogle terrorlovs initiativer, især i USA, overskrider i udpræget grad privatlivets grænser. Det drejer sig om aflytning af telefonsamtaler, screening af elektronisk kommunikation uden kendelse eller profilering af en person på baggrund af data, indsamlet fra forskellige kilder, uden at den pågældende person er blevet informeret.

Et vigtigt princip, der vedrører privatlivets fred, er, at det enkelte individ bør informeres, når hans eller hendes personlige data oplagres og analyseres og at det bør være muligt for individet at få adgang til disse data og bekræfte, at de er korrekte. Personlige data bør kun opsamles og lagres, hvis det virkelig er nødvendigt og de bør slettes, når der ikke længere er behov for dem i relation til det oprindelige formål.

Hvad er din holdning til sikkerhedsteknologier?

- Inspirerende scenarier til diskussion.

I den følgende sektion vil vi introducere dig for Carlas og Peters historier. Vi vil følge dem i deres møder med forskellige sikkerhedsteknologier og sikkerhedsmidler og dele deres tanker og ideer om disse forhold. For at kunne generalisere disse scenarier har vi undgået at anvende specifikke lande, byer eller lufthavne som eksempler. I stedet har vi forsøgt at vise, hvorledes forskellige lande – og autoriteter på sikkerhedsområdet – har valgt forskellige tilgange til at implementere sikkerhedsteknologi. Scenarierne er placeret et sted i fremtiden, for at demonstrere anvendelsen af forskellige sikkerhedsteknologier eller lovgivning, som endnu ikke er trådt i kraft.

Vi håber, at disse historier vil inspirere dig til at reflektere over sikkerhed og privatliv og din holdning til disse to værdier.

Carla er 62. Hun har arbejdet som lærerinde hele sit liv, men hun overvejer nu at gå tidligt på pension. Alt er blevet så teknisk nu om stunder! Og børnene er mere støjende end tidligere. Måske er hun ved at blive gammel? I denne uge vil hun imidlertid ikke bekymre sig om det. Det er først på sommerferien og hun skal besøge sin søn i nabolandet.

Carla stiger ombord i metrotoget for at tage til hovedbanegården. Hun har opgraderet sin *universalbillet* og anvender den til at betale for sin rejse ved at holde den op mod aflæseren ved indgangen. Billetten er et plastik kort, som indeholder en lille chip. Chippen holder styr på, hvor mange rejser hun har tilbage på sit kort. Carla har valgt en såkaldt anonym billet. Hun er klar over, at dette betyder, at pengene er gået tabt, hvis hun skulle tabe sin billet. Det er desuden en smule besværligt, idet hun skal medbringe det ekstra kort. Den almindelige *universalbillet* er selvfølgelig indbefattet i ejerens *mobilenhed*. Man skal blot bære enheden på sig eller i sin pung og identificere sig med fingeraftryk, når man går forbi kontrollen.

Carla kan ikke gøre for det, men hun synes, at det er ubehageligt at skulle bruge fingeraftryk til at identificere sig med. Hun har selvfølgelig bemærket, at de unge nu om dage overhovedet ikke ser ud til at bekymre sig om det, men for hende vil det altid være forbundet med kriminalitet og arrestationer. “Det er slemt nok, at man skal udlevere sit fingeraftryk og vise sit ID kort, når man vil rejse udenlands,” tænker hun. Hun vil helt sikkert ikke gøre det oftere end strengt nødvendigt!

Biometri

Biometrisk teknologi identificerer individer automatisk ved at anvende deres biologiske og adfærdsmæssige karakteristika. Biometri kan anvendes til at kontrollere tilgang til fysiske lokaliteter eller til information (computere og dokumenter). De mest almindeligt anvendte former for biometri er fingeraftryk og ansigtstræk.

Processen, hvor en persons biometri sammenlignes med en tidligere gemt skabelon, kaldes *matching*. Et *match* angiver en score. Hvorvidt personen bliver accepteret eller afvist afhænger af, om denne score overskrider en vis tærskel.

I de fleste tilfælde opbevares det biometriske billede som en *skabelon*, en digital repræsentation af biometrien. Skabelonen er skabt ved hjælp af en algoritme. Af hensyn til vedkommendes privatliv anbefales det, at kun skabelonen opbevares og at det oprindelige billede slettes. I forskellige kontrolsystemer sker det dog ofte, at det oprindelige billede bevares, fx ved brug af biometriske pas og systemer, der kan genkende ansigtstræk.

Vi skelner mellem *identifikation*, som indebærer, at man finder ud af, hvem en person er ved at sammenligne hans eller hendes biometriske aftryk med alle de skabeloner, som er opbevaret i et system, og *autentificering* (bekræftelse), hvor individet i fokus sammenlignes med hans eller hendes arkiverede skabelon for at verificere, at personen rent faktisk er den, han eller hun giver sig ud for at være.

En af udfordringerne ved et biometrisk system er at finde den rette balance mellem den falske acceptrate (FAR) og den falske afvisningsrate (FRR). *Falsk accept* (eller *falsk positiv*) indebærer, at et system identificerer et forkert individ. Hvis systemet ikke identificerer et individ, der er registreret, kaldes det *falsk afvisning* (eller *falsk negativ*).

En af de store fordele ved biometrien er, at den er så stærkt knyttet til en person. Biometrisk autentificering giver bedre adgangskontrol og identitetstyveri bliver meget vanskeligere, når personlige data kun kan forbindes med den rigtige person. Men dette er også den største risiko ved biometriske systemer. Når først et sæt biometriske data er blevet kompromitteret, er det kompromitteret for altid.

Peter er 32. Han arbejder som salgsrepræsentant for en bilforhandler. Her til morgen er han stået tidligt op for at tage til en biludstilling i Centraleuropa. Han står op, tager et hurtigt brusebad, snupper sin taske og tager afsted til lufthavnen. Han er som sædvanlig forsinket, men da han er registreret til *hurtig check-in*, skulle alt være i orden. Den hurtige check-in service tillader ham at springe over alt bøvlet, hvor pas skal forevises, passagererne sammenholdes med kriminelle profiler og

selvfølgelig det gennemgribende sikkerhedscheck. Med den hurtige check-in service gennemgår man én gang for alle en særligt omfattende indregistreringsprocedure – og lader lufthavnen opvare alle sine data. Til gengæld kan man så slippe for den almindelige check-in og blot ved hjælp af biometrisk teknologi ved indgangen godtgøre, at man er den, man er.

Peter sender en tanke til sin kollega, som han synes er for fikseret på privatlivets fred. Kollegaen synes, at der er for megen overvågning i samfundet for øjeblikket og nu vil han ikke engang tillade, at der er cookies på hans computer! Han har endda afinstalleret Googles toolbar – det er der bare ikke nogen, der gør! Hvis det var sandt, at amerikanske efterretningsorganisationer anvender disse data til at kortlægge netværk og søge efter mistænkelige profiler, så ville det da helt sikkert være almindeligt kendt? Lige nu har han sikkert været oppe et par timer og står allerede i kø ved check-in og sikkerhedskontrollen. Nå, men han har jo selv bedt om det! Peter håber bare, at hans kollega kommer igennem sikkerhedskontrollen tidsnok til, at de kan gennemgå deres præsentation en sidste gang, før de går ombord.

- 0 -

Carla ankommer til hovedbanegården. Som i undergrundsbanen er der kameraer alle vegne. Skærme og højtalere på væggene gentager advarsler om sikkerhed, indtil ingen længere bemærker dem. ”Hold Deres bagage under opsyn.” ”Deres billede vil blive sammenlignet med en database med kendte terrorister.” Der var en debat om dette for et par år siden. Mange lande fortæller ikke, at de tager billeder og checker dem i forskellige databaser og det blev foreslået, at det heller ikke skulle være nødvendigt at gøre det her. Men regeringen udtrykte sig vældigt klart omkring det princip, at folk bør vide hvornår og hvor de

bliver checket. ”Det er særligt vigtigt, når man ikke selv er opmærksom på, at det sker. Man kan ikke længere vide, om man bliver fotograferet eller ej,” reflekterer Carla. Hun har hørt, at der er lande, hvor man også screener folks e-mails og telefonsamtaler for ord eller fraser, som er mistænkelige. Men det kan vel helt sikkert kun være rygter!

Carla føler sig lidt stresset med al den støj og sætter kurs mod *stillerummet*. Hun skal vise sit ID for at komme ind, men så snart hun er inde, slapper hun af. ”Ingen kameraer, ingen mobiltelefoner, ingen wifi zone, ingen støjende advarsler! Der burde virkelig være flere af den slags teknologifri zoner,” tænker hun.

Det er ikke fordi, at hun ikke er vant til kameraer. De har været en del af bybilledet hele hendes voksenliv, men er de ikke blevet en smule mere nærgående på det sidste? Efter man begyndte at anvende software til både ansigts- og mønstergenkendelse, føler hun sig mere observeret og evalueret end før: ”Bevæger jeg mig som en terrorist nu?” Bare tanken om hvor pinligt, det ville være at gøre noget, som ville forårsage, at hun ville blive stoppet og checket af antiterrorkorpsset! Rent faktisk er hun aldrig blevet standset, men hun kan ikke lade være med at tænke over det, når der er kameraer i nærheden.

Som de fleste andre kender hun en, som faktisk blev mistænkt for at være terrorist. Da teknologien var på sit tidlige stadium, var der en del problemer med software til ansigtsgenkendelse. Og fordi politikerne ikke ønskede en skandale hvor en person, der var på listen over mistænkte, kom afsted med at snyde systemet, var resultatet en del såkaldte *falske positive*.

En af hendes kolleger, hvis forældre er fra Iran, blev mistænkt for at være terrorist. Han fandt det meget ydmygende og det bebrejder hun ham ikke. Som han sagde:

Kameraovervågning - Closed Circuit Television (CCTV)

CCTV overvågning med *aktive kameraer* fungerer på den måde, at en operatør betragter skærmen og kontrollerer kameraet (ved at dreje og zoome), så det følger et individ eller en situation, som udvikler sig. Aktive kameraer kan anvendes med automatiske visuelle overvågningsprogrammer, som anvender algoritmer til at spore mistænkelige bevægelser eller identificere mennesker ved at sammenligne deres billede med billeder i en database.

Passive kameraer optager, hvad der sker på specifikke steder (for eksempel i en kiosk) på bånd. Båndet ses kun, hvis der er et optrin, som f.eks. et røveri, et slagsmål etc. De tidligere CCTV systemer var analoge, men nu udbredes digitale systemer i stadig stigende grad. Digital billedsøgning kan spare tid, når man skal lokalisere specifikke begivenheder eller spore mistænkte ved at sammenholde dem med en eksisterende database. Men det er et problem, at sådanne billeder også nemt kan manipuleres.

Automatisk Ansigtsgenkendelse

Systemer til automatisk ansigtsgenkendelse tager automatisk et billede af en person, hvorefter det sammenholdes med en database med henblik på identifikation og autentificering. Identifikationen af en tilfældig person, baseret på denne teknik, ville kræve en meget stor database og en behandlingskapacitet, der går ud over, hvad der er muligt i dag. Sådanne systemer anvendes derfor normalt til at verificere, at en person ikke er på en liste over f. eks. kendte kriminelle og terrorister.

Automatisk Nummerplade Genkendelse (ANPR)

ANPR systemer registrerer nummerplader optaget på CCTV og sammenholder dem med en database. Systemer, der kan genkende nummerplader, anvendes i adskillige lande. De anvendes mest ved afgiftsbomme eller ved hastighedskameraer, men de anvendes også til at identificere stjålne biler.

“Når du er blevet arresteret af et antiterrorkorps i skudsikre veste og du ser ud, som jeg gør, så ser folk anderledes på dig bagefter – også selvom du får en undskyldning, når du bliver løsladt.” Carla ved, at han i tiden derefter holdt sig væk

fra områder med megen kameraovervågning, især når han havde sine børn med sig.

På det seneste har flere og flere mennesker sat spørgsmålstegn ved kameraernes berettigelse og effektivitet. I nogle områder af byen forsøger man nu at installere bedre og skarpere gadelygter. Det forlyder, at resultaterne er gode!

- o -

Da Peter arbejder for en bilforhandler, har han altid den nyeste bilmodel. Den som han kører i for øjeblikket har alle de nyeste teknologier: Galileo satellit forbindelse med navigationssystem, automatisk nødopkald gennem eCall systemet og en del andre sikkerhedssystemer. Peter er ikke engang sikker på, hvad alle funktionerne går ud på. I alle nye biler er eCall funktionen nu standard inventar. Hvis bilen bliver involveret i en ulykke, ringer eCall automatisk til nødcentralen. Da eCall er forbundet med Galileo systemet, angiver det bilens nøjagtige position.

Gennem de seneste år har der været forslag om, at teknologien skulle anvendes til andre formål også. Efter et mislykket terrorangreb i Berlin, stjal terroristerne en bil og flygtede gennem Tyskland. Det viste sig så, at systemet også kunne anvendes til at spore bilen og endda standse den! Bilen var nemlig en dyr model med den sidste nye teknologi indenfor tyveribeskyttelse og den kunne faktisk standses med fjernkontrol via en satellit. Terroristerne blev standset og arresteret og derefter blev EU staterne enige om, at systemet også burde kunne anvendes af politiet til at spore kriminelle og terrormistænkte

Efter en forskningsrapport, der beskrev, hvor mange liv, der kunne reddes i trafikken, hvis fartgrænserne blev respekteret af bilisterne, blev det foreslået, at sikkerhedssystemerne burde indeholde et modul, som kunne sammenholde

fartgrænserne med bilens speedometer. Det oprindelige forslag var, at en chip i motoren skulle sikre, at ingen biler kunne overskride fartgrænsen, men dette blev mødt med stærke protester både fra bilindustrien og fra bilejerforeninger. For øjeblikket er systemet udformet sådan, at hver gang en bil overskrider fartgrænsen, foretages der et opkald til det centrale bøderegister, hvor bøden automatisk betales via bilejerens konto.

Lokaliseringsteknologi

Det er muligt at beregne den omtrentlige position af en brugers mobile udstyr ved at anvende GSM base stationernes kendte koordinater.

Hvis man ønsker mere akkurate positioner, anvender man satellitbaserede systemer:

GPS er en forkortelse af *Global Positioning System*, et verdensomspændende satellit navigationssystem, bestående af 24 satellitter i kredsløb om jorden. Ved at anvende tre satellitter, kan GPS beregne modtagerens længdegrad og breddegrad baseret på de punkter, hvor de tre sfærer overlapper. Ved at anvende fire satellitter kan GPS også bestemme højden.

Galileo vil blive et globalt netværk af 30 satellitter, som leverer præcis timing og stedsbestemmelse til brugere på jorden og i luften. Planen er, at det skal være klar til brug i 2010. Det vil blive mere nøjagtigt end GPS systemet og det vil have større gennemtrængningsevne.

eCall

eCall indeholder sensorer, som aktiveres i tilfælde af en ulykke. Den kontakter alarmcentralen og videregiver information om ulykken, inklusiv tidspunkt, præcis lokalisering og identifikation af bilen.

Dette udstyr vil ikke være tilsluttet et mobilt netværk på en permanent basis. Det vil kun tilslutte sig, efter at det er blevet aktiveret. Der er dog bekymring for, at dette kan ændre sig med hensyn til transmission af yderligere data (for eksempel til forsikringselskaber). Desuden kan der være risiko for mulig uautoriseret adgang til databaser, hvor eCall data oplagres. Fra September 2009, vil alle nye biler i deltagerlandene være udstyret med e-Call.

Peter trykker på speederen. Alle vejstrækninger er stadig ikke opdaterede i systemet og han har overført en oversigt til sit navigationssystem. Han får en advarsel, hver gang han passerer et skilt, som er forbundet med systemet – hvilket betyder, at han er ”nødt til” at respektere fartgrænsen. ”Det er fint, at overvågningen virker begge veje,” tænker han.

Peter ankommer til lufthavnen. Hans nummerplade er allerede i systemet og hans bil registreres automatisk, da han

kører ind på parkeringspladsen. Det er den samme teknologi, som anvendes i byerne til at identificere stjalne biler. Han troede faktisk, at sådant et system ville være overflødigt efter at eCall opkoblingen til Galileo var implementeret, men tilsyneladende ved de mere organiserede bander, hvordan man kobler systemet fra. Han ved også, at nogle lande endog også kræver, at føreren selv skal være i stand til at slå eCall systemet fra. Denne type krav gør det altid vanskeligere for bilindustrien! Og hvordan kan det være, at de kriminelle altid synes at være et skridt foran teknologien?

Han parkerer bilen, står ud og går hen mod terminalen og den hurtige check-in. Han placerer sin finger på sensoren og ser direkte ind i kameraet. Et grønt lys blinker og døren åbner sig.

Selvom sensorerne er en del bedre, end de plejede at være, har nogle mennesker stadig problemer med at bruge fingeraftryk; hans bedstefar for eksempel. Selvom han er i rigtig god form for en 80-årig mand, bliver han mere og mere isoleret. Nu om dage skal man anvende sit fingeraftryk sammen med sit ID overalt. Han gider ikke altid det bøvl, som man skal igennem, når sensoren ikke kan aflæse ens aftryk. Så for det meste bliver han hjemme.

Peter går nogle gange på biblioteket for at låne *rigtige* bøger til ham. Det morer ham,

”Function Creep”

Databaser er sårbare overfor såkaldt function creep. Dette begreb dækker anvendelse af data til et andet formål end det oprindeligt tiltænkte. Et eksempel på en sådan function creep var, da den norske database over asylansøgere – som også indeholder biometrisk information såsom fingeraftryk – blev gjort tilgængelig for politiet i dets efterforskning af kriminalitet. Databasens oprindelige formål var, at hjælpe med at fastslå asylansøgernes identitet.

at tænke på, hvordan hans biblioteksprofil ser ud. Skulle den nogensinde blive analyseret i forbindelse med en eftersøgning af mistænkelige individer, ville sikkerhedsagenterne nok undre sig over, hvorfor en mand i trediveerne låner bøger som ”Dating for Seniorer” and ”Vore Venner Fuglene”.

For nogle få år siden, lige efter at et stort terrorangreb blev forhindret i USA, blev det rent faktisk foreslået, at sikkerhedsorganisationer skulle have lov til at søge i alle databaser. Det var ikke blot databaser, som indeholdt data om folk, der var mistænkt for forbrydelser og terror. De ønskede også at analysere alt materialet i biblioteksdataene, elektricitets- og gasforbrugsmønstre, data vedrørende telefon og Internet, rejsedata og indkøbsmønstre. Ved at søge efter mistænkelige mønstre ville de identificere mulige terrorister.

Alex, hans kollega, havde været forarget og Peter havde forsøgt at diskutere det med ham; de ville da helt sikkert ikke bede om dette, hvis ikke de havde gode grunde til det? Skulle myndighederne ikke gøre, hvad der stod i deres magt for at fange terroristerne? Alex var ikke overbevist og havde argumenteret for, at undersøgelsen i det mindste skulle udføres på anonyme data: ”Hvis de finder noget mistænkeligt, kan de skaffe en retskendelse og derpå få den pågældendes identitet at vide. Der er ikke nogen legitim grund til, at de skal vide alt om alle!”

Peter havde ikke rigtig været interesseret i at debattere emnet yderligere, men hans kollega var blevet ved og ved i hver frokostpause og til sidst havde han underskrevet en protestskrivelse imod forslaget. ”Men jeg kan ikke rigtig se formålet,” sagde han. ”Det kan da kun være et problem for dem, der har noget at skjule?” På den anden side tog han sig selv i at spekulere over, om det mon blev registreret et eller andet sted, at han underskrev den protest...

”Total Information Awareness” (TIA)

Total Information Awareness (TIA) blev udviklet af det amerikanske forsvars Advanced Research Projects Agency (DARPA). TIA programmet indeholdt værktøjer i tre kategorier: sproglig oversættelse, datasøgning og mønstergenkendelse, samt avancerede redskaber til at fremme samarbejde og forbedre grundlaget for at træffe beslutninger.

Målsætningen med TIA var at forudsige terrorangreb, før de fandt sted. Systemet skulle scanne private og offentlige databaser, såvel som Internettet, for at spore transaktioner, der kunne associeres med terrorangreb. Den amerikanske kongres standsede den økonomiske støtte til TIA i september 2003, men mange af systemets programmer lever videre under andre navne.

Carla sidder et stykke tid i stillezonen og læser en bog, hvorefter hun går hen mod sikkerheds-gaten.

Sikkerheds-gaten i den internationale togterminal opstod som et resultat af et øget krav om kontrol, ikke blot i lufthavne, men også andre steder, hvor mange mennesker er forsamlede. Hun ved, at i nogle lande er der endog sikkerhedscheck ved indgange til butiksarkader og sportspladser. For et par år siden blev en bombemand fanget i en butiksarkade ikke langt fra det sted, hvor hendes søn bor. Det fremgik, at man netop var begyndt at anvende scanningsudstyr ved indgangen, hvilket bombemanden ikke vidste. Alligevel er hun glad for, at det endnu ikke

er kommet så vidt i hendes eget land. Indtil videre er det kun lufthavne og togstationer, der har sikkerhedskontrol med scanning af passagerer.

Hun bekymrer sig ikke selv så meget om butiksarkader – der har jo ikke været nogen trusler mod hendes land, så vidt hun ved. Men hun har set statistikker, der viser, at flere mennesker nu igen handler i de mindre butikker i byer og bycentre. Desuden har hun hørt, at butiksarkadernes overskud falder, fordi de ikke har tilladelse til at opstille scanningsudstyr, som fx ”the naked machine”,

Carla tager sit pas frem og går op til iris scanneren. Hun ved, at nogle lande stadig anvender fingeraftryk i deres ID og pas. Men hun synes at iris scanningen er sikrere. Aflæseren sammenligner hendes iris med skabelonen, der er lagret i hendes pas. Dette bekymrer hende, men hendes søn, som arbejder i IT industrien, har forsikret hende om, at det er fuldstændigt sikkert nu. ”Den oprindelige kryptering i det første pas var ret svag,” sagde han, ”men med den kryptering, der anvendes nu, ville en supercomputer skulle anvende tusinder af år til at knække krypteringen! For øvrigt lagrede man i de tidlige pas de rigtige billeder af ansigt, fingeraftryk, og iris. Nu lagrer de kun en *skabelon* – en digital repræsentation af det vigtigste aspekt i et givet ansigt eller en given iris. Selv hvis nogen skulle kunne knække krypteringen, ville de ikke kunne genskabe det enkelte ansigt eller den enkelte iris for at give sig ud for at være den person, som passet tilhører.”

Hun er også blevet forsikret om, at aflæseren kun lagrer hendes iris skabelon så længe, som det tager, at sammenligne den med den skabelon, der findes på hendes pas og at det ikke oplagres i en central database. Hun er ikke så sikker på, hvad der sker, når hendes pas aflæses ved en anden grænse. Blicher data også slettet der efter sammenligningen?

Radio Frekvens Identifikation (RFID)

RFID er et system, der anvender radiobølger til automatisk identifikation. Bittesmå integrerede kredsløb (tags), der indeholder information, er tilknyttet dokumenter eller integreret i produkter. En aflæser kan anvendes til at læse informationen på disse kredsløb/tags indenfor en vis afstand.

RFID tags fås som både *aktive* og *passive* tags. Aktive tags har - ligesom de kort, der anvendes til at passere afgiftsbomme – et batteri og vil derfor være større end de passive tags, men de kan indeholde mere information og fungere over længere afstande. Passive tags indeholder ikke noget batteri, men får deres energi fra aflæserens radiosignal. En typisk anvendelse af passive tags ses i det nye europæiske pas.

De fleste tags kommunikerer med en hvilken som helst aflæser, men der er også tags, som kræver, at aflæseren afgiver et password, eller et andet legitimering.

Biometrisk Pas

Et biometrisk pas består af det egentlige dokument, normalt i form af en lille bog, og en lille chip.

Chippen indeholder obligatoriske og valgfrie data. Derudover er der et fotografi af brugeren, der fungerer som et visuelt link mellem ejeren og passet.

The International Civil Aviation Organization (ICAO) har valgt at anvende en chip, som kan læses på afstand (som en RFID tag). ICAO har valgt at anvende *ansigt*, som den primære biometri i pas. *Fingeraftryk* og *iris* anbefales som sekundære biometrier. EU har valgt kun at anvende fingeraftryk som dets sekundære biometri.

Biometriske pas har givet anledning til megen debat, især hvad angår sikkerheden omkring den biometriske information. Det frygtedes, at informationen kan stjæles ved skimming (aflæsning på afstand, uden at ejeren er opmærksom på det) eller aflytning (opsnapning af informationen, når den bliver transmitteret).

For at tage hånd om disse spørgsmål er der udviklet et program for grundlæggende adgangskontrol (*basic access control* (BAC)). I BAC anvender aflæsningssystemet en "nøgle", som er lavet ud fra numeriske dataelementer i den maskinelle aflæsningszone (stregkoden), til

at "oplåse" chippen, således at systemet kan aflæse det. BAC er blevet kritiseret for ikke at være sikkert nok og sikkerhedseksperter har på meget kort tid kunnet knække krypteringen. Hun husker, at der var en skandale for et par år siden vedrørende en central database for fingeraftryk – var det i USA? En del fingeraftryk blev stjålet af en ansat og solgt til internationale kriminelle. Tusinder af mennesker fik deres identiteter stjålet og oplevede alle mulige problemer – fra at blive sortlistet ved grænser til at deres bankkonti blev tømt. Det var specielt vanskeligt, fordi det tog så lang tid før regeringen ville indrømme, at den havde mistet de omtalte data. I mellemtiden troede ingen på, at deres identitet var blevet stjålet – eller at det overhovedet var muligt at bruge en anden persons fingeraftryk til at stjæle vedkommendes identitet!

Men Carla ved bedre. Sidste sommer fik en af hendes søns venner stjålet sit ID lige før han og hans familie skulle på ferie. Han var bange for, at de ville blive nødt til at aflyse alt, fordi han ville blive sortlistet. Det skete dog ikke, da Schengen informationssystemet, som anvendes i mange europæiske lande, registrerer mennesker, hvis identitet er blevet stjålet. Af denne grund kunne han og hans familie rejse som planlagt og han blev aldrig anklaget for at være kriminel eller terrorist, selvom hans ID formodentlig blev checket grundigere end en gennemsnitsrejsendes.

Efter et ID check, skal Carla sende sin bagage gennem scanneren, før hun går gennem det, der tidligere blev kaldt "*the naked machine*". Hun er lettet over, at den virkelige "naked machine" aldrig blev indkøbt

til lufthavne og internationale togterminaler i hendes hjemland. Sikkerhedsautoriteterne evaluerede forskellige maskiner, men besluttede, at det var lige så sikkert at have en type maskine,

Scanning af passagerer (*Naked machine*)

Teknologier såsom røntgen med tilbagespredning (*backscatter X-rays*) eller Terahertz stråling trænger bedre gennem materialer end almindelig optik. Dette betyder, at det kan anvendes til sporing og visualisering af genstande, gemt under tøj.

En "naked machine" anvender denne type teknologi til at afsløre, om der er våben eller eksplosiver gemt på en given persons krop. Der er forskellige systemer i anvendelse. Nogle afslører alt, hvad der er under tøj – ikke bare skydevåben og eksplosiver – deraf navnet. Denne type lufthavnssikkerhed er blevet testet i Heathrow (Terminal 4) siden 2004. Andre anvendelser danner billeder af de skjulte genstande og projicerer dem op på en kønsløs mannequin.

hvor genstande, skjult under tøj, projiceres over på et neutralt billede af den givne person.

Selv i en alder af 62 er Carla bevidst omkring sin krop. Hun er glad for, at de unge mænd ved sikkerhedsindgangen ikke får hende at se nøgen. Hun skal tage sine sko af, men derudover har hun ingen problemer og snart sidder hun igen komfortabelt i toget.

- o -

Peter går igennem lufthavnshallen over til sikkerhedsafdelingen. Selvfølgelig skal de passagerer, der foretager det hurtige check-in også igennem et sikkerhedscheck, men de har deres egen indgang og de gennemgår alle kontrollen på en professionel måde. Ingen i denne indgang bruger bæltet med metalspænder eller er så amatøragtige, at de har mønter liggende løst i lommerne. Og det er flere år siden, at sko fremstillet til forretnings segmentet indeholdt metal. Han trækker maven ind og passerer gennem *the naked machine*. "Hvorfor er temperaturen altid så lav i dette rum?" tænker han, og rødmer, da han ser, at en af sikkerhedsvagterne er en kvinde omtrent på hans egen alder. Han er dog stadig glad for, at lufthavnen anvender

Opbevaring af data

En database defineres som en organiseret samling af data. Det er et velkendt fænomen, at når man sammenholder forskellige data om en person, så afslører det mere om personen, end de enkelte informationer hver for sig. Et vigtigt princip for sikringen af privatlivets fred, som er relateret til databaser, der indeholder information om personer, er derfor, at kun data, som er nødvendige for at opfylde systemets formål, bør lagres og at data bør slettes, når de ikke længere er nødvendige.

På det seneste er der opstået en trend, hvor regeringer har ønsket at oplagre flere data og sammenkøre databasesystemer med andre formål for øje end det oprindelige, for eksempel sikkerhedsformål. Den type data, som der oftest refereres til, når man diskuterer tilbageholdelse af data, er data relateret til IKT (Informations og kommunikationsteknologi), såsom kommunikationsdata fra telefoner, mobiltelefoner og Internet trafik.

EU har godkendt et direktiv vedrørende opbevaring af sådanne data. Data som er relateret til hvem, der kommunikerer hvor og hvornår, vil blive lagret, men ikke kommunikationens indhold. Disse data kan blive lagret i op til to år.

Forskellige amerikanske ministerier rapporterede i 2005, at de havde købt personlig information af såkaldte informationshandlere (*information resellers*) for cirka 30 millioner amerikanske dollars. Disse virksomheder samler og oplagrer personlige informationer fra mange kilder og gør det tilgængeligt for deres kunder. Kilderne kan være offentlige systemer, informationer, der er tilgængelige for offentligheden (for eksempel via Internettet) og informationer fra virksomhedsspecifikke kilder, såsom private foretagender.

den *rigtige* naked machine. Det føles på en eller anden måde sikrere.

Peter bemærker et supplement til sikkerheds-checket, som han ikke har set før. Efter *the naked machine* er der endnu en scanner, som nogle af passagererne anmodes om at passere igennem. Han husker svagt noget om, at et nyt sikkerhedselement er ved at blive afprøvet i denne lufthavn. Det skulle kunne registrere værdier for kropsvarme, sved,

puls... værdier, der kan være indikationer på sygdomme såsom SARS eller fugleinfluenza eller vise, at en person er nervøs. Nogle af de undersøgte personer eskorteres til nærliggende afhøringsrum. Han er glad for, at han ikke blev udtaget til denne test, selvom han er sund og rask og har ren samvittighed. ”Men at afprøve den ved hurtig check-in? Ved de ikke, at folk, der anvender denne indgang, har travlt?”

Han sætter kurs mod udgangen og finder en stol. Måske skulle han ringe til Yasmin og fortælle hende, at han er på vej? Hun arbejder for den bilfabrikant, som hans forhandler repræsenterer og han mødte hende på den sidste biludstilling, han besøgte. De var på bølgelængde med det samme og han ville rigtig gerne møde hende igen. På den anden side tøver han med at ringe til hende fra sin mobil. Han ved, at Yasmins bror er meget aktiv i en ungdomsgruppe i sin moské og at Yasmin, som en del af broderens netværk, formodentlig er på en eller anden overvågningsliste. Han ville ønske, at han havde købt nogle anonyme telefonkort, sidst han var i Asien. Det er ikke længere lovligt at sælge disse kort i Europa.

Aflytning

Der findes forskellige metoder til at overvåge borgere og interaktion mellem borgere, enten via Internettet eller i nærmere definerede områder. En form for aflytning er telefonaflytning. Her installeres der et aflytningsapparat på linien mellem de to telefoner, som bruges i samtalen. Apparatet kan installeres i den mistænkte telefon eller i telefoner, som han eller hun formodes at ville kontakte.

En udvidet version af *aflytning* er overvågning af alle kommunikationslinier (fastnettelefoner, mobiltelefoner, Internet) i søgen efter samtaler, der kunne være interessante. Et eksempel på det er Echelon netværket, der drives i samarbejde mellem USA, UK, Canada, Australien og New Zealand. Systemet blev oprindeligt etableret for at overvåge kommunikation i eller til Sovjetunionen og Østeuropa. Kommunikationsmønstre kan analyseres og indhold kan scannes for interessante nøgleord.

Han ønsker heller ikke at anvende Internettet her. Hvem ved, hvad lufthavnens netværk lagrer af informationer. Han er heller ikke sikker på, hvordan reglerne er nu om dage. Har politiet direkte adgang til denne type data eller skal de bruge en kendelse? Han ønsker pludselig, at han havde være mere opmærksom i debatten om privatlivets fred. Han vil helt klart spørge sin kollega, når han kommer ombord på flyet.

Sidste gang han spiste middag med Yasmin, nævnte hun, at hun var sikker på, at hendes e-mail blev scannet og hun bad ham om at bruge et krypteringsprogram, hvis han ønskede at skrive til hende. ”En ukrypteret e-mail er som et postkort,” forklarede hun. ”Enhver, som får adgang til den kan læse den – vidste du ikke det?”

Han havde faktisk tænkt sig at skrive til hende, men han opdagede, at det mailprogram, som de anvender på arbejdet, ikke har indbygget kryptering og han fik aldrig installeret et krypteringsprogram. Han håber, at hun ikke er fornærmet over, at han har ignoreret hende i al den tid. ”Jeg forklarer det, når vi mødes,” tænker han.

Så er det tid til at gå ombord på flyet. Han ankommer til indgangen, placerer sin finger på sensoren og går ombord som en af de første passagerer. Der er stadig masser af plads til håndbagage. Han sender en tanke til sin kollega, som formodentlig stadig står i kø ved sikkerhedskontrollen, før han læner sig tilbage og lukker øjnene.

- o -

”Min mor er på vej,” siger Carla’s søn til sin kone, efter at han har modtaget en besked på sin mobil. ”Hun burde være her om cirka tre timer.” Hans mor ved det ikke, men den nye mobiltelefon, hun fik i julegave, er forbundet til en børneovervågningservice (*Kid-watch*). Teknologien er en ny version af de sporesystemer, som man kunne se i gamle

Privatlivsfremmende Teknologier

Teknologier som bidrager direkte til at opretholde privatlivets fred går under navnet *Privacy Enhancing Technologies* (PETs).

Anonymisering er en sådan PET. Der findes tjenester, der kan sikre anonym elektronisk kommunikation for almindelige brugere. Sådanne teknologier skjuler forbindelsen mellem brugeren og de spor, han eller hun efterlader sig og kan derfor forebygge uønsket identifikation. Traditionel kontant betaling og uregistrerede (anonyme) telefonkort er midler, som er beregnede til at yde anonymitet.

Forvaltning af identiteter (*identity management*) er også en variation af PET: i nogle tilfælde ønsker man ikke at identificere sig, men anvender et pseudonym (for eksempel i Internet fora). For at gøre det vanskeligere at sammenkøre data, kan det være en god idé at have forskellige brugernavne (som ikke afslører din identitet) og passwords til forskellige formål. Programmer til forvaltning af identiteter hjælper folk med at holde styr på deres forskellige brugernavne. I nogle tilfælde kan det forekomme, at en tjeneste kun anvendes til at verificere en specifik oplysning – såsom alder eller kreditgrænse. I sådanne tilfælde kan identitetsleverandøren (for eksempel din bank, netværksudbyder, eller arbejdsgiver) fungere som en pålidelig tredjepart og garantere for oplysningen uden at afsløre din identitet.

Kryptering handler om at forvrænge indhold for at gøre det ulæseligt for andre. Fordi al elektronisk kommunikation er sårbar overfor aflytning eller manipulation, er det på mange måder afgørende, at kommunikationen foregår ad krypterede kommunikationslinier eller at det indhold, der transmitteres, er krypteret.

spionfilm, hvor overvågerne kunne se deres mistænkte som små prikker på et kort. Den største forskel er, at ved at anvende den indbyggede Galileo teknologi i mobilenheden kan han følge sin mors bevægelser på et kort,

selv når han sidder i sin egen dagligstue i et andet land.

Han forsøger at lade være med at checke denne funktion for ofte – det føles lidt for meget som at snage i hendes privatliv. Han har dog programmeret den til at sætte en alarm i gang, hvis hun ikke bevæger sig rundt derhjemme i længere tid eller hvis hun ikke er hjemme om natten. Når alt kommer til alt, er hun ved at blive ældre og han kan ikke tage sig af hende på den måde, han synes, han burde, når han bor i et andet land. Hans telefon ringer: ”Hej, det er mor. Jeg er på vej nu – jeg skulle være på stationen om cirka tre timer...”

Annex 4 Questionnaire and interview guide (in Danish)

4.1 Spørgeskema om sikkerhedsteknologi og privatlivets fred

Velkommen til PRISE-projektets spørgeskemaundersøgelse omkring holdningerne til sikkerhedsteknologi og privatlivets fred.

Dette spørgeskema vil præsentere dig for en række spørgsmål. *Du bedes slå en cirkel om tallet ud for det svar, du ønsker at give.* Det er ikke muligt at angive mere end *ét* svar for hvert spørgsmål, med mindre spørgsmålet eksplicit rummer følgende formulering: "Du er velkommen til at angive mere end ét svar på dette spørgsmål". Hvis du kommer til at slå cirkel om et forkert svar, skal du blot strege det ud og slå en cirkel om det rigtige svar i stedet. Du er meget velkommen til at stille spørgsmål undervejs, hvis du er i tvivl om, hvordan spørgsmålene skal forstås.

Baggrundsspørgsmål:

1. Køn

1. Mand
2. Kvinde

2. Alder (*åbent*)

Alder: _____

3. Antal personer i din husstand, inkl. dig selv?

1. 1 person
2. 2 personer
3. 3 personer
4. 4 personer eller flere

4. Har du børn?

1. Ja
2. Nej

5. Er der hjemmeboende børn i husstanden? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Nej
2. Ja, i alderen 0 – 14 år
3. Ja, over 14 år

6. Hvad er det højeste uddannelsesniveau, du har opnået?

1. Grundskole - 7 års skolegang
2. Mellemskole - 8 eller 9 års skolegang
3. Grundlæggende erhvervsuddannelse (faglært niveau/håndværker uddannet)
4. Gymnasial uddannelse
5. Kortere videregående uddannelse (mindre end 3 års studier)
6. Mellemlang videregående uddannelse (3 - 4 års studier)
7. Lang videregående uddannelse (mere end 4 års studier)

7. Hvad er dit erhverv? (åben tekstboks)

Beskæftigelse: _____

8. Bor du i en by eller på landet?

1. Hovedstadsområdet
2. Provinsby
3. Landdistrikt

9. Hvor ofte bruger du mobiltelefon?

1. Mindst én gang om dagen
2. Mindst én gang om ugen
3. Mindst én gang om måneden
4. Mindre end én gang om måneden
5. Jeg bruger aldrig mobiltelefon

10. Hvor ofte skriver du en e-mail?

1. Mindst én gang om dagen
2. Mindst én gang om ugen
3. Mindst én gang om måneden
4. Mindre end én gang om måneden
5. Jeg skriver aldrig e-mails

11. Hvor ofte bruger du Internettet?

1. Mindst én gang om dagen
2. Mindst én gang om ugen
3. Mindst én gang om måneden
4. Mindre end én gang om måneden
5. Jeg bruger aldrig Internettet

12. Hvor ofte rejser du med offentlig transport?

1. Mindst én gang om dagen
2. Mindst én gang om ugen

3. Mindst én gang om måneden
4. Mindre end én gang om måneden
5. Jeg rejser aldrig med offentlig transport

13. Hvor ofte rejser du med fly (udrejse og hjemrejse tæller som én rejse)?

1. Mere end 5 gange om året
2. 3-5 gange om året
3. 1-2 gange om året
4. Mindre end 1 gang om året
5. Aldrig

14. Hvor ofte kører du i bil?

1. Mindst én gang om dagen
2. Mindst én gang om ugen
3. Mindst én gang om måneden
4. Mindre end én gang om måneden
5. Jeg kører aldrig i bil

Generelle spørgsmål om sikkerhedsteknologi og privatlivets fred.

Nedenfor finder du en række udsagn om sikkerhedsteknologi og privatlivets fred, som ofte dukker op i den offentlige debat. I hvilken grad kan du tilslutte dig disse udsagn?

For hvert udsagn bedes du angive, hvor enig du er

- Hvis du mener, at udsagnet er fuldstændig korrekt, skal du sætte ring om 1 “Helt enig”
- Hvis du mener, at udsagnet er korrekt, men med visse forbehold, skal du sætte ring om 2 “Delvist enig”
- Hvis du finder det umuligt at vurdere, hvorvidt udsagnet er korrekt eller forkert, skal du sætte ring om 5 “Hverken enig eller uenig”
- Hvis du mener, at udsagnet er forkert, men med visse forbehold, skal du sætte ring om 4 “Delvist uenig”
- Hvis du mener, at udsagnet er helt forkert, skal du sætte ring om 3 “Helt uenig”

15. “Samfundets sikkerhed er fuldstændig afhængigt af den fortsatte udvikling og brug af nye sikkerhedsteknologier”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

16. “Mange sikkerhedsteknologier skaber i virkeligheden ikke større sikkerhed, man anvender dem bare for at vise, at der bliver gjort noget for at bekæmpe terror”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

17. “Hvis man ikke har noget at skjule, behøver man heller ikke at være bekymret over de sikkerhedsteknologier, der krænker privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig

4. Delvist uenig

5. Helt uenig

18. “Når nu sikkerhedsteknologien findes, kan vi lige så godt benytte os af den”

1. Helt enig

2. Delvist enig

3. Hverken enig eller uenig

4. Delvist uenig

5. Helt uenig

19. “Privatlivets fred bør ikke krænkes, med mindre der er begrundet mistanke om forbryderisk forsæt”

1. Helt enig

2. Delvist enig

3. Hverken enig eller uenig

4. Delvist uenig

5. Helt uenig

20. “Det er ubehageligt at være under overvågning, også selvom man ikke har noget at skjule”

1. Helt enig

2. Delvist enig

3. Hverken enig eller uenig

4. Delvist uenig

5. Helt uenig

21. “De nye sikkerhedsteknologier vil sandsynligvis blive misbrugt af statslige institutioner”

1. Helt enig

2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

22. “De nye sikkerhedsteknologier vil sandsynligvis blive misbrugt af kriminelle”

1. Helt enig
 2. Delvist enig
 3. Hverken enig eller uenig
 4. Delvist uenig
 5. Helt uenig
-

Sikkerhedsteknologier:

I dette afsnit vil du blive spurgt om din holdning til specifikke sikkerhedsteknologier og anvendelsen af dem.

De grå tekstbokse fortæller meget kortfattet om de teknologier, der indgår i de efterfølgende spørgsmål. Det er noget af den samme information som er i de tidligere udsendte scenarier. Scenarierne rummer yderligere information.

De fleste af spørgsmålene vil kunne besvares med mere end ét svar.

Den anden del af disse spørgsmål drejer sig om specifikke udsagn. For hvert udsagn bedes du angive, i hvilken grad du kan tilslutte dig udsagnet.

Biometri

Biometrisk teknologi kan automatisk identificere personer ud fra deres biologiske eller adfærdsmæssige karakteristika. Biometri kan bruges til at kontrollere adgangen til fysiske lokaliteter eller til information (computere, dokumenter). De mest udbredte former for biometrisk teknologi aflæser fingeraftryk eller ansigtstræk.

Det biometriske billede kan lagres som originalbillede eller i form af en skabelon, en såkaldt *template*, som er en digital repræsentation af biometrien. Af hensyn til privatlivets fred anbefales det, at man kun lagrer skabelonen og sletter det originale billede. Når det gælder retshåndhævelsessystemer som biometriske pas eller systemer til ansigtsgenkendelse, bliver det originale billede imidlertid ofte gemt.

En af de afgørende fordele ved biometrien er, at den er så snævert knyttet til en bestemt person. Biometrisk autentifikation giver mulighed for bedre adgangskontrol og gør det langt sværere at udgive sig for at være en anden, idet de personlige data udelukkende kan knyttes an til den rette person. Men netop dette udgør også det største faremoment ved de biometriske systemer. Hvis biometriske data først er blevet kompromitteret, vil de være kompromitteret for evigt.

Det biometriske pas

Et biometrisk pas består af det konkrete dokument, som er forsynet med en chip, der rummer biometriske data. Denne chip kan aflæses af en sensor på afstand.

Biometriske pas har skabt debat, fordi det frygtedes, at den biometriske information i chippen vil kunne stjæles gennem skimning (trådløs aflæsning af informationen på afstand uden ejerens vidende) eller når den transmitteres.

En af udfordringerne ved biometriske systemer er at finde den rette balance mellem falsk identificering og falsk afvisning. *Falsk identificering* er når et system godkender den forkerte person. Hvis systemet ikke genkender en registreret person, er der tale om en *falsk afvisning*.

23. Hvilke biometriformer vil du kunne acceptere, at man anvender til adgangskontrol? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Ansigtstræk
2. Fingeraftryk
3. Irisgenkendelse
4. Jeg ville ikke bryde mig om, at der blev brugt nogen form for biometri til adgangskontrol
5. Ved ikke

24. Hvor er det acceptabelt at benytte biometri til adgangskontrol? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Acceptabelt i forbindelse med sikkerhedskontrol i banker
2. Acceptabelt i forbindelse med lufthavnssikkerhed
3. Acceptabelt i forbindelse med sikkerhedskontrol i butikker
4. Acceptabelt i forbindelse med grænsekontrol
5. Acceptabelt i forbindelse med sikkerhedskontrol på bus- og togstationer
6. Acceptabelt i forbindelse med sikkerhedskontrol ved store sportsstævner og andre steder/begivenheder, hvor mange mennesker er samlet på ét sted

7. Acceptabelt i forbindelse med sikkerhedskontrol i andre private sammenhænge end de ovennævnte
8. Ikke acceptabelt nogen steder
9. Ved ikke

Specifikke udsagn om biometri

25. “Registrering af biometriske data (f.eks. fingeraftryk eller DNA-prøver) for alle borgere i en central database er et acceptabelt led i bekæmpelsen af kriminalitet”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

26. “Jeg er utryg ved brugen af biometriske pas, da jeg frygter at mine biometriske data bliver stjålet”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

Videovervågning (ITV)

Videovervågning med *aktive kameraer* indebærer, at den, der følger med på skærmen også kan styre kameraet (dreje det, zoome) med henblik på at følge en enkelt person eller en situation, efterhånden som den udvikler sig. Aktive kameraer kan kombineres med automatiserede visuelle overvågningsprogrammer, der benytter algoritmer til at opfange mistænkelig bevægelsesadfærd eller til at identificere folk ved at sammenholde deres visuelle fremtoning med en reference i en database.

Passive kameraer: Disse kameraer registrerer, hvad der sker et specifikt sted (for eksempel i en kiosk) på et bånd. Dette bånd bliver kun afspillet, hvis der bliver begået et røveri, opstår et slagsmål eller lignende.

Automatisk ansigtsgenkendelse

Automatisk ansigtsgenkendelse refererer til systemer, hvor en persons visuelle fremtoning automatisk registreres og sammenholdes med en database med henblik på identificering eller autentifikation. Sådanne systemer anvendes normalt til at verificere, at en person ikke er eftersøgt for kriminalitet eller terror.

Automatisk nummerpladegenkendelse

Systemer til automatisk genkendelse af nummerplader registrerer nummerplader ved hjælp af ITV og sammenholder dem med en database. Sådanne systemer er i brug i flere lande. De anvendes typisk i forbindelse med indkørsler til betalingsveje eller hastighedsovervågning, men de bruges også til at identificere stjålne motorkøretøjer.

Passager-skanning (nøgenmaskiner)

Teknologier så som røntgen eller *Terahertz* gennemstråling har større gennemtrængningsevne over for stof end optisk skanning. Det betyder, at de kan bruges til sporing af genstande, som er gemt under tøjet.

En "nøgenmaskine" bruger teknologi af denne type til at afsløre, hvorvidt en person har skjult våben eller sprængstof på sin krop. Der er forskellige systemer i brug. Nogle af dem afslører alt, hvad man har under tøjet – ikke kun skydevåben og sprængstoffer – deraf navnet. Denne form for lufthavnssikkerhed har været under afprøvning i Heathrow (Terminal 4) siden 2004. Andre systemer affotograferer de skjulte genstande og projicerer dem op på en kønsløs mannequin.

27. Hvor vil du kunne acceptere brugen af videoovervågning? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. I butikker
2. I prøverum i tøjbutikker for at forhindre tyveri
3. På bus- og togstationer
4. I banker
5. I lufthavne
6. På sportsarenaer og i forbindelse med andre steder/begivenheder, hvor mange mennesker er samlet på ét sted
7. I hele det offentlige rum
8. Det kan ikke accepteres nogen steder
9. Ved ikke

28. Hvordan har du det med omfanget af overvågningskameraer, der er opstillet i samfundet generelt?

1. Der burde være flere overvågningskameraer i det offentlige rum

2. Der er et passende antal overvågningskameraer i det offentlige rum
3. Der burde være færre overvågningskameraer i det offentlige rum
4. Der burde slet ikke være nogen overvågningskameraer i det offentlige rum
5. Ved ikke

29. Hvor er det nødvendigt at skanne personer for skjulte genstande pga. sikkerhedshensyn? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. I skoler
2. I forbindelse med sikkerhedskontrol på større bus- og togstationer
3. I lufthavne
4. I shopping centre
5. Det er ikke nødvendigt nogen steder
6. Ved ikke

30. Hvilken type skanning ville du kunne acceptere? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Scanning, der afdækker alt under tøjet
2. Skanning, hvor billeder og skjulte objekter projiceres op på en mannequin
3. Skanning af kropsvarme, sved og hjerterefrekvens
4. Skanning for metalgenstande
5. Røntgenskanning af bagage
6. Skanning kan slet ikke accepteres
7. Ved ikke

Specifikke udsagn om videoovervågning og passagerskanning

31. "Videoovervågning gør, at jeg føler mig mere tryk"

1. Helt enig

2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

32. “Videoovervågning krænker privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

33. “Skanning af personer for at afsløre skjulte genstande er et acceptabelt led i at forebygge terror”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

Positioneringsteknologi

Det er muligt at beregne den omtrentlige position af en brugers mobiludstyr ved hjælp af for eksempel GSM-antenner.

Til mere nøjagtig positionering benyttes satellitbaserede systemer:

GPS er en forkortelse for *Global Positioning System*, som er det system, der anvendes idag. *Galileo*-systemet forventes at være fuldt funktionsdygtigt i 2010. Det vil være mere nøjagtigt og effektivt end GPS-systemet.

eCall

eCall-apparater rummer en række sensorer, der bliver aktiveret efter en ulykke. Det foretager et nødopkald og videresender information om ulykken, herunder tidspunktet og køretøjets nøjagtige position, retning og identitet.

Apparatet vil ikke være permanent opkoblet til et mobilt kommunikationsnetværk. Forbindelsen oprettes først, efter at apparatet er blevet aktiveret. Nogle er imidlertid bekymrede for, om dette ville kunne ændre sig, idet der bliver transmitteret yderligere oplysninger (for eksempel til brug for forsikringsselskaber), eller idet der åbnes mulighed for uautoriseret adgang til de databaser, hvor eCall data bliver registreret. Fra og med september 2009 vil alle nye biler i deltagerlandene være udstyret med eCall.

34. Med hvilke formål for øje er det acceptabelt at lokalisere mobiltelefoner? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Når politiet lokaliserer mobiltelefoner tilhørende folk, der er mistænkt for terror eller kriminalitet, og der foreligger en dommerkendelse
2. Når politiet lokaliserer en hvilken som helst mobiltelefon, også uden dommerkendelse
3. I nødstilfælde, for eksempel hvis der er sket en ulykke, eller hvis en person har mistet orienteringen
4. Det er aldrig acceptabelt
5. Ved ikke

35. Med hvilke formål for øje er det acceptabelt at lokalisere motorkøretøjer? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Når politiet lokaliserer motorkøretøjer tilhørende folk, der er mistænkt for terror eller kriminalitet, og der foreligger en dommerkendelse
2. Når politiet lokaliserer motorkøretøjer i det hele taget, også uden dommerkendelse
3. Når politiet lokaliserer stjålne motorkøretøjer
4. I forbindelse med fartkontrol og fartbøder
5. I forbindelse med automatisk lokalisering og nødopkald i tilfælde af en trafikulykke
6. Det er aldrig acceptabelt
7. Ved ikke

36. Bør der automatisk installeres eCall i alle nye motorkøretøjer?

1. Ja
2. Ja, men det bør være muligt at deaktivere eCall

3. Nej, det bør være valgfrit
4. Nej, det bør aldrig installeres
5. Ved ikke

Specifikke udsagn om positioneringsteknologier

37. “Muligheden for at lokalisere enhver mobiltelefon er en krænkelse af privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

38. “Muligheden for at lokalisere mistænkte mobiltelefoner er et godt værktøj, som politiet bør have adgang til under arbejdet med at opklare og forebygge terror og kriminalitet”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

39. “Muligheden for at lokalisere ethvert motorkøretøj udgør en krænkelse af privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig

5. Helt uenig

40. “Muligheden for at lokalisere ethvert motorkøretøj er et godt værktøj, som politiet bør have adgang til under arbejdet med at opklare og forebygge terror og kriminalitet”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

Registrering af data

En database er defineret som en organiseret samling af data. Det er almindelig anerkendt, at kombinationen af flere forskellige slags information om en person siger mere om denne person end de enkelte informationer, når betragtes hver for sig. I forbindelse med databaser, der rummer information om personer, er det derfor et vigtigt led i beskyttelsen af privatlivets fred, at man kun bør indsamle de data, der er nødvendige for, at det pågældende system kan udfylde sin funktion, og at disse data bør slettes, når der ikke længere er behov for dem.

På det seneste har der været en tendens til, at forskellige landes regeringer har ønsket at registrere flere informationer og at sammenkoble databasesystemer med andre formål for øje end de oprindelige formål, for eksempel af sikkerhedsmæssige årsager. De datatyper, der almindeligvis refereres til, når man diskuterer datalagring, er data fra telefon, mobiltelefon og Internet kommunikation.

Total Informationsbevidsthed eller *Total Information Awareness (TIA)*

Total Information Awareness (TIA) var et projekt under *US Defense Advanced Research Projects Agency (DARPA)*. Projektet omfattede værktøjer i tre forskellige kategorier - sprogoversættelse, data søgning og mønstergenkendelse, og avancerede værktøjer til samarbejde omkring og støtte for beslutningstagning.

Formålet med TIA var at forudsige terrorangreb, før de blev bragt til udførelse. Det var meningen, at systemet skulle skanne private og offentlige databaser samt Internettet for transaktioner, der kunne stå i forbindelse med et terroranslag. Kongressen i USA stoppede finansieringen af TIA i september 2003, men mange af de enkeltprogrammer, der indgik i systemet, eksisterer fortsat under andre navne.

Funktionsskred

Databasesystemer er sårbare over for såkaldte funktionsskred, dvs. brugen af data i andre øjemed, end hvad der har været den oprindelige hensigt. Som eksempel kunne man nævne, at den norske database over asylansøgere – der også rummer biometrisk information så som fingeraftryk – på et tidspunkt blev gjort tilgængelig for norske politiundersøgelser. Det oprindelige formål med databasen var at gøre det muligt at bestemme asylansøgers identitet.

41. Til hvilke af de følgende formål finder du det acceptabelt at registrere kommunikationsdata? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Forebyggelse af terror generelt

2. Opklaring af specifikke terrorangreb, der allerede er sket
3. Forebyggelse af kriminalitet generelt
4. Opklaring af specifikke forbrydelser, der er blevet begået
5. Kommercielle formål
6. Det er aldrig acceptabelt
7. Ved ikke

42. Til hvilke af de følgende formål finder du det acceptabelt at skanne og kombinere personlige data fra forskellige databaser? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Forebyggelse af terror generelt
2. Opklaring af specifikke terrorangreb, der allerede er sket
3. Forebyggelse af kriminalitet generelt
4. Opklaring af specifikke forbrydelser, der er blevet begået
5. Kommercielle formål
6. Det er aldrig acceptabelt
7. Ved ikke

Specifikke udsagn om dataregistrering

43. “Statslige institutioner bør registrere alle de data, de måtte finde nødvendigt af sikkerhedsmæssige årsager, og de bør registrere dem lige så længe, de mener, det er nødvendigt”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig

5. Helt uenig

44. “Data fra telefon-, mobiltelefon- og Internetkommunikation bør ikke registreres, ud over hvad der er behov for til fakturering”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

45. “Skanning og kombination af data fra forskellige databaser, der rummer personinformation udgør en krænkelse af privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

46. “Skanning og kombination af data fra forskellige databaser er et godt værktøj, som politiet bør kunne bruge til at forebygge terror”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

47. “Det er et alvorligt problem, at databaser bliver brugt til andre formål end det oprindelige”

1. Helt enig

2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

Aflytning

Der findes en række forskellige teknikker, man kan bruge til at overvåge borgere og kommunikation mellem borgere – over Internettet, telefonnetværket eller på særlige områder. Ved *telefonaflytning* installeres et aflytningsapparat et sted på forbindelsen mellem to telefoner, hvor der føres en samtale. Man kan enten aflytte den mistænktes egen telefon eller de telefoner, som vedkommende er i kontakt med.

En udvidet form for aflytning går ud på, at man aflytter alle kommunikationslinjer (telefon, mobiltelefon, Internet) på en mere vilkårlig måde i håb om at registrere samtaler, der kan vise sig at være af interesse.

48. Til hvilke af de følgende formål finder du det acceptabelt at benytte aflytning? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Forebyggelse og opklaring af terrorangreb, *med* en dommerkendelse
2. Forebyggelse og opklaring af terrorangreb, *uden* en dommerkendelse
3. Forebyggelse og opklaring af kriminalitet, *med* en dommerkendelse
4. Forebyggelse og opklaring af terrorangreb, *uden* en dommerkendelse
5. Kommercielle formål
6. Det er aldrig acceptabelt
7. Ved ikke

49. Hvilke former for politimæssig aflytning kan accepteres?

1. Aflytning af alle kommunikationslinjer med henblik på at støde på samtale af interesse
2. Aflytning af personer, som den mistænkte forventes at ville kontakte
3. Aflytning af en mistænkt
4. Aflytning i enhver form er fuldstændig uacceptabelt
5. Ved ikke

Specifikke udsagn om aflytning

50. "Aflytning er et godt værktøj at bruge i forbindelse med politiets opklaringsarbejde"

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

51. "Aflytning udgør en alvorlig krænkelse af privatlivets fred"

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

Teknologier til beskyttelse af personlig information

Disse teknologier omfatter blandt andet:

Anonymisering, dvs. services der muliggør anonym elektronisk kommunikation for almindelige brugere. Sådanne services skjuler forbindelsen mellem brugeren og de spor, som han eller hun efterlader, og vil således kunne forhindre uønsket identificering.

Identitetsstyring, som bruges i tilfælde, hvor man ikke ønsker at identificere sig som bruger og i stedet foretrækker at benytte et pseudonym (for eksempel i fora på Internettet). For at gøre det vanskeligere at matche de forskellige data kan det være en god ide at bruge forskellige brugernavne og passwords (der ikke afslører ens identitet) til forskellige formål. Identitetsstyringssystemer gør det lettere for den enkelte bruger at holde rede på de forskellige brugernavne.

Kryptering går ud på at forvrænge indholdet, så det bliver ulæseligt for andre. Eftersom al elektronisk kommunikation er sårbar over for aflytning eller manipulation, vil det i mange tilfælde være afgørende, at kommunikationen foregår på krypteret basis, eller at selve det formidlede indhold i sig selv er krypteret.

52. Hvilke teknologier til beskyttelse af personlig information burde enhver borger juridisk være garanteret adgang til? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Anonyme telekort
2. Krypteringsprogrammer
3. Identitetsstyring
4. Sådanne teknologier bør ikke være lovlige eller til rådighed
5. Ved ikke

Specifikke udsagn om teknologier til beskyttelse af personlig information

53. “ Teknologier, der beskytter personlig information, er nødvendige for at kunne opretholde privatlivets fred i vore dages samfund”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig

5. Helt uenig

54. “Teknologier, der beskytter personlig information, bør ikke være lovlige, hvis de vanskeliggør politiefterforskning og forebygge af terror og kriminalitet”

1. Helt enig
 2. Delvist enig
 3. Hverken enig eller uenig
 4. Delvist uenig
 5. Helt uenig
-

Dilemmaer omkring brugen af sikkerhedsteknologi:

Vi vil nu præsentere dig for en række specifikke dilemmaer omkring brugen af sikkerhedsteknologier i forhold til deres konsekvenser for privatlivets fred. For hvert dilemma vil vi bede dig overveje såvel fordele som ulemper, før du besvarer spørgsmålet. *Du er velkommen til at angive mere end ét svar på alle spørgsmålene i denne del af spørgeskemaet.*

55. At bruge dine fingeraftryk i Metro og S-tog til at registrere, hvornår og hvor du rejser, ville kunne gøre det muligt at trække billetprisen direkte fra din bankkonto helt automatisk. Det ville gøre betalingen meget lettere, men det ville også indebære en registrering af dine rejser og brugen af dine fingeraftryk som autentifikation. Hvordan ville du have det med det? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Jeg ville godt kunne acceptere en registrering af mine rejser og brugen af mine fingeraftryk i Metro og S-tog, da det ville gøre betalingen langt lettere
2. Jeg ville kun kunne acceptere det, hvis mine fingeraftryk blev registreret som en skabelon, der ikke kan rekonstrueres
3. Jeg ville kun kunne acceptere det, hvis registreringen af mine rejser blev slettet igen efter betaling
4. Brugen af fingeraftryk burde være en valgfri mulighed, men ikke den eneste betalingsform
5. Jeg ville aldrig bruge mine fingeraftryk til at identificere mig i Metro og S-tog
6. Ved ikke

56. Omfattende registrering i en lufthavnsdatabase og godtagelse af visse sikkerhedsteknologier, der kunne opfattes som krænkelse af privatlivets fred, ville kunne gøre check-in processen i lufthavnen meget hurtig. Hvilke sikkerhedsteknologier og krænkelse af privatlivets fred ville du kunne acceptere til gengæld for en hurtigere check-in proces i lufthavnen? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Jeg ville acceptere at blive grundigt checket og registreret i en permanent lufthavnssikkerhedsdatabase for derefter at benytte mig af biometri som autentifikation ved alle senere lejligheder
2. Jeg ville acceptere at gå igennem 'nøgenmaskinen'
3. Jeg ville acceptere at blive skannet på sved, kropsvarme og hjerterefrekvens
4. Jeg ville ikke give køb på privatlivets fred til gengæld for en hurtig og gnidningsløs check-in proces i lufthavnen
5. Ved ikke

57. Aktive overvågningskameraer og automatisk ansigtsgenkendelse, hvor de rejsendes ansigtsprofiler sammenholdes med en database over kendte terrorister er sikkerhedsteknologier, som ville kunne bruges til at forebygge terrorangreb, f.eks. i lufthavne og på banegårde. Disse sikkerhedsteknologier ville muligvis kunne forebygge terrorangreb, men deres effekt er ikke dokumenteret. De ville også kunne medføre, at uskyldige personer blev forvekslet med terrorister og taget til afhøring. Hvilken pris ville du være villig til at betale for, at sådanne teknologier kunne tages i anvendelse? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Aktive kameraer og automatisk ansigtsgenkendelse bør anvendes for enhver pris, uanset hvor mange uskyldige mennesker der så bliver forvekslet med terrorister
2. Aktive kameraer og automatisk ansigtsgenkendelse bør anvendes, men kun hvis det er et fåtal, der bliver forvekslet med terrorister
3. Aktive kameraer og automatisk ansigtsgenkendelse bør kun anvendes, hvis ingen bliver forvekslet med terrorister
4. Aktive kameraer og automatisk ansigtsgenkendelse bør anvendes, hvor der er blevet begået mange forbrydelser, eller hvor man er særlig sårbar over for terrorangreb
5. Aktive kameraer og automatisk ansigtsgenkendelse bør ikke anvendes nogen steder
6. Ved ikke

58. Ny teknologi har gjort det muligt at skanne og kombinere data fra forskellige databaser over personlig information med henblik på at afsløre mistænkelige mønstre i personlig kommunikation og brug af Internettet. Formålet er at forudsige og forebygge terrorangreb, men det indebærer skanning af uskyldige menneskers personlige data. Hvilken adgang bør politiet have til at gennemse og kombinere forskellige databaser? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Politiet bør have adgang til at søge i og kombinere alle databaser med henblik på mistænkelige mønstre, der muligvis vil kunne identificere terrorister
2. Politiet bør have adgang til at søge i og kombinere databaser, hvis de pågældende data er anonyme, og hvis identiteten kun kan afsløres med en dommerkendelse
3. Politiet bør aldrig have adgang til at søge i og kombinere databaser med henblik på mistænkelige mønstre
4. Ved ikke

59. eCall-teknologien ville kunne installeres i alle nye motorkøretøjer, som så automatisk ville foretage et nødopkald i tilfælde af en ulykke. eCall-teknologien ville også kunne bruges til at lokalisere motorkøretøjer i andet øjemed, f.eks. hvis de er blevet stjålet, hvis de bruges til kriminalitet eller terror, men denne brug indebærer en løbende registrering af, hvor alle køretøjer med e-Call befinder sig. Hvilke anvendelser af eCall ville du kunne acceptere? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Jeg finder det acceptabelt, at eCall kan aktiveres af politiet med henblik på at lokalisere et køretøj, hvis det er nødvendigt for at forebygge kriminalitet eller terror
2. Jeg finder det acceptabelt, at eCall er aktiveret hele tiden og kan bruges til at uddele fartbøder
3. Jeg finder det acceptabelt, at man løbende registrerer, hvor jeg kører hen
4. eCall bør ikke bruges til andet end at rapportere ulykker
5. Installering af eCall i køretøjer bør være frivilligt
6. Ved ikke

60. Teknologier til beskyttelse af personlig information kan direkte bidrage til opretholdelse af privatlivets fred i forbindelse med kommunikation gennem telefon, post eller e-mail. Men disse teknologier kan også bruges til kriminalitet eller terrorisme. Hvis formålet er at opretholde privatlivets fred for almindelige mennesker, hvilke risici ville du kunne acceptere til gengæld for lovlige adgang til brugen af disse teknologier? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Jeg kan acceptere, at anonyme telekort er lovlige, selvom det vil kunne vanskeliggøre den politimæssige efterforskning og forebyggelse af terror og kriminalitet
2. Jeg kan acceptere, at kryptering er lovligt, selvom det vil kunne vanskeliggøre den politimæssige efterforskning og forebyggelse af terror og kriminalitet
3. Jeg kan acceptere anonymitet på Internettet, selvom det betyder, at folk, der søger efter instruktioner til bombefremstilling, ikke kan spores af politiet
4. Jeg kan acceptere, at Internet anonymitet betyder, at politiet ikke kan spore folk, der søger efter børnepornografi
5. Jeg kan under ingen omstændigheder acceptere teknologier til beskyttelse af personlig information, hvis de vil kunne vanskeliggøre politiets efterforskning og forebyggelse af terror og kriminalitet
6. Ved ikke

61. Hvis en sikkerhedsteknologi tilvejebringer stor sikkerhed, hvilke konsekvenser kan du acceptere for folk, der ikke er i stand til at bruge teknologien og for folk der afviser at gøre brug af denne teknologi for at sikre deres privatliv? (du er velkommen til at angive mere end ét svar på dette spørgsmål)

1. Jeg ville kunne acceptere, at folk bliver udelukket fra at benytte visse offentlige services, hvis de afviser at gøre brug af en sådan teknologi for at sikre deres privatliv
2. Jeg ville kunne acceptere, at folk bliver udelukket fra at benytte visse offentlige services, hvis de ikke er i stand til at gøre brug af en sådan teknologi
3. Jeg ville kunne acceptere, at folk, som afviser at bruge en sådan teknologi for at sikre deres privatliv, i visse henseender får sværere ved at benytte offentlig transport
4. Jeg ville kunne acceptere, at folk, som ikke er i stand til at bruge en sådan teknologi, i visse henseender får sværere ved at benytte offentlig transport
5. Jeg ville ikke kunne acceptere, at det overhovedet har konsekvenser, hvis man afviser at bruge en sådan teknologi for at sikre sit privatliv

6. Jeg ville ikke kunne acceptere, at det overhovedet har konsekvenser, hvis man ikke er i stand til at bruge en sådan teknologi
 7. Ved ikke
-

Demokratiske problemer:

I det følgende afsnit vil du blive præsenteret for nogle udsagn omkring spørgsmålet om demokrati og sikkerhedsteknologi. Hvem skal have indflydelse på spørgsmålet om sikkerhedsteknologi og privatlivets fred, og hvordan skal den indflydelse udformes?

I hvilket omfang kan du tilslutte dig de følgende synspunkter – vær venlig at angive din holdning til hvert synspunkt. Vi vil bede dig nøjes med kun at anføre ét svar på hvert spørgsmål.

62. “Politikerne bør altid lægge vigtige spørgsmål ud til offentlig debat og offentlige høringer, før der træffes beslutning om nye sikkerhedsteknologier”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

63. “Spørgsmålet om sikkerhed og privatlivets fred er så kompliceret, at det ikke giver mening at inddrage den brede offentlighed i diskussionen”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

64. “Menneskerettighedsorganisationer har altid krav på at blive hørt, når der træffes vigtige beslutninger om sikkerhed og privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

65. “Det er vigtigt, at private firmaer, der er involveret i fremstilling af sikkerhedsteknologier, også bliver hørt, når der skal træffes vigtige beslutninger om sikkerhed og privatlivets fred”

1. Helt enig
2. Delvist enig
3. Hverken enig eller uenig
4. Delvist uenig
5. Helt uenig

66. “Når det gælder afgørende beslutninger om anvendelsen af sikkerhedsteknologier, er det meget vigtigt, at man også inddrager en række velbelyste alternative løsninger i debatten”

1. Helt enig
 2. Delvist enig
 3. Hverken enig eller uenig
 4. Delvist uenig
 5. Helt uenig
-

Forslag om brug af sikkerhedsteknologier på en måde, der er med til at beskytte private oplysninger

I det følgende afsnit vil vi bede dig overveje nogle forskellige forslag til, hvordan sikkerhedsteknologi kan implementeres, bruges og udforskes uden at krænke privatlivets fred. For hvert forslag bedes du angive, hvor stor betydning det har, at forslaget føres ud i livet.

Hvis du mener, at det er af stor betydning, at forslaget føres ud i livet, bedes du slå en cirkel om 1 “Af stor betydning”

Hvis de mener, at det er af en vis betydning, men ikke har førsteprioritet, bedes du slå en cirkel om 2 “Af en vis betydning”

Hvis du mener, at det kun er af begrænset betydning, bedes du slå en cirkel om 3 “Af begrænset betydning”

Hvis du mener, at det slet ikke har nogen betydning, eller at forslaget ikke bør føres ud i livet, bedes du slå en cirkel om 4 “Slet ingen betydning”

Hvis du er usikker på, hvad du skal svare, bedes du slå en cirkel om 5 “Ved ikke”

Forslag

67. Indsamling af personlige data fra personer, som ikke er under mistanke, skal foregå anonymiseret, indtil en dommerkendelse har bemyndiget en identificering

1. Af stor betydning

2. Af en vis betydning
3. Af begrænset betydning
4. Slet ingen betydning
5. Ved ikke

68. Kun autoriseret personale må have adgang til de registrerede personlige data

1. Af stor betydning
2. Af en vis betydning
3. Af begrænset betydning
4. Slet ingen betydning
5. Ved ikke

69. Før de implementeres, skal nye sikkerhedsteknologier altid kontrolleres for deres mulige konsekvenser for privatlivets fred

1. Af stor betydning
2. Af en vis betydning
3. Af begrænset betydning
4. Slet ingen betydning
5. Ved ikke

70. Finansieringen af forskning i nye sikkerhedsteknologier bør afhænge af grundig analyse af konsekvenserne for privatlivets fred

1. Af stor betydning
2. Af en vis betydning
3. Af begrænset betydning
4. Slet ingen betydning
5. Ved ikke

Slutspørgsmål:

Du har nu besvaret mange forskellige og meget detaljerede spørgsmål i tilknytning til sikkerhedsteknologi og privatlivets fred. Vi vil nu stille dig to afsluttende spørgsmål.

71. Har du ændret holdning til sikkerhedsteknologi generelt under udfyldelsen af dette spørgeskema?

1. Ja, jeg har fået en mere positiv holdning til sikkerhedsteknologi generelt
2. Ja, jeg er blevet mere bekymret over sikkerhedsteknologi generelt
3. Nej, jeg har ikke ændret holdning
4. Ved ikke

72. Hvis der noget, du gerne vil tilføje i forbindelse med sikkerhedsteknologier, eller noget, du føler, at du ikke har fået mulighed for at give udtryk for i dette spørgeskema, er du meget velkommen til anføre det nedenfor: (*åben tekstboks*)

1. Jeg har ikke noget tilføje
2. Dine bemærkninger:

4.2 Interview guide

Spørgsmål med fed *skal* debatteres af deltagerne. Under hvert spørgsmål er en lille forklaring på, hvad der er formålet med spørgsmålet.

Til de fleste spørgsmål er der nogle underspørgsmål. Underspørgsmålene er til inspiration og kan bruges til at støtte debatten, hvis det er nødvendigt. Underspørgsmålene behøver ikke blive stillet, hvis det ikke er nødvendigt for at inspirere debatten.

Interview spørgsmål

1. **Efter at have hørt oplægget fra vores ekspert og udfyldt spørgeskemaet, hvad er så jeres umiddelbare tanker om sikkerhedsteknologi og privatlivets fred?**

Formål med spørgsmålet: Et åbent spørgsmål der skal starte debatten og give deltagerne en chance for at give udtryk for deres umiddelbare holdninger

2. **Hvad synes I om scenarierne?**

Formål med spørgsmålet: At få deltagerne til at tale om det de har læst i scenarierne for at få et indtryk af hvad de synes om den fremtid der tegnes i dem

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- Hvordan er balancen mellem sikkerhed og privatliv i scenarierne?
- Synes I at fordelene i scenarierne er vigtige at opnå?
- Tegner scenarierne et billede af en attraktiv fremtid?

3. **Hvad synes I er de største positive muligheder ved sikkerhedsteknologier?**

Formål med spørgsmålet: Få deltagerne til at fokusere på de positive muligheder og få et indtryk af hvad de mener er den vigtigste gevinst ved sikkerhedsteknologier

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- Hvilke fordele kan man opnå med sikkerhedsteknologi – prøv give nogle eksempler?
- Hvad er den vigtigste positive mulighed?

4. **Hvilke negative effekter af sikkerhedsteknologier er I bekymrede for?**

Formål med spørgsmålet: Få deltagerne til at fokusere på den negative side af sikkerhedsteknologierne, truslerne, og få et indtryk af hvad de synes er den største trussel

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- Hvilke negative effekter er der ved sikkerhedsteknologier – prøv at give eksempler?
- Hvad er den vigtigste negative effekt?

5. **Hvornår synes I at sikkerhed er vigtigere end privatlivets fred – og omvendt?**

Formål med spørgsmålet: At få deltagerne til at debattere dilemmaet omkring sikkerhed – privatlivets fred (trade off) for at få et indtryk af I hvilke situationer og hvor meget privatliv de vil opgive for sikkerhed

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- På hvilke områder og i hvilke situationer synes I at det er i orden at

sikkerhedsteknologier griber ind i privatlivets fred?

- På hvilke områder og i hvilke situationer synes I at privatlivets fred er vigtigere end sikkerhed?

6. Hvem bør involveres i beslutninger om implementering af ny sikkerhedsteknologi?

Formål med spørgsmålet: At få deltageres input omkring det demokratiske perspektiv og vigtigheden af at involvere forskellige interessegrupper i beslutninger omkring implementering af sikkerhedsteknologier

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- Hvilke interessegrupper skal høres? (borgere generelt, menneskerettighedsorganisationer, udviklere af sikkerhedsteknologi, politikere etc.)

7. Har I nogle forslag til regulering af udvikling og implementering af ny sikkerhedsteknologi?

Formål med spørgsmålet: At få deltageres input til hvordan udvikling og implementering af ny sikkerhedsteknologi kan styres

Underspørgsmål til at inspirere debatten – kun hvis nødvendigt:

- Bør der være nogle begrænsninger på udvikling og implementering af sikkerhedsteknologi eller skal sikkerhedsteknologi firmaer udvikle det de har lyst til?
- Skal regeringer implementere enhver sikkerhedsteknologi de mener er relevant eller bør der være nogle regler – og hvilke regler?

8. Har din deltagelse i dagens borgermøde ændret din holdning til sikkerhedsteknologi og privatlivets fred? Og i så fald: Hvorfor?

Formål med spørgsmålet: At afdække om information og debat om sikkerhedsteknologi og privatlivets fred har ændret deres holdning til emnet

9. Har I en sidste kommentar eller pointe, som I gerne vil tilføje? (tag en runde)

Formål med spørgsmålet: At give deltagerne chancen for at komme med en sidste kommentar før interviewmødet slutter

Underspørgsmål til at inspirere debatten - kun hvis nødvendigt:

- Er der noget der har gjort særligt indtryk under gruppeinterviewet?

GODE RÅD:

Indledning

Start med at præsentere dig selv, ”Jeg hedder... kommer fra Teknologirådet, og jeg skal være ordstyrer her ved gruppesamtalen. Men snak bare løs, så skal jeg nok gå ind og lave en talerække, hvis der bliver behov for det.” Tag derefter en navnerunde. Ved navnerunden kan deltagerne også lige kort sige, hvorfor de er med.

Derefter SÆTTES BÅNDOPTAGEREN TIL! Det gøres uhøjtideligt, lidt nonchalant, og med en let bemærkning. Det er vigtigt at skabe en let stemning og nedtone det alvorlige, så deltagerne ikke føler sig trykkede af situationen.

Første spørgsmål stilles, og gruppesamtalen er i gang.

Det første spørgsmål er et "brainstorm spørgsmål". Her kan komme en masse umiddelbare holdninger, og det er vigtigt at give plads og lytte i starten.

Undervejs

Det er ikke vigtigt, at alle svarer på alle spørgsmål, men man skal have et indtryk af, hvad alle mener.

Hvis nogen "putter sig", kan man altid spørge: "er du enig i det Jens, eller hvad synes du?"

Der vil være overlap i spørgsmål og svar. Spring spørgsmål over, hvis de allerede er dækket.

Kryds af undervejs, når du synes spørgsmålene er blevet behandlet.

Det er vigtigt, at alle spørgsmål bliver behandlet. Der kan dog også dukke spørgsmål op, som er vigtige for borgerne, men som ikke er en del af interviewguiden. Disse spørgsmål skal der også være plads til at diskutere.

Hvis nogen bliver for dominerende, er det interviewerens opgave, at få de andre borgere på banen. Spørg fx "hvad synes I andre?". Afbryd hvis nødvendigt.

Hvis borgerne ikke siger så meget og interviewet er ved at gå i stå, kan man lige "tage en runde", hvor man siger "ved det næste spørgsmål tager vi lige en runde, hvor alle svarer."

Spørg gerne ind til begrundelser: hvordan kan det være, at du synes ... / hvad er baggrunden for, at du synes...

Hvis I skulle blive færdige før tid, kan I vende tilbage til de spørgsmål, der ikke blev gjort så meget ved undervejs.

Afslutning

Når der er 7-8 minutter tilbage, er det en god ide at tage en runde, hvor alle får lov til at komme med sidste kommentarer. Det kan være ting, de ikke har fået sagt, eller pointer og budskaber de gerne vil understrege.

Man kan også spørge om, "der er noget, der har gjort særligt indtryk ved samtalen."

Annex 5 Transcripts of group interviews (in Danish)

5.1 Transcript of interview by BB

Indledning:

- Alt hvad der er blevet sagt under interviewet er blevet skrevet ned. Dog er øh, pauser etc. ikke gengivet i dokumentet.
- Deltagerne er ikke gengivet med deres navn. Interviewer går under bogstavet I: og deltagerne under K: eller M: [hhv. Kvinde/Mand]. Herudover er det blevet forsøgt, at gengive personerne med et tal. Det er *ikke* samme person, der fx hedder M1 hele vejen, men det er udelukkende tænkt som et hjælpemiddel til læseren i forståelsen af, at nu er skifter det fra en mand/kvinde til en anden.
- Da interviewet lydmæssigt ofte var noget skrattende [fremstod uklart], og når folk snakker i munden på hinanden er det noteret i teksten.
- [] markerer noter i transskriberingen

Interviewet:

I: *Vi skal lige se om den virker, men som sagt så har vi en del spørgsmål som vi skal igennem det er, en del spørgsmål, så hvis jeg bliver lidt streng ind imellem og måske har glemt jer, så er det måske fordi [uklart] fordi vi skal nå igennem det hele.*

Det første spørgsmål, det som var et åbent spørgsmål og det lyder, at efter I har hørt oplægget fra vores ekspert og efter at I har udfyldt spørgeskemaet, hvad er så jeres umiddelbare tanker om sikkerhedsteknologi og privatlivs fred. Så der er frit slag. Umiddelbare tanker.

K: altså 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 lige det kan jeg ikke se noget galt i.

I: *fint nok*

M: Jeg synes helt klart, at hvis der skal være det, så skal det helt klart være mærket at det er der. Jeg synes helt klart at det vi har lige i øjeblikket med at der skal være et skilt med kamera

på, det skal der være. Og jeg synes... for kriminalitet synes jeg også det er okay. Jeg synes det er helt urimeligt, nu tror jeg nok det er kommet, men at banker f.eks. ikke måtte ha' lige uden for deres indgange og hvem der går ind i banken og sådan noget. Det synes jeg er helt urimeligt, fordi at det er en af de steder, hvor at man i hvert fald kan gøre noget. Fordi man ved jo at hættten bliver taget af [uklart ord] lige når de træder ind i banken. Der synes jeg det er vigtigt at man har en mulighed for at kunne gøre noget ved det. Eller ha' en chance for at identificere.

K: Jeg er helt enig, om ikke andet så kan det også forebygge bare det at der er kameraer. Og jeg er også enig med dig, altså i det offentlige rum, der foretager vi os stort set ikke noget, som kan betyde noget for privatlivets krænkelser. Jeg synes det er helt fint at der er kameraer. Om ikke så at forebygge kriminalitet, får klart første prioritet.

K2: Jeg tror ikke der er så meget forebyggelse i det. For jeg tror i virkeligheden, at hvis kriminelle ved at der er videoovervågning og hvis vi ved der er videoovervågning, så ved de kriminelle det også, og så vil de i hvert fald prøve, at skjule hvem de er. Så på den led, så tror jeg ikke der er så meget hugget. I hvert fald de klogeste af de kriminelle, de vil da prøve, og skjule hvem de er. Så..

I: *jeg synes*

K2: Så er der jo ikke noget vundet.

K: Så er der jo det der med, det der med genkendelsen, de der biometriske ting. At det kan man jo så bruge på de her kriminelle, der tager hætte over hovedet eller et eller andet, men vil jo stadig kunne genkende højde deres måde at bevæge sig på, og...

K2: Hvad så hvis du bliver forvekslet med sådan en, kunne du tænke dig det.

P. Men, jeg kan ikke lige så situationen, men nej selvfølgelig kunne jeg ikke tænke mig at blive forvekslet med, med - hvad hedder det - en kriminel. Det ville da være ubehageligt. Men skal jo selv kunne bruge dem, altså kun kunne bruge dem når man har fået en dommerkendelse, til at have fået lov til det.

M: Det synes jeg [uklart tale] som vagt formuleret i det der spørgeskema, som vi var udsat for også i Anders Albertslunds fremlæggelse, der er stor stor forskel på, det at data er lagret og så det at søge i data og der er meget stor forskel på om, om man har nogen agenter, der så at sige leder efter nogle adfærdsmønstre i de her data. Altså nogle mønstre eller om man er hurtig til at opklare en forbrydelse bagefter, hvor man leder efter en specifik hændelse eller en specifik forløb.

K: eller en specifik person.

M: Ja

M2: Altså det jeg kom til at tænke på, det var at dele den der overvågning op i en overvågning af lokalitet og så i en overvågning af en person. Og lokaliteten det er det samme som i siger, det har vi ikke noget imod og det har 4/5 af Danmarks befolkning heller ikke påstår Albertslund. Der er blevet lavet en undersøgelse, det står i Politiken.

M2: Altså lokalitet er, hvor jeg befinder mig lige nu, eller...

K: Nej

[snakker i munden]

M: Næh, overvågning over lokaliteten som vagtmiddel [lidt uklart]

M2: Men det er så passiv overvågning, det handler om at man har et videokamera og så filmer man de her data og ligger det på et bånd og hvis der i øvrigt ikke sker noget.

M: Det gør heller ikke noget den er aktiv, der sidder derinde. Det med [snøvler: 4:38]

M2: Jeg synes altså ikke den skal være aktiv, Men aktiv betyder det også, at man f.eks. som hans eksempel, at man overvåger adfærdsmønstre i en adgangsdør, siger at en mand der har en mistænkelig adfærd, uanset om der foregår kriminalitet. Om der foregår kriminel handling eller ej.

M: Det vil jeg ikke ku.

M2: Så for mig er det ganske afgørende om det er et aktivt system eller om det er et passivt system, som man bagefter bruger til at søge efter en specifik forbrydelse. Eller, eller om man bruger den som en agent til at sige nu tror vi snart der sker en forbrydelse, og derfor kan I gå ind.

M: Ja, men så er det jo nok det passive ik, som de i og for sig [uklar], så giver jeg dig ret i at, altså hvad forebygger det.

[Snak i munden på hinanden...]

M: Altså vi forsøger ikke at lave ansigtsgenkendelse på alle de mennesker, der gik ind i banken. Vi prøver bare på at finde ud af, hvem gik ind i banken i det øjeblik, hvor der...

M2: uklart:

M2: Dels så opklarer du, dvs. der er ikke nogen indgriben der.

M: men det er passiv.

M2: Man kan ikke forhindre det på nogen måde.

M: Nej, men det opklarer sager.

M3: Og der kan man jo også se på den terrorhandling, der skete i London ik, hvor hurtigt man egentligt kom videre med efterforskning fordi der var så mange billeder man kunne gå ind og se, hvad skete der? Hvad, Hvordan var der adfærd, hvad gjorde de ik?

Det synes, jeg er en meget vigtig ting på. Det er ligeså meget præventivt, tror jeg, ved at

K: Jo mere reel straftruslen er, det større er muligheden for at de kriminelle tager det med i betragtning, når de overvejer.

M3: Det er jo nemlig det

[Munden på hinanden]

K: Jamen sandsynligheden for at en forbrydelse bliver opklaret, er meget meget lav, så er sandsynligheden for at forbrydelsen bliver begået meget meget høj.

M: Ja

K: Til gengæld hvis 90% af en forbrydelse, en slags forbrydelse bliver opklaret, så vil den type forbrydelse sandsynligvis ikke, altså... ikke nok blive begået i nær så høj grad.

M: Det gælder om at opklare en almindelig forbrydelse der ude:

K: Der er nok, det med det at jo mere man skærper overvågningen, jo mere vil dem der vil gøre noget ulovligt selvfølgelig prøve at skjule det, men det vil måske også blive meget voldsommere end det ellers ville være, hvis det var sat lidt ned i bero.

K2: hvad mener du med voldsommere.

K: Jeg mener de, der urmagerbutikker, som jo er blevet røvet De får jo, det koster jo rigtig mange penge, at de skal holde deres forretninger sikre. Men det.. så bliver de der tyverier, fordi det vil der jo altid, der vil jo altid være tyverier. De bliver voldsommere.

K2: Jamen hvordan voldsommere? Mere avancerede eller?

K: Ja, mere avancerede, mere voldelige og mere truende og de bliver jo også dygtigere, altså man skal ikke tro at kriminelle er dumme.

K2: Nej men.... De kriminelle bliver jo dygtigere uanset hvad vi bruger af sikkerheds teknologi eller ej

K: Men har vi nogen glæde af at det bliver voldsommere?

M2: Jeg er enig med at de kan blive mere avancerede, så de kan forsøge at omgås den her overvågning på den ene eller anden måde. Men jeg forstår ikke, hvordan en overvågning skaber et mere voldelig røveri i og for sig.

K2: Nej det kan jeg heller ikke se. Det er mere sandsynligt, at det vil skabe et mindre voldeligt røveri. For hvis de nu bliver opklarede, så øh...

M: så øh

[uklar samtale i munden på hinanden]

M: Det der sker er, at de sætter større og større tremmer for vinduerne og [lidt uklart] højere vægge, pistoler under disken og alt sådan noget. Det har ikke noget med overvågning at gøre det er i højere grad den voldelige konfrontation [uklart] 8:08

Det her handler om at overvåge og identificere folk når forbrydelsen er sket. Så det er en meget meget passiv strategi. Den handler bare om at sige, hov der skete noget, som var imod samfundets regler så nu forsøger vi på at hitte ud af hvem der gjorde det.

K: Men den overvågning, hvis du begår nogen kriminalitet, så ved dem der er kriminelle - laver kriminaliteten - de slå bare de overvågningskameraer i stykker ik'. Fordi de ved jo også, de er der.

M: Der er jo i sandheden, de hænger lige udenfor, så er det jo lagret [ganske uklart]

K: Det er da også det, der er mere skjulte altså. Men du har da ret selvfølgelig vil de kriminelle da prøve at være lidt grove overfor overvågningskamera.

M: Jeg tror det skaber mere frygt, jo mere overvågning man laver, jo mere frygt vil det skabe af, hvorfor skal det være der? Man får sådan en falsk tryghed af, men går på en gade hvor der er 27 kameraer, men så bliver man falsk tryk af dem når man bevæger dig ud af den gade, så vil man blive nøgen uden kameraerne. Jeg tror at [munden på hinanden]. Det har jeg ikke tænkt over, men vi er jo allerede overvågnede, men jeg har bare ikke tænkt over det , fingeraftryk og ditten og datten og jo mere vi siger god til nu, jo mere vil vi lige pludselig en dag side og tænke tilbage og sige, jamen nu er vi overvågede over det hele. Men det tror jeg at det skaber sådan en falsk tryghed, som jeg ikke rigtigt kan....

M2: Overvågningsstrategien igen er passiv, så føler man sig faktisk ikke overvåget, så synes jeg at det er helt fint, at der er nogle kameraer som lagre nogle data og man begynder kun at søge i de her data, hvis der er sket en kriminel handling.

[i munden på hinanden]

M: Vi har ... mistet en åbning, hvis 11. september aldrig var sket, så var det ikke gået de skridt videre, som der er nu vel? Altså man man for tjekker.. [i munden]

M: Det tror jeg personligt, fordi der har jo været mange episoder herhjemme, hvor man har talt om det foran banker og foran alt muligt ik' og det tror jeg var kommet lige meget om det var sket eller ej, fordi det er små lokale problemer, det du jo ikke måle med f.eks. at en flyver der styrter ned i et hus, der kan du jo ikke sige at fordi der foregår et røveri på en bank eller din bank eller foran en, en pengeautomat eller sådan et eller andet. Der tror jeg, det er to vidt forskellige ting med den overvågning.

M2: men jeg tror bare ikke grænsen er så lang, for hvis kameraet ude foran banken lige pludselig fanger noget andet, at man har muligheden for at se det. Altså hvis kameraerne lige pludselig kan drejes om, hvis der sker noget over på den anden side af hjørnet, så er du også overvåget der. Altså jeg er bare bange for, at det bliver svært at administrere, hvornår går grænsen af, hvor meget man bliver holdt øje med.

M: Det er derfor jeg siger personligt, at jeg synes ikke, at der må sidde nogen bagved. Det skal helt klart være passive overvågning, hvis det er at jeg skal acceptere det her.

K: jeg begynder først, at sætte hælene i når vi når til det her biometriske overvågning, med at man skal bruge fingeraftryk for at komme ind et sted og ansigtsgenkendelse osv.

M: Hvorfor er det problematisk?

K: Fordi at så vil jeg begynde at føle mig overvåget, så vil jeg begynde at føle at jeg gjorde noget forkert. Havde gjort noget forkert eller det vil blive forventet at jeg ville gøre noget forkert. Uanset om jeg har gjort noget forkert eller ej.

M: Det handle jo bare om et [?]identifikation, som dig som person og at der ikke er en anden der udgir' for at være dig.

K: ja, men også risikoen for at, altså at det bliver nemmere og nemmere og give sig ud for at være en anden end den man er.

M: Det forstår jeg ikke det der, argument var også oppe i rummet derinde.

K: Det bliver nemmere...

M: Nej Det bliver ikke nemmere..

K: det er da det der står.

M: Hvordan kan du omgå et biometrisk datasæt? Det kan du hvis det biometriske [peache?]rum er for lille.

M2: Det vil altid være for lille tror jeg. Altid for lille..

K: Der vil altid opstå nye metoder til at omgå de forskellige sikkerheds foranstaltninger. Man vil altid finde en eller anden måde at omgå det på, du kan ikke lave et perfekt system.

M: Okay, som teknikker kan jeg så, er der så selvfølgelig ikke noget negativt bevis for at man ikke kan, men jeg kan jo lave et frækt spørgsmål og så spørge om man kan ændre sin DNA-profil?

K: Det ved jeg ikke.

M: Det vil være så ret specifikt

[I munden på hinanden]

K: Det er jo det de forsker i, hvis de kan ændre på børn -æh fosterstillingen, så kan de forebygge genetiske sygdomme. Jeg er helt sikker på at man kommer til en dag, hvor man vil kunne ændre det. Det er ikke så meget det, det er mere følelsen af at være overvåget, er en krænkelse af privatlivets fred i sig selv. Og jeg ville føle mig alt for overvåget, Øh altså....

M: Jeg forstår ikke, hvor overvågningsperspektivet er altså det...

K: Tag ind i lufthavnen.

M: Det er sådan set et spørgsmål om at det er en re-identifikation af dig som person.

K: Ja, og hvorfor skal nogen vide hvad jeg laver 24 timer i døgnet?

M: Det er ikke det det handler om, det handler om. Det handler om at lave en unik identifikation af dig, sådan at det...

K: Det er jo det det handler om.. Fordi lige så snart jeg er overvåget så kan folk se hvad jeg laver.

M2: Nu skal vi have det for at gå ind i den butik og så skal vi også have det for at gå ind i den butik. Nu skal vi have det for at køre med bussen, nu...

M: Så kan du sige nu har du gået nøjagtigt sådan her - en streg rundt.

K: Ja lige præcis.

M: Og det er igen nogen mennesker, der kan gå ind i det her og sige jamen det har hun gjort.

K: ja, og man ved ikke om nogen...

M: den, den den person, den person

M2: Det er jo en sammenkøring af data og filtrering af data.

K: Og jeg har ingen sikkerhed for at det ikke er kriminelle der får fat i de data. OG det kan omgås.

M2: Men altså sådan som identifikation er i dag, så går du hen til skranken i tjek inn og så viser du dit pas og så smiler du og siger jeg hedder Preben.

K: Jamen det gør du så i lufthavnen . Så skal man begrænse hvor man kan bruge de her ting.

[uklart i munden]

K: Hvis man skal bruge dem hver eneste gang du skal med toget eller med bussen eller ind i en butik eller ind i et shoppingcenter.

M: det er for meget.

K: Så det for meget, at man kan

M3: Det tror vi alle sammen også...

K: Altså dt vil jeg også synes..

[I munden på hinanden]

I: *Er der nogen der har spørgsmål? [uklart 13:31] Til det at blive overvåget med kamera, hvis man nu forestiller sig sådan en situation, hvor man gerne må overvåge offentlige steder.*

K: Det kommer så igen an på om det er aktive eller passive kameraer, hvis det er et passivt kamera, så for det første så ligger der ikke helt så mange oplysninger i det kamera omkring,

hvem du er. Det er ikke lige, så nemt at gå ind og finde, okay nu har vi et fingeraftryk og så kan vi gå ind i politiets database, finde navnet og så kan vi gå ind og finde. Du kan se billeder af personen og så kan du måske bruge det til at gå videre, men ikke i nær så høj grad og ikke lige så nemt, som med f.eks. de biometriske data.

I: *Okay*

M: Jeg forstår ikke hvorfor den samme differentiering ikke gælder for biometriske data, netop om det er en aktiv eller en passiv identifikation.

K: Fordi det er så meget nemmere at bruge de biometriske data, hvis man først er kommet ind og har fået fat i dem.

M: Det forstår jeg ikke.

K: Det er min person. Det er mit indtryk, det er mit personlige indtryk..

M: Okay.

K: altså, af [uklart] hvordan det kan komme til at se ud i fremtiden

M: uklart

K: Og det er jo fremtidsversioner, vi vurderer. Altså at jeg bliver ved med at afbryde dig, men du afbryder også mig. ha ha...

M: okay men jeg mener bare, at det er. Jeg synes det er faktisk forkert, den måde det bliver fremstillet på, at det er nemt at omgå biometriske data. Det er er ganske vanskeligt, hvis man har en for snæver biometrisk feature, ja så er det relativt nemt at omgå, hvis det handler om et enkelt fingeraftryk, ja så vil man kunne finde på en handske. Hvis det handler om et enkelt

feature sær fra irisscan, ja så vil man kunne konstruere en kontaktlinse eller noget anden, men hvis det er et komplekst sæt af feature så er det ganske vanskeligt at omgås.

K: Ja, men hvis det først er gjort så kan man ikke få et nyt sær personligt til sig selv. Fordi så er der nogle andre, der [uklart]

M: Få et nyt personligt sæt. Der er ikke nogen kopi, altså der er ikke nogen der har det samme biometriske feature sæt, som dig.

K: men hvis nu man skaber det samme biometriske feature sæt, som du kalder det, så vil du jo ikke kunne gå ind og sige okay, hvad gør jeg så nu med mig selv. Så er der en eller anden der render rundt og er dig. Ingen vil på noget tidspunkt kunne vide om det er dig eller din kopi, der render rundt og laver de her ting.

M: På mig så lyder det som at folk opfatter featuresættet, som fingeraftrykket i sig selv,

K: Nej det kan ligeså godt være...

M: Der er ikke nogen, der er ikke nogen afbilledning fra feature sættet tilbage til personen. Så det er ikke sådan at hvis du har en...

K: Det er jo det det gør, det identificere dig som værende dig. Hvis en anden identificere sig selv, så er. Kan du se hvad jeg mener?

I: *Jeg tro at vi skal stoppe nu her, fordi.*

M2: Men det er meget væsentligt at man kan identificere personer.

M: Jeg synes bare...

M2: Det kan du gøre på den ene eller den anden måde, vil jeg sige. Alt det der ik'. Men altså hvornår har vi brug for en æh, lad os nu bare se lyst på tingene, når jeg skal have hjemmehjælp en gang. Så vil jeg sgu kunne identificere den hjemmehjælp, og det ikke er en eller anden røver der kommer og tag med. Hvordan kan man gøre det uden de der feature sæt og iris og alt muligt. Hun skal have et eller andet bevis for, at hun er den ik'.

M3: Men altså hvorfor skal man gøre det. Jeg tror mere der hvor jeg er. Altså hvorfor er vi helt derude, hvor man for gud og alt skal finde ud af hvem man er. Jeg tror at man skaber en verden, hvor man får en masse utrygge mennesker af, hvis man ikke har sikkerhed for, at den man udgiver sig for, så er verden af lave og det bryder jeg mig ikke om. [17:05]

K: Ufrihed

M3: Det tror jeg simpelthen starter den her frygt vi gerne vil proppe alle, at terroren står lige om hjørnet og banker på. Altså jeg har ikke følt mig utryg i Danmark og jeg vil ikke føle mig utryg fremover. Jeg vil hellere være fri for det og så tage den chance må jeg sige.

I: Og det leder frem til, synes jeg, det næste spørgsmål om hvad I synes om scenarierne sådan generelt - for den fremtid det tegner. Du har sådan lidt taget hul på det.

M: Det ved jeg ikke... he he

I: Har I andre nogle kommentarer til det?

K: Jeg synes det er lidt ubehageligt og tæt på at vi i virkeligheden kan overvåges på kryds og på tværs og fuldstændig næsten på vores DNA. Og hvad kan det bruges til fremover, altså det er jo meget uigennemskueligt at se nu hvad det i virkeligheden kan bruges til. Samfundet bevæger sig jo hele tiden og bliver mere og mere komplekst, men som den almindelige borger er det meget svært at se, hvad det kan bruges til.

K2: eller jeg tror at man, altså - dem der ved hvad det kan bruges til kan også få fat i de oplysninger. Det jeg er mest bekymret for er hvem der kan få fat i oplysningerne.

K3: Altså som helt almindelig bruger, hvad er det det kan bruges til. Altså fint nok med alt det overvågning - passivt.

K: Det er fint

K3: Nej, [uklart] det der passive, [uklart] alle mulige steder og så kan vi opklare det hvis der har været en forbrydelse. [18:26] Og hvis der ikke har været en forbrydelse så bliver de folk bare spottet. [uklart]

M: De bliver jo tjekket automatisk. Det kører jo.

K3: Fint nok altså med den slags overvågning, det har jeg det helt fint med og efter 11. september er det lidt svært at forestille sig hvad det kan føre til, synes jeg.

M: Det opmærksomme [uklart] vi skal er at identificere os som person. Det kan jo godt være det ikke er spændende, men jeg mener det kommer. Du bliver nødt til at identificere sig, det er mig.

K: Ja i nogen tilfælde, men i hvor mange tilfælde altså.

M: Og det er de tilfælde vi skal begrænse ikke.

K: ja

[I munden på hinanden]

M: Det er jo det med hjemmehjælperen ik'? Og også når du skal ned og hæve nogle penge i banken osv.

K: Ja, så er det også okay. Skal man til at identificere sig for at få lov til at gå ind og handle, ja så er vi altså langt ude vil jeg sige.

M2: Jeg tror altså også der hvor vi kommer hen, hvor hjemmehjælperen identificere sig ik' altså, der tror jeg også vi er meget meget langt ude,

[uklart i munden på hinanden] 19:18

M2: Altså kommer man jo ind til nogen, som måske er lidt senile og alt muligt og der altså om de sætter et fingeraftryk, så må de hellere have et kort som de kører igennem en scanner ik, altså. Jeg synes det der med at de, fordi man er hjemmehjælper, så skal du altså kunne identificere dig, af de helt nøjagtigt veje og sådan noget ik'. Og så synes jeg vi er en tand for langt ude.

M: Det er jo det der igen med, hvor går grænsen, hvis vi siger ja til noget, så siger vi også ja til det næste, næste og næste ik' altså. Hvordan man skal finde ud af,

K: Men vi har jo også forskellige grænser for, hvad vi synes er acceptabelt ikke?.

M: jo, jo. Jo bevares. Det tænkte jeg jo også over når jeg krydsede af. Der havde jeg det jo egentligt også fint med, som du siger, med overvågningen i en kiosk. Man kan vælge eller lade være med at gå i kiosken. Man det er fint med mig, at det er der men.

K: ja

M: Og det er også fint, at man har mulighed for det. Men det der med at man decideret overvåger alt. Det bryder jeg mig ikke om.

K: Nej.

M: Og er ikke sikker på at man skal gøre det. Altså så må man hellere putte nogle flere penge til politiet, vi de har brug for nogle pga. opklaring, eller gøre det på en måde frem for at sku' kunne finde ud af hvor vi hver især er, og de vil vide det - altså det kan jeg ikke se nogen...

M2: Jeg synes at det bliver fremstillet som om, at alle de her teknologier bliver lavet i en stor central database.

K: nej

M2: lad mig lave et forsigtigt eksempel. Lad os nu sige at en eller anden biometrisk identitet bliver registreret på alle der går ind i kiosken og lagre det på det her bånd, analogt måske.

M: Ja

M2: Ikke noget digitalt system, der er ikke nogen netværksadgange, der er ingenting. Det bliver lagret analogt på den her bånd. Nøjagtigt ligesom filmen, hvad er så egentligt forskellen på den profil og det at kunne blive filmet af et kamera. For mig er der ikke nogen stor forskel. De her data er ikke..

K: Det er ikke aktivt kan man sige.

[i munden på hinanden]

M: De der data er ikke tilgængelige på nogen og de bliver kun brugt i det øjeblik, hvor der foreligger dommerkendelser, hvor man ønsker og opklare en forbrydelse. Det andet spørgsmål som jeg synes er ekstremt vigtigt, men som er et andet spørgsmål end det hvor ønsker vi udviklingen, hvor ønsker vi vores samfund skal gå hen, og jeg synes det er vanskeligt og diskutere både den konkrete identifikationsteknologi eller hvad det måtte være, og så hvad er det så egentligt vores samfund mere generelt ønsker. Det er næsten to forskellige skalaer, synes jeg.

K: Mmmm

M2: Der tror jeg grundliggende vi er enige men terroren.

K: Det er jo et overvågningssamfund vi er inde i ik', med alt det teknologi der nu er fremme. Det er et overvågningssamfund, vi er på vej ind i. Eller hvis vi er inde i det allerede.

K2: Jeg synes det samfund, der bliver fremstillet i scenarierne er for voldsomt. Der er for meget overvågning.

M: Jeg også synes, jeg synes det er lidt skræmmende, når det er du siger det kan man ikke, det er komplet umuligt at kopiere det. Jeg tror ikke det er mere end 3-4 år siden, måske mindre år siden, hvor man sagde at det her landkort det er helt sikkert, der er ikke nogen der kopiere dem, der er ikke nogen der kan gå ind og bruge de kort. Der er ikke nogen der kan - det er så sikkert som det kan blive. Og hvad siger de nu - nu ved vi at alt sådan noget kan lade sig gøre.

K: Og alting bliver [uklart]

M: Og det andet der, du siger med at det er komplet umuligt at dert kan lade sig gøre.

M2: Det har jeg ikke hørt mig selv sige, at det er komplet umuligt. Det jeg siger er at den data, der er lagret på det der bånd. Om det kommer fra et videokamera eller en fingeraftryksscanner, der er egentlig ikke nogen forskel og en hver vil kunne gå en og røve båndet hvis røveren synes det er nok interessant og vide hvorfor nogle kunder der har været i denne her butik, så kan de gå ind og stjæle båndet, som er videokameraet - som videokameraet har filmet [22:45].

K: Der er en aktiv, passiv forskel. Hvis det er et passivt videokamera, der filmer på et bestemt sted indeni eller uden for kiosken, kontra det at sku' aktivt gå hen og vide at man altså, at føle at nu tilkendegiver jeg aktivt, at jeg er her. Og så føler man sig tit rimeligt overvåget.

K2: Det er jeg helt enig i og det er kun en følelse, fordi man ved jo godt det er den.

I: [uklart] - *kunne man sige man selv skulle gøre noget.*

K: Jeg og bevidstheden om, at man gør det og det skaber, vækker bevidstheden om at man bliver overvåget. Så går man over en gade og altså et eller andet sted fjerner bevidstheden om at man godt ved der er kameraer. Men hvis jeg ikke tænker over det, så bliver jeg jo ikke bange fordi altså.

M: Jeg har det næsten lige omvendt, jeg vil hellere have at det er aktivt valg, jeg skal tage, nu identificerer jeg mig, hvor jeg er. End at det foregår skjult altså en [uklart] gang i de her scenarier, hvor vi er i...

I: *Hvordan har I andre det med det, det vil jeg egentligt godt vide? Altså forskellen på passivt, at blive overvåget og så aktivt gå hen og vælge..*

M: Jeg har også det der med at jeg vil nødig sige. Altså jeg vil nødig have det der med at der er nogen der, at der er, at der er lige meget hvordan der er, så kan sige så gik han ind i den butik klokken det og det. Så var han tre sekunder om at gå derhen og lave det der og så gjorde han sådan der, hvor han skulle der, og så gik han på toilettet, så trak han og altså..

M2: Det passer slet ikke, hvordan kan man det altså.

K: Det kan man også, nej hvis

M: Hvis du nu får stjålet de her videobånd eller hvordan

M2: Det handler om

M: Nej, nej

[Uklar snak i munden på hinanden]

M: Om tid, hvis det er du mener man skal kunne identificere med et fingeraftryk. Jamen så er det jo kun et spørgsmål om tid, hvornår det så bliver globaliseret, at det er lige meget hvor henne, du går hen, så skal du...

M2: Det er jo et ganske afgørende valg om distribuere alle data ud, så de er [uklar] tilgængelige eller de er lokalt ting, som ligesom vi gjorde.

K: Jamen hvorfor er det nødvendigt og overvåge os på den måde? Hvorfor er det nødvendigt at man er bliver...

M2: Det er spørgsmålet

K: Ja.

M2: Men jeg synes stadigvæk, at jeg godt kunne tænke mig ligesom dig at høre svaret på det der spørgsmål, at det bedre at man bliver anonymt overvåget end at man tager en aktiv stilling og siger okay her vil jeg faktisk gerne..

M: Det kan man ik' for som vi snakkede om så bliver.

M2: Når kameraet er der, så bliver du overvåget uden at man aktivt tager stilling til, at man

[Uklart] 24:53

M: Du er ikke anonym på noget tidspunkt, fordi du ved hvorhenne det sker fordi der er alle de små kameraer og skilte, sådan er det hvis du går ind i en bank eller hvis det er at du går ind i en butik der er videoovervåget, så skal der være et lille skilt, her er der altså videoovervågning.

K: Ja og det er så en anden vigtig ting, at altså for at kunne få udleveret de her overvågningsbånd f.eks., så skal der dommerkendelse. For at få lov til at overvåge skal der være en lille seddel, der siger her bliver der overvåget. Sådan så..

M2: Så er det ikke anonymt.

K: Så altså sådan så det.

[Uklart i munden på hinanden]

K: Det skal der heller ikke være alle steder altså, det er der da ubehageligt at man skal være overvåget evig og al tid [host], altså så længe man ikke har fundet ud af, hvor stor en kriminalitet - det er jo det det handler om ik', det er at nogen tager noget fra nogen ik'. Altså det kan jo ikke være meningen, at en hel masse mennesker skal overvåges fordi, der er nogen der ikke kan holde fingrene for sig selv.

I: Ja så vil jeg springe over til, undskyld at jeg afbryder, spirngne over til. Der kommer to spørgsmål nu og det første går på, hvad synes I er de største positive ved de her sikkerhedsteknologier og bagefter så snakker vi om de negative. Så prøv og start med... Hvad siger du? I har nævnt at man kunne opklare forbrydelser altså after the fact altså efter det er sket. Er der andre?

K: Ja, bevidstheden om at en forbrydelse i højere grad bliver opklaret ved at skabe en større forebyggelse, sandsynligvis. En øget opklaringsprocent vil skabe mindre kriminalitet. I hvert fald i følge mine bøger.

M: Det jeg synes er sværest ved det her scenarie er jo nok, at man blander kriminalitet og terror op i samme gryde. Og det synes jeg er rigtigt svært og svare på, fordi i min verden er det to forskellige ting. Politiet har til dags dato været rimeligt gode til at opklare de ting, hvor de sætter ressourcerne ind. Nu snakker vi om en masse ting, vi vil gerne bekæmpe terror, men terror og en butikstyv, der er godt nok lang vej, i min verden i hvert fald. Så det er svært at komme med, hvad der er positivt og hvad der er negativt.

M2: Det skal ikke være kriminaliteten.

K2: Jeg kan ikke forestille mig, at man vil begå terror i Danmark.

M: Det er begrænset at hvor mange gange terror, der har været ikke, når man tæller efter, men jo. Så er det svært at måle.

M2: Der er ingen sikkerhedsteknologi, der vil gå ind og forhindre [uklart] for en selvbombe vel.

M: Overhovedet ik'

K: Men det skulle da så være den der [uklart]

M2: Gå ind på markedspladsen, så skrev den selv hvordan du vil kunne gøre det. Eller en nøgen øh, hvad var det.

K: Maskine.

I: *Men Kjeld, tror du det vil skabe mere overvågning, når det har med terror at gøre?*

M2: Nej, men det er mere at jeg er skræmt af, hvem der lov, hvem der sidder med magten og kan bestemme hvornår er det vi kun kan kigge efter noget terror, og hvornår vi kun kan kigge efter noget andet, altså. Den del er jeg nok mest skræmt af.

K: Et eller andet sted, så – altså - overvågning. Hvis man ikke vil have mere overvågning i forhold til terroren, i forhold til forbrydelser, så kan man jo sige, at terror er jo en forbrydelse så et eller andet sted, så er der måske ikke så stor forskel igen. Der er mængden af mennesker, der kommer til skade. Det er den eneste forskel der er.

M2: men det er vi meget enige om, men hvornår er man mistænkt og hvornår er man ikke mistænkt. Du kan i bund og grund være mistænkt i morgen og være overvåget, fordi at man har dig mistænkt for at være terrorist. Det er nok snarere det jeg ikke bryder mig om. Jeg har ikke noget problem med, at man har videoovervågning i en bank eller noget. Man kan bruge det til opklaring bagefter.

M: Men det er jo også derfor mener det, der med den aktive ik'. Hvor at det, hvis der er man lige pludselig går ind med en aktiv og siger, jamen hans kropssprog det indikere, at måske er han terrorist.

M2: Det synes jeg da også er et vildt skræmmende scenarie.

M: Ligeså snart der sidder én bag kameraet, så kan han hov, vi må hellere lige følge ham ik'. Hvor jeg mener, at den passive den er der jo, hvis der skulle være sket et eller andet og man har en mulighed for at opklare bagefter. Men ligeså den er aktiv, hvor man kører efter en speciel person eller hans gangbevægelser eller hans noget andet, hans ansigtsudtryk et eller andet ikke, så synes jeg så er vi derhenne, hvor det ikke er noget jeg bryder mig om i hvert fald.

I: Lige en sidste chance for at svare på det positive [uklart - host]

M: Det der med bilerne der er blevet indført. Det synes jeg da helt er noget hvor man bruger teknologien til noget positivt.

K: Jeg mener da også at kunne sige noget om det. Ja, ældre mennesker der fare vild og som gerne vil ud, men ikke kan finde tilbage. Det vil være en god ide og overvåge, så man kan gå ud og hente dem, når de har været ude i lang tid nok.

M: Og det er helt klart en god ting.

K: Det er jo, det er jo en god ting. Selvom, ja det ved du jo selv.

K2:[uklart] dårligt demente eller hvad det er. De ved det jo ikke selv.

[uklart]

K: Det ved jeg. Jeg tror nok, der findes noget teknologi, som bliver udviklet.

K: [uklart]

M: Eksperimentere med det

I: *Så lad os springe over til de negative effekter, hvad er det for nogle I er mest bekymrede for.*

K: Det er at blive forvekslet med en forbryder eller en terrorist. Bare den der følelse af at man bliver overvåget, kan være allerede. Jeg ved, jeg er meget bevidst om alt det, jeg foretager mig ligeså snart jeg ved, at folk kigger på mig uden jeg ligesom har gjort noget for at påkalde mig opmærksomhed.

M: Jeg synes bare der kan være en chance for folk bliver... lige pludselig, hvis man gør det for terror-bekæmpning eller hvis man gør det på nogle andre, i en bank eller et og andet, hvor man lige pludselig kan blive mistænkt for noget, som man overhovedet ikke har noget med at gøre. Der synes jeg det er meget meget negativt, altså det. Der er jeg i hvert fald...

K: Fordi - altså - en mistanke, selvom man er blevet hævet for den mistanke, så er man et eller andet sted i omgivelsernes øjne altid, der vil altid være en tvivl.

M: ja

K: ik', man er aldrig helt sikker på...

M: Man skal være tryk ved dem der har magten til de teknologier. Det kan vi måske være heldige med ik'. [uklart]

I: *Hvad tror du de kan finde på, at gøre med dem?*

M: [uklart] 31:31 Så bliver det jo Stasi ik'

K: Og så også hvad andre missioner kan være med teknologien. Altså kan man ha' hjælp fra et andet land til at se på og sammenholde oplysningerne og finde ud af, altså - hvad render folk rundt i det her land og gør lige nu. Hvis der måtte være oplysninger, de kunne få noget hjælp på den måde. Altså man kunne godt forestille sig, at de kunne få nogle oplysninger de kunne bruge på en eller anden måde, som ikke kunne blive brugt positivt.

M: Du er jo ikke anonym, så længe du - altså hvis du bruger Internettet f.eks. eller hvis du bruger telefoni eller et eller andet, så er du jo ikke anonym på nogen måder.

K: Altså det er jo, så det jeg sætter spørgsmål ved. Det der med anonyme telefonkort f.eks. Så man kunne være anonym i en eller anden forstand.

I: *Hvad synes I er den største bekymring?*

M: Det er klart hvem der står med magten. Hvor går grænsen? Det er det for mig i hvert fald, og jeg tror også det vil kunne blive

M2: Man ved ikke hvem der sidder der...

K: Man ved ikke hvad det vil kunne bruges til. [uklart]

K: Ja, hvad det bliver brugt til - altså - i forvejen er vi meget registrerede. Hvis vi så også skal registreres teknologisk, så er vi langt ude.

I: *Er der flere bud på negative effekter og vigtige bekymringer?*

M: Man kunne tænke sig nogle privatiserede - altså ligesom i Amerika, der har man butikker, der er fuldstændig overvågede med vagter og alt muligt ik'. Det er vås. [uklart]. Så er den gal ikke, så er det bare... [uklart]

K: Det er det jo heller ikke på nuværende tidspunkt.

M: Det er det ikke?

K: Nej. Der hvor jeg [uklart], der er vores garageanlæg overvåget, sådan at når jeg kører ned eller at også andre de kører ned. Jamen så [grin], selvom man både kører ud og ind ik'

K2: altså i et villakvarter, der er den overvågning der er ved noget stop [uklart] privat, eller hvad?

K: Det ved jeg faktisk ikke?

[I munden på hinanden]

K: Ja alle kan, det kom jeg da til at tænke på bagefter

M: Der står også et skilt at der er overvågning?

K: Ja, ja der står da, at der bliver overvåget. Og så umiddelbart så tænker jeg ikke over det, men så i dag så kom jeg da til at tænke nærmere over det, så tænkte jeg de kan da se hvad jeg har gang i både med at køre ud og ind og... eller andre. Men det er faktisk politiet, der har bedt dem om at sætte det op, fordi der har været helt [uklart] 34:02.

I: *Nå, lad os springe til det femte spørgsmål. Det går på, hvornår synes i sikkerhed er vigtigere end privatlivets fred? Og hvornår synes I omvendt? Hvornår er privatlivet det vigtigste og hvornår er sikkerhed det vigtigste?*

[uklart]

M: Jeg synes da helt klart, at privatliv, der må jeg indrømme der altså, der føler jeg det er mig meget højt. Og jeg synes til hver en tid, at hvis det er at der skal være et eller andet med sikkerhed, så er det at der skal dommerkendelse og der skal alt muligt. Jeg ville være meget meget ked af det noget med, hvis magten siger, nu skal vi lige finde ud af om det er rigtigt eller forkert. Det tror vi, at der er et eller andet eller vi har en mistanke om, at der er et eller andet. Hvis det er, man ikke kører, de der systemer, som vi har nu i hvert fald, så vil jeg føle mig meget meget utryk ved det hele. Altså jeg ville altid have at der skulle være dommerkendelser. I stedet for at man bare, at du kan gå hen og, som hver mand næsten ik? Og sige nu tager vi lige og tjekker ham deroppe ik?

I: *Men i hvilken situation kunne sikkerheden veje tungere så?*

K: Altså på en offentlig [- uklar] eller en, jo , på et offentligt sted. Minus de steder, der er nævnt i starten. Hvor der ofte eksempel sker overfald, hvor der ofte bliver begået en eller anden form for kriminalitet, vil jeg mene eller vil jeg gerne have, at der var overvågning, så jeg vidste [host - uklart]. Der vil være, altså hvis. Altså dem der har gjort noget før og er blevet stillet til ansvar for det og hvis nogen gør det mod mig, vil jeg da placere det et eller andet sted, hvor jeg ved der ikke er nogen i nærheden til at kopiere det, så.. Hvis man gør det bliver de i hvert fald opklaret.

M: Der er også igen, hvordan siger man med sikkerhed, fordi der er den igen, at jeg synes, at den sikkerhed, der er rimelig, der. Det er f.eks. at der er en passiv overvågning. Og som, det føler jeg ikke krænker mig, og den føler jeg, at hvis det er det man siger, at sikkerhed vil være størst der, frem for min privatliv og privatlivets fred. Jamen, så synes jeg, at så er det okay, men svært ved at se. Det er jo et meget spørgsmål, hvad betragter man som sikkerhed, hvad er højest der altså. Hvor skal man sige, så er det højere end privatlivet. Fordi der er jo nogen, der synes at bare den passive, det er for meget. Og så er det lige pludselig mere end dit privatliv

ik'?. Hvor at nogen skal op og sige det skal være det og det, om aktiv ik' og nogen skal helt hen, hvor det er den med skatterne ik'? Og det er jo ingen et spørgsmål om at være din grænse, hvor man siger at sikkerhed, den er mere end privatlivet.

K: Et eller andet sted så...

M: Altså jeg vil gerne have sikkerhed i et stor [Uklar - 37:01] magten f.eks. ik'? Der er overvågning helt sikkert ikke noget som helst, der ville jeg være stolt af at have det skidt [uklar sætning]. Det er en af tingene, som vi slet ikke har talt om ik' altså, det er kommende teknologi. Vi har slet ikke rørt ved det, der ved vi altså ikke hvad der kan ske.

K: Det er vi fuldstændige enige i, altså. Jeg tror også det vil virke langt bedre.

M: Det er jo også klart bedre end teknologien, kan man sige så.

M2: jo, jo jeg mener det giver meget med at der står sådan en med en kasket der. Det giver ti gange mere end der står videoovervågning. Men det er jo også det man kører meget med, når man ser de der gader, hvor at der sker en masse ting ik'. Altså hvis det var man havde noget patruljering af to politimænd, der gik og fløjtede ik', jamen det giver ti gange mere end at der er et videokamera.

K: plus at hvis der så sker noget, så kan de gribe ind med det samme i stedet for at opklare det bagefter. Så måske skulle man i virkeligheden, i stedet for at satse på teknologien, ligge - det er mere min holdning...

M2: Jeg synes bare emnet for det her er vigtigt

K: Nej, og ja...

M: Ja synes da, at spørgsmålet er relevant. Og jeg har næsten det modsatte synspunkt, at hvis man, at hvis man vil forsøge på og have betjente på gaden i stort omfang, så synes jeg jo at man optrapper den holdning op på stationen, hvis der er, hvis der er videoovervågning i S-

togene, så minimere man sandsynligheden for at der sker et voldeligt overfald på dig fordi, at sandsynligheden for at det bagefter bliver opklaret stiger.

M2: Det tror jeg ikke på. Jeg tror at hvis du kommer for en generation, hvor du er vokset op med videokamera, så ser du det ikke på samme måde. Så har du problemet ingen om ti år eller om en generation. Så kan det være, at kameraerne er der, hvis...

M: Men de ved, at de bliver opklaret, hvis de gør det.

M2: folk bliver slået ihjel i [by?- uklart 38:46] selvom, der er kameraer og selvom du bliver overvåget bliver folk stadigvæk slået ihjel deroppe. Så jeg tror ikke, det er kameraet - gør - det vi gerne vil have dem til. Jeg tror det måske har en god virkning i starten, men så tror jeg det bliver...

K: hverdag

M2: Bliver hverdag igen.

M: Men man kunne også pege på en masse totalitære regimer, som har rigtigt meget politi på gaden, hvor der også er høj, hvad er det nu det hedder.

M2: Så det er ikke et bevis i sig selv, eller hvad?

M3: Der er jo også forskel på, stadigvæk stater og de forskellige lande rundt omkring og så Danmark ik'? Hvis det er, at vi virkeligt går så langt ik'? Fordi der er forskel på folk i staterne, hvor de er ik'? Altså nu ved jeg ikke om vi taler, sådan helt generelt klodemæssigt eller vi taler vores lille Danmark, hvad vi vil her ik'?. Jeg synes jo, det er hvordan vi reagerer her i Danmark. Og jeg tror at man reagere meget anderledes, hvis der går to politimænd og fløjter med kasket på ned igennem strøget en, hvis der er kameraer ned gennem.

K: Så er der også [uklart], man skal have tillid til dem, der har magten. Altså hvad enten det er dem der har magten over teknologien eller om det er de to politimænd, der går på gaden. Jeg

har prøvet at min kæreste, han blev anholdt uden egentligt at have gjort noget og da jeg fik ham hjem klokken seks om morgenen, der var han fuldstændig forslået. Efter det så har jeg mistet meget af min tillid til politiet. så... det kommer an, altså det gælder om tillid til den, der har den der form for magt.

M2: Det er [uklart]

M: legitimemiddel ik'?

K: hvis, ja poli, hvis polit...

K2: Og så hvis vi snakker...

K: Og så hvis man gennemfører politipatruljering f.eks. så skal man have tillid til, at de ikke går ind i en konfrontation, hvor de kunne have valgt noget mindre. Altså hvor de ligesom istedet for, at anholde folk f.eks. kunne bare give dem en advarsel eller bare lige have stoppet, et eller andet.

I: Så tror jeg, jeg vil springe videre til det næste spørgsmål, som går på hvem der skal involveres i beslutninger om implementering af ny sikkerhedsteknologi. Altså hvad er det, hvem er det der skal inddrages i de beslutninger om hvornår man skal bruge ny sikkerhedsteknologi.

K: Hele befolkningen, det synes danskerne også.

M: Især hvis vi er henne drabs... [uklar], så bliver....

K2: Altså grunden til, at vi alle sammen drejer, så

M2: Det er da kun, hvis det er det offentlige ikke, for et privat firma har vel lov til og sætte folk på prøve ik' med fingeraftryk og alt muligt.

M: Nej.

M2: Der skal være en lovgivning for.

M: Ja, det skal der. Det vil jeg helt klart tro, at der skulle. Det må du også som jura vurdere. Der er jo en eller anden registrering..

I: altså spørgsmålet går på, hvad I selv synes. Det I selv synes, der skal

M: Hvad mener du?

[uklar i munden på hinanden]

K: Vi skal jo ikke vide hvad der foregår. Vi skal da ikke føle at blive overvåget uden at vi ved noget som helst.

[I munden på hinanden]

M: Det må jo ligesom være vores udvalgte repræsentant [uklar].

I: Ja, det er så spørgsmålet til jer. Skal der være folkeafstemning f.eks.

K: Nej det skal der ikke. Altså man kan jo ikke spørge folk om alt vel, der må man...

M: Jeg synes, at hvis man skal til at have tiltro til...

K2: Jeg føler at tingene skete over hovedet på mig, hvis der ikke kom en eller anden form for folkeafstemning.

K: Ja men, hvor tit skulle der så det? Altså hvor meget. Det kommer ikke for at skulle folkeafstemme altså...

K2: Det kommer jo så igen an på, hvilket indgreb til ting som foretages.

M: ja

I: *Hvem kunne du f.eks. være tryk ved vil træffe sådan nogle, var at inddrage sådan nogle beslutninger, hvis ikke man skulle spørge hele befolkningen?*

K: Det kan jeg ikke sådan lige svare på, men jeg synes bare det er meget at lave folkeafstemning, alt efter hvor stort, det vil selvfølgelig også få betydning, hvor et indgreb det er ik', men. Der sker jo hele tiden nogle nye tiltag og hver gang, der kommer nye tiltag kan man jo ikke lave folkeafstemning om det nu skal være?

I: *Er det så hvor politikerne tager stilling til det eller...*

K: Hvem har tillid til det?

K2: Det er jo vores folkevalgte. Det er jo vores... Om der så skal være en ekstra gruppe det...

K3: De kender jo ikke hele. De bestemmer over politik ikke, men kender jo ikke teknologien, så det må jo være de mennesker, der har forstand på teknologien, der er medvirkende, så man får det belyst ordentligt. Fordi politikere de gør det jo kun ud fra deres politiske synsvinkler.

K: Nu har vi jo en, der har forstand på teknologien her i dag.

K2: Og det bliver jeg ikke mere tryk ved.

[griner, og snakker lidt i munden på hinanden]

M: Jeg synes jo, at jeg bliver misforstået konstant bare fordi vi siger biometriske data, så mener I det er et aktivt system, der mener jeg tværtimod det er et passivt system. Men jeg synes det er helt fundamentalt i hvor demokrati at der foregik en debat om, hvad det er. Hvordan vi vil indrette vores samfund, så det her et skridt i den rigtige retning og helt generelt offentligdebat og den slags ting synes jeg er ganske ganske afgørende for demokratiet. Men jeg mener omvendt ikke, at man skal. At man ikke skal tage magten ved det repræsentative demokrati, som - altså detailspørgsmål skal ikke ud til folkeafstemning. Men det er vigtigt, der er offentligdebat også under sådan noget som sikkerhedsteknologi.

K: Grunden til at vi betragter de biometriske teknikker, teknologier, som aktive er fordi det er sådan de bliver præsenteret både i de scenarier, vi fik hjem og sådan som det er blevet præsenteret i dag. Der er ikke på noget tidspunkt blevet nævnt passiv-biometriske teknologier. Bortset fra at du nævner dem.

M: Jeg mener ikke, at der står aktiv i den tekst. Der mener jeg at

K: Nej, der står. Der får man et meget klart indtryk ud af [host] nu og her, når du f.eks. blir' - altså lufthavn vil jeg så sige jo, men altså hvis du igennem den der 'naked machine' i lufthavnen, så er der nogle der kan sidde og se på en skærm, nu og her så har den her person noget på sig som vedkommende ikke må og skal vi så stoppe vedkommende? Frem for

I: Men tilbage til spørgsmålet, er der nogle interessegrupper eller interesseorganisationer, som man skal med på råd?

K: ja

M: Det ville kræve et oplæg eller ligesom det her, måske i større perspektiv. Hiv nogle grupper ind, der har - det må der være nogle kloge hoveder der kan finde ud af - så man får et bredt billede af, hvad Danmark har. Det synes jeg, da helt klart ville være.

K: Som repræsentanter på, altså f.eks. nogle der repræsenterer f.eks. dem der er for og måske producere den her teknologi og så dem der mener at privatlivets fred har en meget stort vægt.

M: Det tror jeg ikke, jeg er enig med dig dem der producerer [host]. Jeg mener de er jo økonomisk involveret, så længe der er noget der har med privatlivets fred at gøre, så skal det være folk der tager en personlig, altså jeg bare ikke producent..

K: Producenter lige præcis kunne til at passe sikkerheden, hvor man på den anden side taler om privatlivets fred.

K2: Der er jo etisk råd eller hvad sådan noget hedder ikke. Eller hvad det måtte være.

K: Altså sådan at man lige som har.

M: Den med producenter, den tror jeg ikke på. Fordi der synes jeg ikke...

[uklart i munden på hinanden - de snakker om økonomi]

K: Økonomiske interesser, der er nogen der taler mere for det ene og nogen mere for det andet. Og sådan en, hvor kan de komme til en grænse som er bedst mulig for flest mulig.

M: Jeg tror at teknologien sælge sig selv. Det er der folk der lever af. Jeg tror mere man skal have befolkningen inde over på en eller anden facon...

K2: Ja fuldstændig enig.

M: Det er jo folkevalgte, der i den sidste ende beslutter hvad det er man vil [uklart]

K: Jeg synes bare, at som befolkning jeg har ikke meget forstand på teknologi, så jeg har da brug for og få det så bredt belyst som overhovedet muligt. Så det er da ikke kun, som almindeligt menneske man kan finde ud af det her. Det kan jeg i hvert fald ikke, men jeg har da brug for at nogen, der har forstand på det kan fortælle om det og belyse det, så man kan tage en diskussion. For ellers så kan man jo ikke, sige noget som helst vel? Hvis du ikke ved noget som helst.

M: Men jeg synes tror jo at teknikerne i det her spil har den opgave at vi skal være med til at tilvejebringe beslutningsgrundlaget. Vi skal ikke være meningsdannere, vi skal fortælle hvilke muligheder teknologien giver. De skal ikke beslutte om teknologien er noget samfundet ønsker eller ej. Det er borgerne, der skal tage den beslutning.

K: Du er jo nødt til at få alle tingene belyst for at kunne tage en beslutning.

M2: Dem der har forstand på teknologien skal være med til at tilvejebringe beslutningsgrundlaget. De skal fortælle hvad kan den her teknologi og hvad kan den ikke.

K: Og hvad den kan bruges til. Altså både negativt og positivt. Den kan jo også bruges negativt ikke, i forhold til borgene. Det skal man jo lige være opmærksom på. Det er ikke kun positivt.

I: Så vil jeg springe videre igen til et spørgsmål, der lyder om I har nogle forslag til regulering, udvikling og implementering af ny sikkerhedsteknologi? Altså kan I komme på nogle ideer til hvordan man skal regulere udviklingen af teknologien? Og beslutningen om at bruge det?... Det er et svært spørgsmål.

K: Er det ikke lidt det samme, som du lige har spurgt om? Altså før spurgte du om, hvem der skulle tage beslutningen og nu hvordan man skal regulere den beslutning, der skal...

I: *Skal der være nogen begrænsninger i udvikling og implementeringen af teknologien?*

K: [uklar] 48:05

M: Det er ikke teknologien. De regler der bliver laves, det er altså lovbestemt, hvad der bruges til, så er det sgu' ligegyldigt, hvad du gør ved hvad for en salg teknologi. De udvikler sig jo hele tiden ik'?

K: ja, det kan man ikke stoppe.

M: Man skal have nogle regler til, hvor man må bruge den teknologi til ik'. Må man bruge det til personidentifikation i det offentlige rum ikke og så må vi se om. Det er det der skal laves noget lovgivning for ikke.

M: Ikke kun for udviklingen, men... [uklar]

M: Det kommer jo an på, hvad den må bruges til ikke.

K: Du kan ikke stoppe udviklingen. Det skal man vel heller ikke, men til gengæld skal det administreres ordentligt.

I: *Jeg prøver lige med det her underspørgsmål, som lyder på. Skal regeringer implementere en hver sikkerhedsteknologi de mener vandt eller bør regler, men det er jo stort set noget vi har snakket lidt om [uklart til sidst]*

K: Det er rigtigt nok.

I: *Så har vi næste spørgsmål og det er om jeres deltagelse i dag har ændret jeres holdning til sikkerhedsteknologier og på hvilke sted og hvis det har hvorfor?*

K: Jeg tror ikke den har ændret min holdning, men jeg tror - altså man kommer automatisk til at tænke lid mere over det. Der er nogen ting, det gør man så jo netop ikke i dag man hører ikke det [?] argument altså. Man kan ligesom se, nårh ja sådan kan man jo også se på det.

K: Jeg vil ikke sige jeg har ændret holdning som sådan, men jeg har tænkt mere over det. Og kommer nok til at tænke mere over det i fremtiden. Netop man bliver mere bevidst om det.

M: Jeg synes mit er blevet lidt mere forstærket i den tro jeg havde, hvor jeg blev lidt mere skræmt af især [navn ?]

M2: Det være den holdning du har.

M: Den skræmmer mig en lille smule og den skråsikkerhed du har med det, hvordan sikkert det er og alt det der. Der har jeg det stadigvæk sådan, at sådan som - da vi stod og snakkede ude på gangen. Da vi stod der ude og talte ikke. Og der sagde du det der med, at det var noget af det bedste der findes og det kunne ikke lade sig gøre alt det. Der var mange ting du puttede ind.

M2: Jeg tror ikke på, at jeg har sagt, det ikke kan lade sig gøre.

M: nej, nej men jeg tror ikke på falsk/positive beviser.

M2: nej, nej. Det jeg sagde var [host] du mistede din identitet med det ik'. Det var det jeg sagde jeg var bange for ik' og lige pludselig så har du fundet en eller anden som kan finde ud af at stjæle din identitet, så når han bruger sit fingeraftryk, så er det egentligt dig, der bliver brugt til det ik'. Og der var det jeg sagde, det [uklart]. Når man så siger man har et sikkert system, det kan ikke lade sig gøre, så er det dig der har gjort det lige pludselig, når den mand finder ud af at gøre det. Det samme det var da dengang med Dankort ik, tænk på hvor mange, der blev mistænkt for, at de havde hævet på deres eget kort, hvor det var blevet stjålet. Hvor de havde fundet ud af at kopiere det som var indeni. Før man fandt ud af det og sagde, gud det er jo også rigtigt det kan lade sig gøre.

M: Jeg synes jeg bliver taget til indtægt for noget, som jeg ikke

[I munden på hinanden]

M: Jeg er langt mere teknologi skeptisk end du tror. Så jeg vil gerne have at du lader være med at fortælle mig, hvad jeg mener.

M2: Jo, jo men det er det jeg er blevet bedt om.

M2: Det er meget stort indtryk eller udtryk for, at du mener det dernede da vi talte sammen.

I: *Jeg vil meget gerne nå vejen rundt og høre om I har ændret holdning i løbet af dagen?*

M: Nej det kommer op på et højere plan [uklart]

I: *Hvad siger du Lars?*

M1: Det er mere at jeg er blevet så bekymret af det hele bundet eller har baggrund for, det er terror, terror, terror. Det bekymrer mig, altså fordi nu kan jeg godt se, hvor man gerne vil hen. Jo skrapere en aftale du har.

I: *Du er blevet mere bekymret.*

M1: Det må jeg ærligt indrømme, det er jeg. Fordi der er mange ting jeg ikke får at vide, som borger og hvis den frygt for terror er så stor. Og det bekymrer mig at man vil prøve og trække nogle ting henover befolkningen pga. det. Det bliver lidt kompliceret.

M: Ja, jeg bliver mere bedrøvet af, at vi troede.

I: *Hvad er du bekymret for siger du?*

M: At man kan skabe sådan en frygt i befolkningen af, at man kan sidde og sige at man gerne vil have mere overvågning overhovedet. Det bekymrer mig da, at du vil have mere overvågning, for det burde ikke være der. For noget jeg ikke rigtigt kan se, om det vitterligt er en trussel eller om det ikke er en trussel. Det bekymrer mig. Det gør det egentligt ikke da jeg læste. Der læste jeg det lidt mere som en film, men... ja.

I: *Hvad siger du Kirsten?*

K: Jamen i virkeligheden så synes jeg efter alt det her, så virker det noget mere uoverskueligt og bekymrende, som du også siger at man kan blive overvåget på alle leder og kanter og hvad gavn har det i virkeligheden ik'. Har det den store gavn, at vi skal overvåges så mange, eller vi kan overvåge så mange.

K2: Jeg er bekymret over, at det er, men ellers så har jeg da også decideret valgt, simpelthen imod overvågning, så det er ikke sådan at jeg på den led har skiftet indstilling.

I: *Mads*

M: Jeg tror ikke jeg har skiftet holdning. Jeg tror, at vi står med et kæmpe kommunikationsproblem, ved at fortælle hvad teknologien kan og hvad teknologien ikke kan. Og jeg synes, den der. Jeg synes ikke, at teknikere fremstiller teknologi som værende en fejlfri teknologi. Sådan som jeg synes det bliver fremstillet, hvad alt. Så det virker som om, at der er nogen der har [kroppen?] og kan oplyse om, hvad de forskellige teknologier kan. Det var også helt tydeligt, at de går ind og slår igennem [uklart], trianguleringen af sendemaster, at folk havde nogle forestillinger om, hvad der kan lade sig gøre.

M1: Jeg synes ikke det kan være teknologien, der har eller hvad kan, det er hvordan den kan misbruges. Det er ikke, hvad den kan.

I: *Vi skal også lige nå og høre hvad navn? [Mette] hvad hun ville svare.*

K: Jamen mere, det sagde jeg i forbindelse med. Jeg er blevet mere bevidst om det og tænker over det. Men min holdning er ikke ændret som sådan.

I: *Så har vi et sidste spørgsmål, der lyder på om I har en sidste kommentar eller pointe, som I gerne vil tilføje? Er der noget vi ikke har fået dækket i diskussionen med de spørgsmål I har fået stillet, som er vigtige at bringe op?*

M: Jeg synes lige den pointe her, det var det jeg lige sagde før. Det er ikke hvad teknologien kan, det er hvordan den kan misbruges.

K: Jeg har siddet tænkt minority report, det med at dømme folk på forhånd, altså pga. af deres opførsel, eller pga. det er så deres tanker ik' eller deres hensigt. Det er ikke aktuelt her, men på hvordan man bevæger sig og hvordan man, hvor man går hen eller altså hvordan man gør ting, eller hvad man gør. Og dømme folk på forhånd uden at vide om de faktisk har gjort noget forkert eller har til hensigt at gøre noget forkert.

I: *Nogle andre der har en sidste kommentar?*

M: Det jeg tænker på, det er at vi næsten ikke har talt om DNA-registret. Vi har alle sammen CPR.nummer. Har vi noget imod et DNA-register også?

K: Så længe det det kun blive brugt i forbindelse med opklaring af forbrydelser altså. Det gør det meget nemt og udelukke folk.

M: Men hvordan kan man være sikre på, at de kun bruger det til det.

K: Altså den måde det bliver brugt på i kriminel.. Kan jeg godt acceptere. Fordi det ikke drejer sig om personen som sådan, medmindre du faktisk har gjort noget. Eller i hvert fald har været på det sted, hvor der er sket noget.

I: *Andre sidste, sidste kommentarer? ... Så tror jeg nok hellere vi må løbe ned til Anders i grupperummet.*

[trækker stolene ud]

I: *Nårh, det kunne vi da godt have snakket en time længere om*

K: *Det kunne vi såmænd sagtens.*

5.2 Transcript of interview by IL

Indledning:

- Interviewer er markeret med I: og *kursiv*. Ny taler er markeret med lineskift og mellemrum.
- Transskriberingskommentarer er markeret med []. ... markerer udeladte passager. Fx markerer ... [8:41] at der ved det 8. minut og 41. sekund var en uklar passage, som ikke blev transskriberet.

Interviewet:

I: *Og så vil jeg bede jer om simpelthen lige at fortælle om jer selv i en kort runde - og ja man kunne måske i forbindelse med at I lige siger jeres navn, så lige lidt om hvad i sådan umiddelbart sige lidt om hvad I sådan lige har af reaktioner på hvad I lige har hørt i oplægget i dag og det spørgeskema i har udfyldt og om der er et eller andet I har lyst til at sige. Men skulle vi ikke starte med dig?*

Jo, det kan vi godt. Ja jeg hedder Anders og jeg er uddannet brandmand. Jeg læser lige nu på overbygningen på datalogi som er noget lidt andet. Og arbejder dels ... i løbet af mit studie har jeg arbejdet ret meget med en masse af de teknologier som er blevet nævnt i dag. Min holdning til dem er ret positiv fordi jeg ved hvad de gør og ved hvor deres begrænsninger ligger...

Jo, jeg hedder Lotte og jeg arbejder i rekrutteringsbranchen. Mht. det er er blevet lagt ud så har jeg ikke sådan de store negative følelser omkring det. Til gengæld synes jeg at meget af det lægger negativt op. Bruger mange negative ord omkring det. Jeg ved ikke om det er en måde at forarge os på, eller hvad? Men jeg synes at der er rigtig mange negative ord om krænkelser og sådan noget som kommer igen og igen hele tiden. Det synes jeg måske er lidt overdrevet.

Ja, jeg hedder Lise [?] og er pensionist. Jeg er tidligere bankuddannet og de sidste år arbejde jeg som sekretær i en kommune. Jeg synes det er meget spændende at være med, men jeg har bare sådan lidt sådan at vi borgere måske alligevel ikke rigtig har nogen indflydelse på det der vil ske fordi teknologien den udvikler sig, og tingene vil ske, altså, forskellige stater, og folk der bestemmer de vil alligevel gøre det hen over hovedet på befolkningen, tror jeg. Men jeg synes det er meget spændende, sådan at høre om de ting, hvad der lige har at sige.

Ja, jeg synes også at det har været meget negativt lagt op, men jeg kan da godt se det er nødvendigt med at gøre en hel masse, men som sagt så tror jeg alligevel ikke at vi har så stor mulighed.

Jeg hedder Konrad og jeg er ...-inspektør - stadigvæk, selvom jeg går på pension om kortere tid. Nå, jeg synes at det har været et ret spændende oplæg og at det handler om sikkerhedssystem i dag der er kendte. Der er register, og min bekymring går på at man samkører registre eller som man har set, sælger data fra registre til privat brug. Det er bekymrende. Men jeg synes at det er godt med nogle sikkerhedsforanstaltninger, men ikke at man går ud i ekstremerne for at tækkes fx USA og andre regeringer. Det synes jeg ikke er godt. Det kan også drives for vidt i forhold til sikkerhedsteknologi. Det var den korte version. [latter]

Jeg hedder Anette og jeg er selvstændig, jeg hjælper så virksomheder med deres økonomi. Og jeg må sige efter at skulle være med i det her, så er jeg begyndt at interessere mig betydelig mere for det der hedder sikkerhed og sikkerhedsproblemer og privatlivets fred. Og alene det spørgeskema har gjort at jeg har vendt holdning, ikke så meget, men lidt mere omkring at det er vigtigt at sikre privatlivets fred. Med de her spørgsmål. Og jeg er meget bekymret for det misbrug der kan finde sted.

Jeg hedder Anis.

I: *Hvad var det du sagde?*

Anis, det har ikke noget at gøre med numerologi eller noget, jeg hedder faktisk Anis. [latter] Jeg har i mange år været i underholdningsbranchen og arbejdet med PR Marketing, men så her for nylig fandt jeg ud af at jeg nu kunne få den uddannelse som jeg ikke lige nåede at få da jeg var ung. Da jeg havde travlt med alt mulig andet. Så jeg går faktisk på universitetet og læser informationsvidenskab. Har også en grundlæggende positiv holdning til ny teknologi. Jeg er overhovedet ikke bange for det og jeg er altid den første til at købe en ny computer og en ny mobiltelefon og sidder og roder med den og hjælper min mand og den slags. Så lidt atypisk for en kvinde i min alder. På den måde. Mht. til det der med grundholdningen så var det egentlig det der berørte mig mest da vi startede her, det var den dame som talte om krænkelse. Jeg synes faktisk personlig at der er en meget stor forskel på den krænkelse der ligger i når nogen overtræder loven, så overtræder de jo loven. Og det er så men en ting. Noget andet er at staten ligesom legitimerer at den krænker mig. Det synes jeg der er meget stor forskel på at nogen overtræder loven og dermed krænker mig, og nogen overholder loven og dermed krænker mig. Og det synes jeg ikke rigtig at den dame udviste forståelse for den forskel. ... føle mig stødt.

Ja, men... Hej, Søren, jeg er folkeskolelærer. Har været ude og arbejde med det i en små fire år. Varierede forhold. Mest små unger. Specialklasser og lidt forskelligt. Og det jeg synes er sværest at skelne for mig selv da jeg skulle besvare spørgsmålene det var at skelne mellem hvad jeg følte og hvad jeg logisk kunne se var smart. Og der er det lidt omvendt af hvad man

lige tænker, fordi jeg føler ikke nogen bekymring for det. Jeg er egentlig ikke bekymret. Jeg har en oplevelse omkring det som egentlig måske burde gøre mig bekymret. Men, hvad skal vi sige, det eneste sted, hvor jeg sådan har tænkt videre logisk og sådan, det er at hvis jeg skal have en bekymring så er det i forhold til den danske grundlov. Som jeg mener er meget på kant med nogle af de nye tiltag.

I: Er det kun mig, der ikke er helt sikker på hvad du mener med grundloven? Hvad det er der er på kant med den?

Der er ... Jeg har den faktisk med. Jeg er folkeskolelærer og ... [latter] Jeg har fundet den på nettet og fik klemt den ned på syv sider [latter]. Der paragraf 71, 72, 73 om boligen er ukrænkelig, ejendomsretten er ukrænkelig og personlig frihed er ukrænkelig. Det står i vores grundlov og når det står i grundloven, så skal man jo holde ved det. Fordi den er jo ikke sådan lige at ændre... Hvis man skal ind til telefon og telegrafmyndighed ... Ja telegrafer er nok ikke så relevante i dag [latter] ... Opgraderet sidst i 53, men der var der igen det her med telefon-... og hvis man skal ind og hente informationer derfra så uanset om det er positionen fra den eller hvad end, så kræver det en dommerkendelse i følge grundloven og det - det oplever man ikke i dag. Så det, hvad skal man sige, det kunne være at de her nye ting bliver ... mindre i grundloven.

I: Ja, nu har jeg nogle spørgsmål. Det kan godt være at der var nogen af jer, der havde lyst til at kommentere på det I har hørt hinanden sige ved runden, så synes jeg lige at vi skal give plads til det

Grundloven, det synes jeg er meget fedt, fordi de ... [8:41] ... hvor de bare kan starte en aflytning og så senere få dommerkendelsen. Og det synes jeg er et problem.

Sådan har jeg det også ja. ... [8:54] ...

Så er det også derfor jeg mener at vi kan sige nok så meget, men jeg tror alligevel ikke at de lytter så meget til hvad vi siger. Lidt fordi at,

Det er helt forkert

Tror du det?

Tror du det?

Det tror jeg er helt forkert. Jeg tror godt at vi kan gøre meget. Men hvis vi netop læner os tilbage og siger, jamen vi kan ikke gøre noget for det er de andre der bestemmer. Man kan fx bombardere politikere med mails.

Det er rigtigt.

Der er mange ting man kan gøre.

Det er rigtigt, det er rigtigt.

Et tegn på at der bliver lyttet meget det er netop at politikerne er uenige om den der terrorpakke der er vedtaget. De vil godt have den bildes ind [?] ... så ok.

Men det er rigtig som du siger, personligt er jeg heller ikke bange, men der er alligevel meget i det nye. Men jeg er heller ikke bange personligt altså, for hvis man sådan er en lovlydig borger, så er man jo egentlig ikke bange vel? Der kan jo egentlig ikke ske... Vel?

Du kan tro der kan ske meget. Det kan da blive misbrugt. Det er det jeg er bange for.

Ja, det er jeg også.

Det er fint. Jeg har haft et par oplevelser med det. [10:01] Været ved at komme lidt i fedtefadet et par gange. Ikke fordi jeg som sådan har gjort ... Men der er jo de her mønstre og genkendelsesstrategier som jo bliver brugt verden over. Jeg var i London for en 4-5 år siden. Og der var jeg meget tæt på at ryge et uheldigt sted hen, fordi der var det her, jeg kender en familie derover, fordi min kæreste på det tidspunkt var au-pair for en engelsk familie og hun

var på besøg ... meget meget velkendte familie og moderen i familien havde en ret høj stilling i ... [Shell?]. Og nu er jeg ikke ligefrem typen der normalt går i skjorte og den gang var jeg sådan en der rendte i poncho og havde langt krøllet hår. Så de her demonstranter for uha og ting og sager, I kan godt forestille jer udenfor en ... [officiel?] bygning, de lignede faktisk mig lidt. Så da jeg sådan pænt gik bagerst i den her lille gruppe af folk der var på vej hen til ... bygning, så var der selvfølgelig en af de her meget store bredskuldrede engelske betjente der meget kontant stoppede mig i at gå ind i den bygning. Der fortsatte jeg lidt, jeg kunne ikke et ord engelsk på det tidspunkt, så jeg var nok meget meget tæt på at faktisk blive behandlet meget meget lidt pænt. Så altså. At genkende mønstre og så videre, det er altså noget der meget hurtigt kan blive misforstået og brugt. Og jeg ved også at i samme tidsperiode, fordi jeg kendte en af butiksdetektiverne i Lyngby Storcenter. Og jeg ved via hende at jeg er en af dem de holdt øje med. Rigtig meget. Og da hun var elev der, i sådan butikcenter, da var jeg sådan en der blev peget ud som sådan en man skulle holde øje med. Og det grinte jeg jo bare af den gang. Det var jo vanvittig morsomt, ikke? Så gik man jo efter at ... Men logisk set så var det egentlig noget der burde have bekymret mig og jeg burde vel egentlig have følt mig lidt krænket.

I: Det var en historie fra virkeligheden. Hvis nu man tager scenarierne, hvad synes I så om dem? Synes I de giver en god fremstilling af balancen mellem denne her beskyttelse, sikkerhed på den ene side, altså, at man bruger teknologien til at sikre vores sikkerhed, også så på den anden side individets privatlivsfred. Synes I scenarierne var gode og inspirerende at læse, kunne man også sige.

Jeg synes det var godt fundet på at ham der den meget sådan lalleglade Peter alligevel stødte ind i et problem. Det var meget godt fremstillet, sådan meget godt. Hvad skal man sige. Godt manuskripttænkt. ... Fordi han drøner bare derud af, han er bare fuldstændig happy og synes det er hele kører og så rammer han alligevel imod det. Og i og med at han bliver tvunget til at tænke over det, så bliver vi også, altså på en god måde, tvunget til at tænke over det. Det synes jeg bare er et godt træk.

Ja, jeg har det ligesom dig. Jeg tænker på Clara, som var imod overvågning og gjorde meget for at undgå det, og så bliver hun overvåget af sin egen søn. ... til sidst. ... Så det er meget godt, det er rigtig godt tænkt.

I: Søren?

Den sidste del, der med Clara, der blev 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 hvor jeg sådan blev ÆV. Hvis mig teenager og min mor vidste hvor jeg var, ÆV. Aj, det havde altså ikke holdt. Der tænkte jeg, det ville jeg virkelig føle mig krænket over. Altså.

I: *Hvordan har I det med det?*

Arh... Jo, de var meget sjove at læse og, men jeg synes igen holdningen var måske sådan lidt at man prøvede at opstille nogen skræmmescenarier. Men det var ikke rigtig skræmmende alligevel. Fordi man havde kendskab til dem. Jeg synes måske de gav dem for meget. Men det var måske fordi jeg kendte dem i forvejen.

I: *Havde du det også på den måde, Lotte?*

Ja, jeg synes de var sådan meget kunstigt opstillede, men det var jo nok også for at komprimere så mange forskellige teknologier på så kort et område. Og det følte jeg var urealistisk et eller andet sted. Og det var sådan meget overdrevet.

... ellers skal man jo skriv sådan en roman...

Ja det er også derfor at jeg synes det er komprimeret på en smart måde.

Nu læste jeg også om det med Clara, hun skulle ud og køre med tog, og så var der sikkerhedstjek, ik, ved toget. Det kunne jeg da godt forestille mig, der var nogen der var lidt ... på. Men det er jeg så modstander af, men jeg kunne godt forestille mig at det ville komme.

I: *Hvorfor er du modstander af det?*

Hvis det er så besværligt at bevæge sig fra det ene sted til det andet ... Så ville vi komme langt ud af sporet, hvis vi skulle begynde at lave så store sikkerhedstjek for at køre 50 km, ville jeg mene, det synes jeg er noget af et problem. ... [taler i munden på hinanden 15:12] ... nogen andre indsatser man skal have fat i for at ...

Det var meget cool, der var jo ikke nogen der stod i kø. I London, i Heathrow der, sidste år da jeg var derovre, hvor de stod med iris-scanningen. Det synes jeg var, der var ingen der stod i kø til den fordi, det var jo så hurtigt, altså. Så stod vi andre bare og ventede og ventede og ventede. Så det kommer vel på et eller andet tidspunkt. Alle de her forskellige ting. Jeg kan klart se en fordel ved dem når man flyver. Måske er det lidt overdreven brug til bustransport. Lidt overkill, men det er klart til bytrafik, det er jo en sikkerhed for os alle sammen også. Så

hvorfor ikke?

I: Og du skelner, du tager ligesom et skridt længere frem og siger når først det bliver rigtig nemt med irisgenkendelse, altså irisscanning, så bliver der noget ved det. Fordi jeg hørte Bue sige at det var besværligt nu, ik?

Mmmh...

I: Eller hvad?

Jo, det er besværligt at... Det tager lang tid og det er en besværlig proces, og man skal stå i kø mange gange og man bliver sådan lidt irriteret over sådan ...

Det ville give større mening, selvom der er de her risici, selvfølgelig for de her fejl, så giver det større mening med irisscanningen end det giver at have tandpasta i en plastikpose. Synes jeg.

I: Giver større risiko for?

Altså det giver større mening end at have tandpasta i en plastikpose. Jeg synes det er fuldstændig grotesk ... at komme ud og flyve, man skal bruge en dag på at komme til England. Grotesk altså.

Med hensyn til risici. Der er jo også risici ved de midler vi har nu, altså dankortet er jo også et misbrugt kort. Altså, hvorfor skulle, altså. Vi bruger det jo stadig glædeligt, altså.

Det er selvfølgelig klart når man taler om decideret identitetstyveri så er det virkelig skræmmende, ik.

Men ...

Det kan jo sagtens ske med dit dankort og alle dine ting i dag også.

Jo jo.

Du går jo ikke og...

Der var blandt andet de der journalister fra BT eller Ekstrabladet, der for et par år siden fandt et... Altså de lavede det jo så på hinanden ik, men ... fandt et sygesikringsbevis og fik de skiftet adresse og stjålet identitet og fik lavet pas med dem. Så blev der strammet op og hvor man senere lavede det samme nummer en gang til.

Ja.

I: *Men synes du at vi alle sammen skal have lavet sådan en scanning af iris og fingeraftryk?*

Nej, de er ikke gode nok endnu.

I: *Nej.*

Det er de ikke.

Det skal vel også være ... [17:47] ... eller hvad?

Ja, det... [17:49] ... Altså, det er ikke nok med irisscanning, det er ikke nok med fingeraftryk, det er ikke engang nok med DNA, jo. Hvad nu hvis man har en enægget tvilling? [Latter] Der er ingenting der er 100 %.

Så det skal vel være en kombination af det vi har i dag plus noget ekstra.

Ja, og nogen gange bliver man bare nødt til at stole på folk.

Nu stod der jo i spørgeskemaet, at hvis de fik den irisscanning. Hvis man fik gjort det en gang for alle, altså der var et eller andet til allersidst, hvis man fik gjort det en gang for alle. Og det var jo smart. Hvis man kunne det, og det så var ca. nok ik.

Jo.

Det synes jeg, så man ikke skal stå så længe og vente mere end nødvendigt.

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. Og alle ved hvad der sker når mennesker får magt. Power corrupts. Absolutely, power is kind of nice, men altså, stadigvæk, det går jo galt, ikke? ... Før eller siden er der jo nogen der misbruger det til reinformationer om hvad vi egentlig gør et eller andet med det.

Det kan ikke undgås uanset hvor stramme regler man har omkring hvem der sidder med det, ik. Som det lige er sket. Og så må man jo bare prøve at gardere sig så vidt man kan så den enkelte lille person har så lidt magt som muligt i de systemer.

Men kan man også sige, at når man svarer på sådan et spørgsmål, spørgeskema, der, så er det i den danske demokratiske kontekst at man svarer. Fordi hvis man nu var kineser, så ville man svare noget helt andet. Eller, jeg ville i hvert fald. Fordi jeg ikke kunne have nogen som helst tillid til systemet og fordi at alt det jeg gjorde blev monitoreret med den hensigt at kaste mig i fængsel hvis jeg mente noget forkert eller gjorde noget i myndighedernes øjne forkert. Det skræmmende er jo at hvis den glidebane du lige nævnte før i forhold til grundloven, den fortsætter, så den kontekst som jeg har forsvaret det her spørgeskema i, så vil det være en anden. Og så ville jeg have svaret noget helt andet [20:00] og så ville jeg have fortryde at jeg havde afleveret alle mine data og at jeg havde sagt ja til samkøring af registre og hvad jeg nu har sagt ja til, i den demokratiske trygge kontekst, ik?

I: Hvad siger I andre til dit udsagn her?

Men jeg er meget enig.

Det er jeg også. Vi er et af de lande hvor vi stoler mest på hinanden, og det tror jeg at vi... Det kan jeg godt tro at undersøgelsen viser. At vi har tillid til systemet. Vi tror på det offentlige, det gør vi jo. Det tror jeg meget mere end mange af de andre europæiske lande. Altså det er jo også lidt et problem. Hvis det er hele Europa der bliver spurgt om det her, så har vi nogen forskellige forudsætninger for at svare.

Er vi ikke også et af de lande i Europa der er mest registrerede? Vi er registrerede på alt, vores CPR-nummer, der er jo ikke rigtig nogen lande der har sådan et system. Altså. Så vi er jo overvågede simpelthen. På den måde, altså.

Vi er jo også så vant til det. Jeg er gift med en udlænding og omgås mange udlændinge. Og de er alle sammen, det er meget sundt som dansker, for de er alle sammen fx sådan noget med feriekonto. Det får alle udlændinge helt op under taget. Er der nogen der skal skrive under på at jeg må få penge jeg selv har tjent? Og vi. Jeg ved godt at det ikke har noget med det her at gøre, men det har det alligevel, fordi det er noget med at vi er fuldstændig vant til, vi er vokset op med feriekonto, vi ved at det er sådan. Vi tænker ikke over det. Når man så hører udlændinge, der siger, er der nogen der skal bestemme det? Det er da mine penge, det mine penge. Så kommer man til at tænke på hvor vant til vi er til denne her foranstaltning.

Altså jeg har nemlig oplevet det samme i den branche jeg er i, det er så trygt her i Danmark at ringe til skat, hvis man har problemer. Det hedder det jo nu, ik. Men nogle udlændinge, når de hører det, det gør I da ikke her i Danmark? I ringer da ikke frivilligt til jeres skattevæsen? [latter]

Nu har jeg ikke gået på arbejde i ti år og der er jo sket utrolig meget i den tid, jeg er gået på arbejde. Fordi jeg har på et tidspunkt været i en socialforvaltning, hvor man jo ikke måtte sammenkøre. Vi havde jo klienter som kom, som vi vidste lavede noget som de ikke måtte og de gik alligevel på bistandshjælp og alt den slags. Det måtte man jo ikke. Fordi vi vidste det jo. Den ene afdeling vidste noget som den anden ikke vidste. Og som de ikke måtte sige at man vidste. Og det må man jo godt i dag. Der må det gerne køres sammen, der er sket meget de sidste 10-15 år. Rigtig meget. Det er der altså. Og det vil der jo nok blive ved med.

Ja, det er jeg meget bekymret for nemlig. Fordi, med sådan som det ser ud i Danmark fx med rygning og med alle vores registre og alt det vi ved om hinanden og med fedme og, hvor man med bedste hensigt, altså det offentlige, det kunne man godt finde på i Danmark, vil jeg sige. Vi kan se at du spiser for meget fedt der hjemme, [latter], sidder og ryger der hjemme, så det

kan da godt være at man så kan blive... Så kommer du bagerst i køen på sygehuset ikke, altså, der er da nogle ting der begynder at. Der er da nogen politikere der begynder at snakke om sådan noget, det synes jeg er meget alarmerende. Det virker så uskyldigt, men det er det altså ikke.

Den er godt på vej, med hvis du er for overvægtig, så må du overveje om din stilling ...[23:03]... Har du så solgt registrene hvor der står dine data i til private firmaer, så er man ude på herrens mark, hvis du skal have nyt job, ik?

Med digital signatur, det så jeg hos min svigerfar, det vidste jeg slet ikke. Nu har jeg ikke selv en digital signatur, men at du faktisk kan gå ind og se hele din lægehistorik, om du har været på hospitalet, og hvornår du er blevet opereret og alt mulig. Det anede jeg ikke at man kunne se på den måde. Det var jo egentlig ret underholdende at se at nå så har du ... og du har fået udstedt det og det, men det bliver jo registreret. Så kan man jo bare lige selv gå ind med sin digitale signatur og så slå det hele op. Det er jo...

Men det er stadigvæk personligt, ikke? Du kan kun gøre det...

Jo, jeg ved faktisk ikke hvem, der har gjort det. Det er jo kun dig selv der kan se det. Men jeg ved så ikke om lægen har den oplysning eller hvordan det hænger sammen. Det ved jeg faktisk ikke.

Praktiserende læger kan ikke få adgang til det. Jeg har skiftet læger et par gange og de spørger hele tiden, nå, hvad har du så på nettet. Det kan de ikke, i hvert fald, det er kun ene sygehuse der kan det og forskere der kan det.

...

I: Hvis vi lige skulle samle lidt op, så vil jeg gerne høre jer, hvad I synes de største positive muligheder ved sikkerhedsteknologi er. Altså eksempelvis nævnte du det der med irisscanningen i London, det er nemt at komme igennem. Kunne I nævne andre, som I synes er de største fordele. Så kommer vi bagefter til ulemperne, ikke?

Jeg kan godt tænke over det med S-togene og kameraer, det er da vigtigt og det er fint. Det optakten. Det forebygger overgreb og vold set på fine maskiner osv... Positiv.

De overlagte overfald forhindre de i hvert fald. [mumleri]

I: *Er der andre der kan nævne nogle oplagte fordele, som I synes?*

Meget af det kan gøre dagligdagen nemmere, det kan da klart have en fordel at jeg ikke behøver tage penge med når jeg skal i toget. Det jo bare at få frakken på og så.

Det der eCall eller hvad det hed. Det der med bilerne. Det var jo også smart på en måde, med ulykker og alt mulig der, det synes jeg også var smart.

Ja.

Ja, men man kunne da også. Hvis der var en eller anden form for margin for de gange hvor man lige kommer til at opdage at gud nej, nu har jeg trykket på ... speederen. Hvis man skulle få en bøde hver eneste gang, så kunne det nok blive måske lidt dyrt, ik... Mest lovlydige, men hvis der var en eller anden form for [25:53] ... model, så kunne man jo sagtens forestille sig at det kunne forøge trafiksikkerheden betydeligt, hvis folk fik et knald, hver eneste gang de kørte for stærkt, altså rigtig for stærkt.

Der kunne man ellers sige, i stedet for at bruge de mange milliarder man bruger på at udvikle et Gallileo, som et system vil bruge, på at bilfabrikanterne skal måske, blive tvunget til at skulle indkode de der ting i deres produkter, så kunne man måske bedre forsvare at bruge pengene på at give folk førstehjælpskurser, så de ville kunne gøre noget, hurtigere. Det er måske et bedre alternativ end at bruge så mange milliarder.

Ja.

Det er et spørgsmål som bringer op netop pengene i de valg, det her det koster. Det er jo et stort, stort spørgsmål i forhold til effekten, ik. Det kan man nok godt sige. At de penge. Fordi de andre, der er terrorister, de andre er jo ligeså kloge som os.

I: Ja, så er vi jo næsten ovre ved nogle af de, om vi kan se nogle negative effekter ved sikkerhedsteknologierne, altså. ... og prioriteringerne og nytter det overhovedet, ik? Er der nogle andre ting I synes der skal nævnes af negative effekter, altså alt det der blev sagt tidligere om grundloven og sådan noget. Det hører selvfølgelig også under her, men det var bare lige hvis vi lige skulle binde et par sløjfer

Jamen det er jo det du har sagt.

Så ... [27:14] ... synes jeg i meget høj grad giver en falsk tryghed, faktisk. Jeg synes det er lidt, altså egentlig lidt bekymrende, det er sådan lidt for at tækkes de gamle damer, undskyld, det var altså ikke sådan ment.

Jamen, det er i orden. [latter]

Sådan set ikke mere trygt at gå i storcentret af det. Det er der ikke nogen som helst dokumentation for at det er. Så jeg det er helt enormt negativt den falske tryghed.

Jeg synes også det er lidt bekymrende at det der hedder eCall, at det står nævnt i vores oplæg at det skal forsikringselskaberne også ...

Ja

At man har været ude i en ulykke, altså, så kan man jo godt forestille sig at der ikke bliver tegnet så mange forsikringer.

Det vil blive meget meget dyrere for nogle.

Så vidt jeg husker blev det også nævnt nogen gange at de så også kunne få adgang til at se hvor tit man kørte for stærkt.

Jo.

[Snakker i munden 28:15]

Den er mulighed er, og det er hvor man skal både, hvor sætter man skodder i mellem de registreringer der er og så de kommercielle, ik?

Altså, man kører jo ræs i sin bil engang i mellem, på en lukket bane, så er det vel ok?

Ja

Mmmh.

Så kan man vel ikke give bøder fordi man kører for stærkt på en privat vej.

Men jeg er enig din betragtning fra før omkring at førstehjælp er vigtigere end anden hjælp. Så man fokuserer for meget på teknologier.

Ja

Mmmh

Ja, det er faktisk rigtig.

Ja, men det gør man. Der er ikke noget. Så stort er Danmark heller ikke og så mange øde steder er der altså ikke i Danmark til at der ikke er nogen... og alle har jo nærmest en mobiltelefon og ringe efter hjælp. Nærmest lige så hurtigt som ...

Relevant i Australien.

Ja, Australien, det ville måske være smart, ik. Men, i Danmark...

Der er ikke så mange af os der har nævnt at vi tror det kan forhindre forbrydelser. Teknologien.

Nej, det tror jeg heller ikke at det kan. Det er et spørgsmål om vilje og penge. Altså, alle de der sikkerhedsteknologier er jo med for at gøre det mere besværligt. De udelukker ikke noget. Det gør det bare mere besværligt, og derfor vil man måske godt kunne se en tendens til, men de udelukker ikke noget, altså. Hvis folk vil, gøre noget, så gør de det. Allerede nu, nu er der allerede masser af sikkerhedstjek i lufthaven og derfor er der jo stadigvæk folk der kapre fly...

Får nye ideer, og ja.

Men den industri vi snakker om her, hvor man ... den udvikler sig jo på forkant mange gange i ... På visse områder, ik? [30 min] Økonomiske områder specielt, ik. USA har jo mange problemer i forhold til deres banker og kunder osv. pengeoverførsler osv., ik. Der er jo ikke nogen sikkerhed i den teknologi i dag, der kan gå ind og dæmme op for det.

Arh. Nu ved jeg ikke lige konkret...

Vi kan da bare tage her, dankort blev der nævnt tidligere, ik. De er opbevaret i en database ovre i USA som der blev stjålet oplysninger fra, det vil sige der var et x antal dankort der skulle ændres med ny ...-numre på osv. Det er økonomisk skal man se det. Så det er ligeså gennemsigtigt som ...

Ja, jo, altså relativt jo. Selvfølgelig, der er huller når det er bygget op som det er.

Men sto... hullerne?

Ja, hvis der er et hul ...

Ja, men som du siger, det er mennesker, det sagde du før.

Der er faktisk, altså, undskyld at jeg kommer til at nævne grundloven med vilje

Nej, men [latter]

Nej, det her er en krænkelser, hvor vi alle sammen tænker, åh, og der er de her fine linier, og vi kan blive enige om de her faste regler og vi kan ikke, og er der også nogen regler osv og osv. og frem og tilbage. Og alligevel er der altid noget der går uden om de her regler. Der er altid undtagelser fra de her regler, der er altid nogle der har denne her ekstra opmærksomhed. Jeg har en god ven, hvis morfar har haft en meget høj stilling indenfor dansk militær. Så hans telefon og alle samtaler han har haft er aflyttede. Og er det stadigvæk. Og der er ikke noget med nogen dommerkendelse og sådan noget der, det er noget med at han er en vigtig person for landets sikkerhed, derfor bliver alle samtaler der er lige omkring ham aflyttet. Og der en hel del af mine samtaler jeg ved der ligger båndede et eller andet sted, når jeg har haft ringet hjem til min kammerat osv. Fordi de telefoner omkring ham de blev aflyttet. Samt. Ja, vi kan godt blive enige om nogle regler her. Og så er der militæret og så er der nogen helt andre omkring det. Og så er der nogen helt andre spilleregler. Og det skal man være opmærksom på, ik? Altså fordi der er reglerne der gælder generelt og så er der alle de her undtagelser, vi aldrig hører om. Men det finder du jo også i andre erhverv.

Ja.

i virksomheder, de bånder jo også deres samtaler, altså. Det er der jo nogen der gør.

I: Men nu kan jeg nok få lyst til at skyde et spørgsmål ind, for vi er ved at nærme os spørgsmål nummer fem. Nej, men det fordi. Det er jo det her, hvornår er sikkerhed vigtigere end privatlivets fred. Altså du har givet et eksempel med militærmanden, sikkerheden er vigtig der, ik. Kan I forestille jer nogen situationer hvor det ikke er vigtigt, eller synes I. Altså hvornår, ja, hvornår synes I sikkerhed er vigtigere end privatlivets fred og omvendt?

[lille pause, så i-munden-snak]

Der hvor, hvis jeg må tage et eksempel fra den tekst vi har læst, den med Carla der bliver overvåget af hendes søn, hvor jeg mener at den slags overvågning - . Jo, jeg kan godt se en pointe med den, at hvis det er en gammel svagelig ældre dame og holde styr på det her med den, jeg vil kunne se noget hjemmepleje der blev meget mere effektiviseret af det her. Det kan vi se, men jeg kan også se det brugt på en hel masse andre med nogen meget overbeskyttende forældre og deres stakkels små teenagebørn og lignende ting. Som i den sammenhæng hvor der går ind og bliver noget privat overvågning og sådan noget, som jeg synes er meget, meget uheldigt.

Ja, mmh.

Som det kan bliver brugt til.

Jeg vil sige det kommer an på hvordan man definere personligt sit privatliv, fordi hvis du sidder på en arbejdsplads, så er du jo ikke en privatperson. Så er du jo en del af virksomheden og så er det i princippet skal man jo ikke sidde og snakke privat i telefonen eller hvad man nu laver.

Eller på mail.

Eller mails. Så derfor, så har jeg det sådan lidt, så har jeg ikke noget problem med at blive overvåget når jeg er på mit arbejde, fordi det er en del af mit arbejde. Altså jeg er i en virksomhed og jeg er ansat der til at gøre et stykke arbejde. Når jeg er hjemme privat, indenfor hjemmet fire vægge, så er det måske en anden sag, hvor jeg måske ikke ville føle at det var så fedt at blive overvåget på samme måde. Men det er jo hvordan man definerer hvor er min privatsfære.

Men det er vel også hvordan virksomheden orienterer medarbejderne. Så hvis virksomheden ligesom fra scratch siger, jamen vi monitorerer alle telefonsamtaler og alle mails og vi skanner

Mmmh

alle computere for porno og whatever, de der ting der, som vi nu gør. Jamen så ved man det

Ja

og så er man selv ude om det. Og derfor har der faktisk været flere sager ved domstolene, hvor det er det, der er det afgørende kort. Om fx en virksomhed fik ... Der var en sag om en medarbejder der blev fyret, fordi hun sendte ting, hvor der kan ...[35:09] som privat, og hun fik erstatning, fordi virksomheden ikke havde sagt det.

Mmmh

Jeg tror at de faktisk brødte persondataloven og ...

Ja.

Men der er som regel, de fleste virksomheder har en eller anden form for

Nej det har de desværre ikke

Ok, der hvor jeg arbejder, der ... [taler i munden på hinanden] ... omkring de ting og hvordan man skal begå sig i virksomheden, med hvordan det foregår og at de har lov til at kigge i mine mails

Ja

Og det har jeg det fint med, altså, jeg har ikke, altså, det, jeg er jo ansat der, altså. Det er jo deres ressourcer jeg bruger. Ja, det er jo det. Så.

For mig går grænsen ved det der med dommerkendelsen. Altså, det er der, hvor det bliver grænseoverskridende for mig. Altså, hvordan ... 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 ind i mellem sidder nogen 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 sådan lidt mere rolig. Det, der med, alt det der de nu må uden dommerkendelse, det er min allerstørste bekymring. Og det synes jeg er krænkende. Altså at de må det.

Ja, det synes jeg også.

Det kan godt være at det lyder gammeldags, det der med dommerkendelse, men det gør også mig tryk. For som du siger, selvfølgelig, alt kan jo omgås, det ved vi jo godt, men alligevel. Der har været en og kigge på, en udenforstående.

Jo, altså vi har jo magtens tredeling her i Danmark og det er en af grundene til at vi har et ret velfungerende samfund, synes jeg. Jeg synes også at jeg lyder som en gammel skolelærer [latter] men virkeligt...

Jeg synes også det er væsentlig at få defineret hvad der skal overvåges og hvad der ikke skal overvåges. Jeg tænker på private centre, osv., boligkomplekser, hvor går grænsen til overvågning? Uden på ... [37:15] ... og inden i ... Selvfølgelig skal der også være nogen billeder i gang ik? Jeg har set det i Irland, hvor alt bliver overvåget. Der er store master med syv kamera på. Det tager her firmaet og boligkomplekser. Det er de vant til derovre, men det er vi ikke vant til her. Altså. Det er fint med overvågning hvor man ved der skal være noget, sene aftentimer og nattetimer.

Man skal heller ikke overdrive.

I: *Nogen der har noget at tilføje?*

Næ, ikke andet end det der, med vi snakkede tidligere om samkøring af registre. Altså, persondataloven. Altså hvis ens data ligger et sted, så kan man sige, den må ikke ligge der. Så skal I stemme, ellers så ... [38:12] Også selvom man selv har givet dem lov til at opbevare

data, så må man godt sige at de skal fjerne det igen. Det er måske en meget rar ting at vide, som der ikke bliver gjort så meget opmærksom på.

Af gode grunde måske.

I: Er det noget der, altså nu, ja, altså betyder det noget for dig at du? Ville det betyde noget for dig?

Det betyder at jeg har muligheden for det. Det er rart for mig at vide at hvis der står et eller andet på en eller anden hjemmeside, så kan jeg bede dem om at fjerne det. Det giver mig en personlig sikkerhed. I at jeg kan vælge og vrage i hvad for nogle informationer der er på ...

I: Og hvordan var det med dig? Altså du lagde ligesom op til at der må være en grænse eller. Man skal ikke overdrive det der med tv-overvågning fx. Men hvor går grænsen for dig?

Nå men det er at man kan gå udenfor en forretning, der udenfor deres eget fortovej og begynder at lave overvågning osv. ... Der går grænsen for mig. De må godt have overvågning på inde i forretningen, men hvis du sætter 100 hvor der måske var rigeligt med at der var en 10-12 stykker, så er du ligesom begyndt at gå i dybden, ik, det er både ansatte og kunder vi snakker om her. ...[39:31] materialet, hvor lang tid skal det gemmes osv., nogle regler omkring det. Hvornår skal det slettes, hvem har adgang til de data og hvornår ik. Jeg har også prøvet få aktindsigt i hvad der er registreret. Det er meget interessant egentlig.

Ja.

I: Sådan noget som det Bue nævner, og det Konrad nævner, er det noget nogen af jer andre har gjort jer nogen tanker omkring det? Altså hvor mange overvågningskameraer eller flere overvågningskameraer eller? Dataregistrering?

Jeg synes godt vi kunne have flere overvågningskameraer. Især, nu nævnte du lige det med butikkerne [40:09]. Der har jo været meget oppe i medierne med tyvens omklædningsrum. Står ude foran butikken og klæder om og så kan han gå ind i butikken og tage hvad han vil have. Tage en maske på lige udenfor, det kan han gøre lige i svingdøren nærmest, fordi de ikke må filme der, altså lige ude på gaden. Det synes jeg faktisk godt de kunne få lov til.

Bestemmer en forretning selv om de vil have overvågning? Det ved jeg slet ikke.

Ja, det tror jeg de gør.

Ja, det er virksomheden selv der afgør.

Men de må ikke filme udenfor på fortovet,

Nej.

og det er der jeg synes godt de kunne, det måtte de godt. Dengang jeg læste, da arbejde jeg i en butik inde på strøget, og så skete der et overfald lige ude foran butikken og politiet kom ind for at skulle se overvågningskameraerne for at se om der var noget, som måske filmede lige fra hovederne af sådan så det kunne have fanget et eller andet, men der var ingenting. Fordi de jo ikke må filme den vej. Så de kunne ikke rigtig opklare det. Og det kunne være en stor hjælp for dem, lige at have haft den meter mere eller noget. Så, det synes jeg sagtens at man kan.

Det er igen, man er nødt til at lægge en grænse jo, fordi at så kan man sige, skal det så være en meter fra hoveddøren at de godt må filme. Eller skal det være i hele krydset som de godt må filme. ...

Jeg er ikke ekspert på det område, men jeg synes bare at man giver spillerum til en masse mennesker, som udnytter det.

Du har da lov at provokere. Så kan du ligeså godt sætte nogle kameraer op i Voldsmose og alle de andre store steder, hvor man mener at de potentielt kriminelle de kommer fra, osv. har erfaring med. Altså indenfor forretningen ja, men udenfor i det offentlige område, nej. Der vil altid ske nogen hændelser, ik, ... [41: 53] er det jakkesæt eller gælder det noget andet, ik. Så. Den, den er ikke gangbar. Det er min opfattelse, ik.

Jeg vil sige, i det omfang, at kameraernes data bliver slettet efter et døgn, to døgn eller sådan noget, der er også et spørgsmål om lagerplads, ... informationer, hvis det bliver slettet efter et-

to døgn og så er ude af verden, ved du hvad, så synes jeg inde i indkøbscentre og så videre, så vil det være udmærket med kameraovervågning der. Jeg arbejder fx på en skole, der ligger lige ved siden af et indkøbscenter og der ved jeg der er en masse ballade oppe. Og der tror jeg at der kunne politiet have meget stor glæde af at lave noget også forebyggende kriminelpræventivt arbejde. Hvis de kunne nemmere ... når andre lavede ballade deroppe. Og jeg tror inde i et storcenter af forskellig art, butiksarkader og forskellig slags og sådan noget. Der kunne jeg ikke se noget galt i det. Det er jo et offentlig rum, ja, men det er stadig ofte et rum der bliver alligevel lukket af om aftenen osv. ik. En ting er at gøre det i parker, eller hvad ved jeg ik, men inde i et butikcenter, så synes jeg altså ...

Nu hæfter du dig også lidt ved den præventive effekt, som de jo også har erfaring fra i England, at den er der ikke.

Nå, men jeg, du misforstår mig, fordi, nej, jeg tror ikke at de lader være med at lave kriminalitet, men opklaringsmæssigt, og den, når det er, som i mit tilfælde med mit arbejde, unge mennesker, der gør det, så kunne det måske forhindre dem i at få en lang fængselsdom, hvis de få en række skideballe af en betjent inden de fylder 15.

Ja,

Så,

Ja,

I: Hvad siger I andre til den diskussion om overvågningskameraer? Det er jo sådan en meget aktuel problemstilling, kan man sige.

Jamen, som jeg nævnte tidligere, så hvis der er regler omkring det bliver ... [44:03] ... så ... også private firmaer. Dem vil jeg godt sælge. Fordi det er der ikke i dag. Ikke sådan nogen der bliver henvendt i hvert fald. Men det præventive, det er ret væsentlig for mig, altså. Det er lige meget hvor det skal lægges det præventive arbejde. For det, man kan ikke hylde sig ind i overvågning og så tro at så kommer der noget udvikling i gang. Det gør der desværre ikke.

I: Altså du mener det skal hæftes sammen med noget præventivt arbejde?

Præcis. Det er da ret væsentligt, ja.

Ja.

Ja, altså man kan sagtens forstille sig at det meste af det der CCTV, de er jo privat regi, og hvis de så måtte overvåge fortovet og gaden og alt muligt, så kan man bare forestille sig alle mulige ting de har ... Altså der er jo altid underlige mennesker de kunne finde på at sætte, kameraet fanger at ham der urmageren overfor, han har en affære og så kan han blive, altså alle mulige ting. Som ikke kommer folk ved, som de kan ... overvåge deres eget. Altså. Og ikke ... et helt butikcenter, så er ... et form for regelsæt, hvor man ...

Så må man gå ud fra et eller andet fælles.

[taler i munden på hinanden] leve op til.

Altså nu sidder jeg bare og ringer lidt, en det kan man misbruge i privat regi. For så kan man sige, ham der, han går først ind og kigger på ure, så går han ind og kigger på dameundertøj. Ok, nu går han hen til en lysreklame. Så viser de en reklame for et eller andet ur. Sådan noget der.

Jo, men det gør jo allerede...

Det tror jeg også de gør

Jo, jo,

Google gør det. ... Når du sidder og skriver en mail ud, når du så skriver et eller andet så kommer det jo op derovre og så handler det om det, ik.

Sådan nogle informationer bliver helt misbrugt, faktisk.

Tror du ikke at sådan foregår det i nye centre og alle de større centre? Tror du ikke det? Der bliver du da overvåget over det hele, gør du ikke?

Jo, men det er ikke målrettet decideret på dig,

Naaaaj,

Det gør de på nettet, det ...

Men så kan de alligevel at nu er du lige der hele tiden

Men altså vi hørte jo inden at der er et eksempel på at Jomfru Ane Gade skal videoovervåges og det synes jeg er uhyggeligt, at man begynder at overvåge et helt gademiljø. Det er det offentlige rum. En gade er et offentlige rum. De kan så gøre det inde på det enkelte værtshus eller sådan nogle ting, det synes jeg nu altså er ...

Der vil jeg nu også mene de i stedet for skulle diskutere deres politik lidt omkring forskellige udskænkninger

Ja.

og i stedet for det der med overvågning. Det er måske nok der den lidt den ligger begravet.

Du nævnte lige Google. Jeg har lige købt et firma der er eksperter i ... [47:06] ... og de bedste på markedet. Og det ligger inde i de der søgemaskiner de har og andre ting. Der skulle også være nogle regler der. I mine øjne. For der er stor trafik på nettet.

I: Hvem synes I skal involveres i en beslutning om at tage noget ny sikkerhedsteknologi i brug?

Det kunne jo også godt være situationen på Jomfru Ane Gade, hvem skal være med til at tage beslutningen om at der skal sættes overvågningskameraer op? I det hele taget, altså generelt, at beslutte at tage nogle sikkerhedsteknologier i brug, hvem skal involveres i det, synes I?

Det skal statsmagten, og så det lokale styre der er udfra den lovgivning der er.

Jeg mener også sagtens der kunne være nogen udefra rådgivende kræfter. Jeg kunne sagtens se god brug af en sociolog og en antropolog i den sammenhæng. Til at varetage nogle ting. Jeg ved at de i forvejen rådgiver politiet om en masse ting og benytter sig en masse af dem, så der kunne jeg godt forestille mig at nogen med en lignende uddannelse kunne være meget nyttige. Også med en juridisk baggrund måske.

Ja, det skal høres af ... [48:18] organisationer af en eller anden art, og ikke dem der skal sælge udstyret.

Nej [latter]

I: Hvad med sådan nogen som jer selv, eller altså dem der bliver berørt af det? Altså almindelige borgere, tænker jeg på.

De skal da klart med ind i en høring, ... [48:38] hvis det var oppe i Jomfru Ane Gade, så vil der komme en god diskussion om mon ikke problemet med et værtshus man kunne fokusere på.

Hvis der er beboere i Jomfru Ane Gade, de er da også inficerede.

Det må da være kedeligt at bo der.

Ja, det konkrete eksempel vil jeg også sige en høring, men andre eksempler må man jo altså. Det synes jeg måske nok at man må fæste sin lid til de der mennesker, man nu en gang har stemt ind i forskellige...

De kan jo heller ikke smide alt ud til os. Noget... Så bliver det simpelthen for trægt det demokratiske system.

Ja,

Mmmh,

Bare de holder sig inde for grundloven, så er jeg tilfreds.

Ja. [latter]

Men for lige at tage den med Jomfru Ane Gade, hvis jeg boede der, ville jeg være lykkelig, hvis jeg fik kameraer rundt på gaden.

Der må da også være mennesker der er uddannede i sådan noget som det her. Altså som virkelig har forstand på det, ikke også? Altså der er jo uddannelser sådan i sikkerhed. Det må da også være nogen der må være relevante at tage med. Om det er gavnligt der eller ikke gavnligt der, ik.

Jo, men jeg har ofte en interesse i det. I den sammenhæng er det vigtigt også at have sådan en fyr som ham der filosofen

Ja.

med til at perspektivere

Ja

de her ting. For hvis du arbejder med sikkerhedsteknologi og i det hele taget, hvis man arbejder meget koncentreret med en teknologi, så bliver man sådan lidt, altså måske lidt for teknologiglad [50min]

Du tænker han

Ja

han gerne vil gøre det uden, altså, uden at blive interesseret i at lave det?

[taler i munden på hinanden]

... fx når man er optaget af noget og man selv er et ordentligt menneske, om man så må sige, altså, så kan man nemt glemme, de etiske komplikationer der kan være. Og så kan det være godt med sådan en filosoftype eller en sociolog, som du sagde.

Hvad skete der nogensinde med Etisk Råd? Sådan et havde vi engang?

Det findes stadigvæk.

De findes stadigvæk? Det er bare lang tid siden vi har hørt fra dem.

Nej, de har lige været her med abort.

De ville nok være meget relevante at have med i sådan en sammenhæng.

Ja

Ja, det er fuldstændig rigtigt

Ja, det er rigtigt.

Men nu blev vi også spurgt om menneskerettighederne ... om vi synes. Og de er også gode, men de har jo en helt anden vinkel på det. Altså, jeg synes jo det er rigtig godt at spørge dem også, ik. Men de vil jo tage meget meget hensyn til privatlivets fred og ...

Måske for meget?

Nej, jamen det ved jeg ikke. Det kan jeg ikke rigtig udtale mig om, men jeg synes, jeg tror i hvert fald, at de vil jo tænke meget mere på individet end på sikkerheden også, ik. De tænker meget på individet, tror jeg.

Det er jo deres job. [taler i munden på hinanden] Det er det de gør. Det er det input de kommer med. [taler i munden igen]

Ja, og det er derfor der skal være flere instanser så der er nogle, der ser det fra den ene side, og nogle der ser det fra den anden side.

Ja, det er der jo god grund til, hvis vi kigger på Danmarks love.

Jo, man kan jo risikere at gå på gaden og så blive bortført af en eller anden ... Det er jo godt nok skræmmende, ik. Altså.

Fordi man lignede.

Ja, fordi man lige kom til at ligne en.

Min bror ...

I: Synes I der skal stilles nogen krav til dem der udvikler nye sikkerhedsteknologier? At de skal sørge for at de fx tager hensyn til privatlivets fred eller ?

Ja, det kunne da nok.

Det er der relevans for.

Skulle man ikke mere stille krav til dem der bruger det? Altså, dem der udvikler et system, ja nu ved jeg ikke hvor meget de sidder og tænker over fordele og ulemper ved at bruge det i forhold til privatlivet, men spørgsmålet er om man ikke skulle stille nogle krav og regler op for selve brugen af det og dem der sidder bag ved det.

Anvendelserne af det.

Ja.

Jeg kan sige så meget, at jeg har ikke tænkt, før det her oplæg kom, så meget om privatlivets fred i forbindelse med de teknologier. Jeg har mere tænkt det der tekniske med, jamen, de er ikke 100%; så kan man ikke bruge dem. Agtigt. Så hvis man kombinerer dem, så kommer man tættere på 100%, men det er stadigvæk ikke helt godt nok. Det er sådan mere denne der tekniske del jeg har tænkt over.

Ja.

Ja, det tror jeg også er.

Ikke privatlivet. Jeg kan tilbyde dem teknologien og så kan de jo så, så er der så nogen der må sige ja eller nej til det.

Mmh.

Man kan jo sætte nogen begrænsninger på det.

Einstein... Ja [latter] Jamen hov, det var ikke det der var meningen med min opfindelse.

Nej.

Aj, men det kan da også være at fra man er nødt til at have flere ind og ... efter hvad det skal være...

Ja.

Altså Etisk Råd og alle sådan nogle. Folk, der ser på det med nogle andre øjne, ik. Menneskerettigheder og alt sådan noget, synes jeg. Vi kan da jo også lave en verden. Man kan da jo åbenbart også opfinde alting nu om stunder.

Det har du jo inde på hospitalsvæsenet ... og Etisk Råd. Det er jo en god grund til det, for der er jo højteknologi så det batter. Sætte nogen begrænsninger, ik.

Ja.

Nu har jeg sådan en føling med at I sådan lidt lægger fabLottens og dem der producerer de her ting, lægger deres ansvar ret langt væk for dem. Og det synes jeg måske ikke er helt på sin plads.

Nej.

Der er også sådan noget som et firma, der havde ... til at overveje, hvordan vil man gerne udvikle, hvad, man har også et eller andet som fabLotten er. Det firma, som har tænkt sig at udvikle de her ting. Et eller andet ansvar for at man udvikler noget, som er i overensstemmelse med det, som, ja hvad skal vi sige, etiske overvejelser. Der mener jeg da, at de fabLotten osv., man skal ikke bare opdage noget for at det kan jo opfindes. Det skal man ikke bare gøre, se hvordan det gik med atombomben, ik. Den var nok blevet opfundet før eller siden alligevel, måske. Det kan jeg et eller andet sted godt se, men hellere senere end før.

Det skal vel være samfundet der regulerer det, ik. [taler i munden] Man kan jo også bede dem om at regulere sig selv. Desværre.

I: Hvordan kan samfundet regulere, så? Har I nogen forslag til det?

Nå, men så ... ligesom man forsøger at regulere at virksomheder fx ikke må forurene. At de ikke må kaste alt deres affald ud i Skjern Å og whatever, ik. Så ... [54:53] ... det samme må man jo også kunne stille nogle krav til virksomheder, der fremstiller sikkerhedsteknologi. Det er meget svært at sige konkret om det, når man ikke selv er teknolog.

I: Med mindre at gøre lige som dig og sige de skal kende Grundloven, og det vi laver.

Altså, det, hvad skal man sige. Det ironiske er jo, at der er jo mange lande, europæiske lande, som laver en masse ting som ikke må bruges i landene selv, men så sender de det til nogle afrikanske lande og tjener en masse penge. Det er jo lidt samme princip, ik.

Det er medicinalindustrien du tænker på.

Nej.

Nej.

Det er fx våbenindustrien og sådan noget. Hvad hedder det. De laver en masse ting, som et eller andet sted ikke er etisk forsvarlige at lave, og som man ikke må bruge i landet. Jeg kunne da godt tænke mig, at der var en eller anden lovgivning om, at hvis det ik er lovligt at bruge og ... osv. i Danmark, så skal de sgu ikke rigtig lave det. Altså.

Nej, men så mister du bare arbejdspladser. [taler i munden]

Ja ja. Men ved du hvad, hvis de så lægger en fabrik i Polen, sådan en polsk fabrik og sætter nogle våben til Afrika i stedet.

Ved du hvad, det er måske lidt dobbeltmoralsk, men jeg har altså ... [56:08]

Ja, skål skål.

Men så er det ligeegyldigt jo.

Ja.

Nej, det er det ikke, for så har jeg ikke en dansk fabrik, der udvikler et eller andet som måske kan komme til at blive brugt i Danmark.

Ja. Jo jo.

I: Ja, nu tager vi lige. Jeg tror vi skal til at runde af. Og vi tager lige det sidste spørgsmål. Eller de sidste to spørgsmål i et hug. Og det ene det er om det at I har deltaget her i dag, om det har været med til at ændre jeres holdninger eller om I har den samme holdning som før, til spørgsmålet om balancen mellem privatlivets fred og sikkerhed, det er det ene. Og det andet det er, om I i øvrigt har nogle kommentarer som I gerne vil nævne her til sidst. Meget hurtigt.

Ja. Jeg må jo starte. Det har, ja, jeg tror også jeg sagde det før, det har fået mig til at tænke mere om sikkerhedsproblematikken, og det har også fået mig til at prioritere privatlivets fred højere, helt klart.

Ja.

Skal vi ikke alle sammen sige noget om...

Det glider på et højere plan.

Jeg har det samme fokus på som Jane. Det har ikke ændret min holdning, men jeg kan da godt se at der er udviklet noget nyt som jeg ikke lige var klar over.

Ja, der er i hvert fald meget mere, end jeg måske havde forestillet mig. Der er også meget jeg godt kunne tænke mig at sætte mig lidt mere ind i. Det må jeg sige.

Ja

Altså, jeg synes stadig ikke. Jo altså, der er selvfølgelig nogle ting sådan lidt mere i forhold til den der case og alt det der, hvor man sidder sådan lidt og tænker, nå ok, kan man nu også det, og sådan noget. Men jeg føler mig ikke hverken mindre tryk eller mindre negativ på nogen måde over for det. Og jeg har stadig den samme holdning. Mere overvågning. Aj. Heller ikke på den måde. Alt med måde. Men jeg synes helt klar at man skulle se på fordele og ulemper.

Ja. Er der andre der har mere at tilføje, eller skal vi gå ind til de andre nu? Var det kl. otte, det var det?

Det var det.

Så lad os se at komme af sted.

[58:18 min]

5.3 Transcript of interview by MIH

Indledning:

- Transskriberingen er foretaget med fokus på forståeligt dansk. Fyldord og problematiske sætningskonstruktioner er udeladt af transskriberingen.
- Interviewer går under bogstavet I er er markeret med *kursiv* og deltagerne med begyndelsesbogstavet i deres (anonymiserede) navn.
- [] angiver interviewerens kommentarer i transskriberingen

Interviewet:

I: På mit papir her, der har jeg en række spørgsmål. Ni spørgsmål. Jeg vil ikke tvinge jer igennem dem, fordi det er spørgsmål, der naturligt vil komme op. Jeg vil gøre mit bedste for at holde min mund, når vi først kommer i gang, fordi det er jer vi vil høre på og ikke mig, jeg har læst en masse materiale og har en masse holdninger, men det er fuldstændig ligegyldigt i dag. Jeg vil foreslå at vi starter med en runde, hvor vi siger hvad vi hedder, og hvad vi laver og noget i den stil og så stiller jeg det første spørgsmål og så kører vi derfra.

A: Jeg hedder Anders og er pensioneret lærer.

B: Jeg hedder Børge og jeg er, eller hvad jeg laver nu er måske ikke så repræsentativt, men jeg er tidligere fængselsfunktionær.

C: Jeg hedder Carl. Jeg er arbejdsløs civilingeniør.

D: Jeg hedder Dina, jeg er efterløner og designer.

E: Jeg hedder Elin, jeg arbejder i et videnscenter om børns brug af Internettet.

F: Jeg hedder Finn, og jeg er grafisk produktionsleder.

G: Jeg hedder Gitte og jeg er på [...] som produktionssupporter.

I: *Det er godt med nogle brede baggrunde. [...] Jeg vil starte med at spørge jer – efter i hørte vores ekspert, der gennemgik det, der stod i scenarierne, og efter i udfyldte spørgeskemaerne – hvad er jeres umiddelbare tanker om sikkerhedsteknologier og privatlivets fred? Det er et meget bredt spørgsmål, så start hvor som helst.*

A: Det er ligesom når man begynder at snakke om døden. Det er smadder uhyggeligt, altså det perspektiv, der er i alt det vi har læst om. Jeg synes man skulle basere diskussionen på hvilket samfund vi ønsker og hvad vi ikke ønsker, fordi der bliver talt meget til vores angst for fremtiden og det der store dyr, der hedder teknologi, og som vi ikke ved hvad er.

G: Jeg har det helt modsat – jeg synes det er helt i orden med alt det der, og det er fuldstændig ligegyldigt om vi bliver monitoreret på kryds og tværs. Formegentlig bliver det kun brugt i få sammenhænge og resten af tiden vil det bare være væk. Det generer mig ikke.

B: Jeg mener også at vi ikke kan få for meget overvågning, så længe at vi føler at det kan forbedre vores sikkerhed og samfund. Sådan noget som et DNA-register vil være en hel naturlig ting, hvor vi alle sammen blev registreret i sådan et. Jeg har ikke noget at skjule, derfor har jeg ikke noget at være bange for i den forbindelse.

G: Lige der er jeg virkelig uenig. DNA synes jeg slet ikke hører med i biometri. Det blev nævnt i et af spørgsmålene [i spørgeskemaet] og det opponerede jeg imod. Jeg synes ikke det hører sammen.

A: Det kan godt være det ikke hører sammen, men derfor synes jeg at det er i orden alligevel.

G: Det synes jeg ikke.

D: Jeg har det sådan, at jeg godt kan acceptere en hvis overvågning i det offentlige rum. Stationer osv. Men ikke når det drejer sig om iris-analyse eller ansigtsudtryk. Der står jeg fuldstændig af.

G: De bruger det allerede i lufthavne. Fingeraftryk og sådan noget.

D: Ja sikkert. Men det gør mig ikke mildere stemt.

F: Jeg mener det er utrolig vigtigt for vores sikkerhed og for sikkerheden i fremtiden, at vi bliver nødt til at acceptere denne form for teknologisk overvågning. Jeg mener det er den eneste måde vi kan sikre vores samfund imod al den terror, der desværre bliver mere og mere af og alle de syge mennesker, der render rundt og laver alverdens ting mod børn og andre mennesker. Der mener jeg at det er vigtigt at kunne finde frem til dem hurtigst muligt og sikre at der ikke sker noget med os andre. Jeg tror ikke det vil blive brugt i alle mulige andre sammenhænge, for der vil være så meget data tilgængeligt, så det er kun i tilfælde hvor der er en forbrydelse, og her bliver man nødt til at gå ind og finde ud af hvad det er for nogle mennesker der laver det her og så går man ind og bruger den her teknologi. Man vil ikke bare sidde for forgodtbefindende og synes at der er da meget sjovt af se hvad Fru Hansen laver her til formiddag. Det er ikke det, det vil blive brugt til.

D: Det ved du da ikke.

F: Nej, men jeg kan forestille mig at der er nogen der har lyst til at bruge tid på det.

B: Hvem skulle have interesse i det? Det kan godt være at man sidder her nu og tænker 'hvad mon naboen laver' eller hvis jeg kunne gå ind på min computer og se hvor mange penge han har på kontoen. Det kan da godt være at det er meget interessant, men i det lange løb, så er det jo altså ikke noget man kan bruge til noget som helst. Jeg synes at risikoen er stærkt overvurderet, for hvem har interesse i at vide, hvad jeg laver, ud over måske lige min kone, der gerne vil vide hvor jeg nu er henne. Derudover er der jo ikke nogen. Er der nogen af jer, der er interesseret i at vide, hvor jeg skal hen bagefter og hvor jeg kom fra inden jeg kom herind? Hvorfor skulle i det?

E: Jeg tror jeg sidder lidt og har det helt modsat. Jeg synes virkelig det er problematisk også nu med den der nye Terrorpakke, på engelsk hedder det 'data retention', hvor man begynder at logge vores informationer – vores adfærd på nettet, med forskellige teknologier, der kan følge os rundt omkring. Det er ikke et spørgsmål om hvad de teknologier bliver brugt til, det er mere et spørgsmål om hvad de gør ved vores kultur som sådan. Når vi begynder at regulere hinanden og lægge vores adfærd ind efter hvad vi ved der findes af teknologier – man går nogle andre steder hen på netter, eller når man taler sammen i det offentlige rum, så taler man lidt lavere eller at der er nogle ting man ikke vil sige nogle steder. Det gør noget ved vores frihed. Nu taler vi om at bruge de her teknologier i Danmark og det er fint, her har man respekt for folks

rettigheder, men der er jo steder i verden, hvor man jo bruger de her overvågningsteknologier, fx i Kina hvor man ikke kan lægge noget information ud på nettet uden at det bliver fundet af en eller anden regeringsinstans. Der er eksempler på at folk bliver fængslet for at bruge nettet til de forkerte ting. Det er så i udlandet. Derfor synes jeg at det er vigtigt at tage diskussionen. Jeg er ikke kun anti-teknologi, men jeg synes det er ekstremt vigtigt at man ikke bare siger at 'det er lige meget at der er nogen der overvåger mig. Jeg gør ikke noget.' Teknologierne gør noget ved vores kultur, som jeg synes er ekstremt vigtigt at tage højde for.

D: Jeg kan kun give dig ret. Jeg havde en kineser boende et år, som var IT-ekspert. Han sagde: 'Når du mailer til mig, så skal du være forsigtig med hvad du skriver'. Og det er jeg selvfølgelig. Det tænker vi ikke over som danskere. Vi skriver bare hvad vi egentlig lyster til vores venner og bekendte. Her skal du altså være forsigtig.

B: Hvis vi nu tager et tænkt eksempel. At jeg synes at min chef er en dum skid. Eller jeg har tænkt mig at gå fra konen, eller har en elskerinde eller et eller andet. Det sidder jeg og skriver til en kammerat eller ven. Så sidder der en, på en eller anden overvågningscentral og ser det og hvad så? Ham der sidder og kigger på de her kameraer ude i byen, han ser jeg piller næse. Og? Jeg vil være mest træt af at være ham der skal sidde og kigge på det. Jeg møder ham jo aldrig nogensinde: Jeg kender ham ikke, jeg ved ikke hvem han er. Det er jo ligegyldigt.

E: Det er jo fordi at vi i Danmark har nogle bestemte kriterier for hvad der er mistænkeligt. Hvem skal sætte de kriterier for hvornår dine handlinger er mistænkelige? Fx hvis nogle mener at når man begynder at tale om det og det emne, så er man mistænkelig, så er det problematisk. Der er ikke nogle grænser for hvornår en adfærd er mistænkelig. Det er det jeg synes er vigtigt at fokusere på. At det er en glidebane hen mod noget der ikke er ønskværdigt. Man snakker meget om terror og du [til A] snakkede noget om angst og jeg troede at du snakkede noget om en påduttet angst omkring terror. Terror har altid eksisteret, nu er den så rykket til vores samfund. Jeg ved ikke hvor meget teknologier faktisk kan gøre for at sikre os mod terror eller terrorangreb. Hvad giver jeg køb på? Det mangler også i den her debat.

A: Jo mere vi taler om sikkerhed, jo mere bange bliver vi. Hver gang jeg går ind på min netbank, står der: 'Du skal passe på fordi der er nogen, der er ude efter dig.' Og det står med rødt. Man må ikke åbne bankmails, som du ikke lige ved kommer fra banken. Du skal passe på, hver gang du kører med S-tog forbi Hovedbanegården. Du skal passe på at der ikke står en taske og passe på din egen taske. Hele tiden: 'Pas på – pas på'. Når man læser gratisaviserne har alle overskrifterne en eller anden form for aggression: 'Du skal passe på fordi det går galt eller fordi det er gået galt. Nu skal du bare læse alt det her.' Det er det jeg lægger mærke til.

E: Der bliver skabt en eller anden form for angst.

A: Så når der kommer et eller andet firma: 'Vi har lige lavet en eller anden sikkerhedssystem. Du skal tro, det skal nok passe på dig'. 'Ja!' [siger modtageren] 'Det har jeg brug for, for jeg er så bange i forvejen.'

G: Det er en god måde at se det på, men siger det ikke mere om modtageren, end brugen af det? Er det ikke modtageren der er syg?

E: Hvordan?

G: Hvis vi ser hele vores samfund. Hvis du ikke har den tillid til at vores regering eller noget vil bruge det på en måde som du kan acceptere, er det så ikke der du skal tage fat i stedet for? Så sidder de gale mennesker på toppen. [Alle griner] Der må være tillid et eller andet sted til at det bliver brugt [ordentligt]. Du kan ikke stoppe det. Det vil brugt uden din viden ellers. Så kan man ligeså godt selv styre det.

E: Det er jo lige netop det. Jeg ville ønske at sikkerhedsteknologier, hvis de skal fungere, så skal de være synlige, så vi ved hvordan de bruge, hvornår vores ting bliver logget, så vi kan vælge dem fra og til. Vi kan også have nogle mekanismer, hvor vi selv kan bruge dem, hvor vi selv kan rapportere. Give teknologierne over i hænderne på os, på borgerne, så vi selv kan udnytte dem. Det skal ikke ligge et eller andet sted, hvor jeg ikke ved hvor det ligger, og det er ude af mine hænder. Det er det jeg synes er problemet, også med sådan nogle sikkerhedsteknologier, at det er en glidebane mod at folk føler sig falsk sikre, og så gør de ikke i deres hverdag for at se hvad der sker omkring dem.

B: Det ville selvfølgelig være smartest når man var på vej hjem fra byen i en ordentlig koger og man ikke lige kan huske hvor man satte bilen, at man lige kan tage mobiltelefonen og få den til at spore, hvor den er henne.

F: Så du vil have det tilgængeligt, så du kan se hvad der er af oplysninger på dig, er det det du mener?

E: Også det. Men nu taler vi jo om mange forskellige former for teknologier. Nu bliver alt jo logget. Før i tiden ville jeg have sagt at jeg gerne ville vide hvilke websteder der loggede mine informationer og min adfærd på nettet.

F: Det gør de jo stort set alle sammen.

E: Det er jo det! [Alle griner] Det er jeg faktisk ikke særlig glad for.

F: Hele den kommercielle verden er jo langt fremme med logging af data og brugen af data. Når du er inde på en site, hvad du så klikker på, det ved den til næste gang, så ved den at sidste gang, der var du inde og klikke på denne farve kjoler, og de her bukser og sådan noget. Så vil den vise billeder af den type tøj som du var interesseret i sidste gang. Så ved de også at de personer, der har interesse for lige den slags tøj, de interesserer sig også for den her slags smykker. Så der vil også være nogle links til dem. Den kommercielle verden er langt længere fremme, rent teknologisk med de her ting, end de statslige er.

I: Jeg skal lige høre hvad Anders havde at sige, du markerede lidt.

A: Nogle af de spørgsmål, hvor jeg ringede ind [til AJ i Teknologirådet]. 'Vil du gerne registreres i busterminaler, i flyterminaler og stationer og sådan noget?' og jeg tænkte at det ville jeg vel egentlig gerne, for der kunne jo komme nogen og gøre mig et eller andet. Så tænkte jeg: 'Der er den igen'. Hvorfor skal man gå rundt og være bange? Hvorfor er det psykisk syge, der render rundt i samfundet og laver ulykker? Hvorfor er der nogen der smider alle affaldskasserne ud i Sortedamssøen? Burde man ikke stille nogle apparater op, som kan tage billeder af dem om natten? Vi må gå i stedet gå ind under og stille spørgsmål om hvorfor der sker sådan nogen ting og få fat i de her mennesker og hjælpe dem på en eller anden måde. Det er en gammel diskussion, den havde vi i '70erne, det kan være den er jo 'out'.

D: Jeg må sige, jeg blev lidt rystet i forgårs, da jeg blev ringet op af en gammel ven, jeg ikke har hørt fra i 23 år. Så siger jeg: 'Hvordan fandt du mig?' Så siger han 'Ja, du har et sjældent efternavn, så jeg fandt dig på Google.' Det var jeg ikke klar over at jeg kunne, så jeg slog mig selv op: 'Dina har samlet [xxx] underskrifter til fordel for [xxx].' 'Dina har blandet sig i debatten om [xxx].' Og det står der, og jeg står allerforrest. Det var lidt chokerende for mig. Så man skal nok være lidt forsigtig.

F: Det er den kommercielle verden.

B: Hvis man bruger tiden på det, så kan man jo næsten finde hvad som helst i små bitte detaljer. Lignenøjagtig med Google, der bruger jeg Gmail.. Hvis man får en eller mail, hvor der bliver talt om et eller andet bestemt emne, så ude i siden, der er nogle reklamer, der dækker det der stod i mailene, på det sprog som mailen er skrevet i. Det er jo vildt. Man må håbe at de ikke bliver gemt, mange af de oplysninger, men det gør de jo.

F: De bliver gemt, og de bliver solgt. Der er jo handel mellem de virksomheder med al det data her.

B: Så kan man købe én der er interesseret i ferieboliger i udlandet og kører på cykel. Så kobler man det sammen.

G: Men gør det noget? Det bliver jo nemmere at finde en ferie så.

B: Næ, egentlig ikke. Jeg ville ønske det var mig, der havde sådan en Google-maskine dér, jeg kunne lave penge på.

E: Så havde du lavet mange penge. [Alle griner]

B: Så havde jeg nok ikke haft tid til at komme forbi i dag.

A: Det er jo meget smart at vi kan google hinanden. Det gør jeg da også selv. Og jeg synes det er et pragtfuldt arbejdsredskab. Jeg kan også godt se den modsatte side. At det kan være ubehageligt. Jeg har skrevet en hel del læserbreve. Nogle gange så har jeg talt lige ud af leveren. Jeg bryder mig ikke om at se det linet op et sted på Internettet, for så vil jeg gerne have redigeret lidt i det.

F: Hvis du har skrevet et læsebrev, så er det vel fordi du gerne vil give din mening offentligt tilkende. Så er der vel ikke noget i vejen med det.

A: På det pågældende tidspunkt, ja. Men man bliver jo klogere. [Alle griner].

B: Så skal du lave en tilføjelse, hvor der står: 'Ved nærmere eftertanke, så ...'

A: Det er virkelig et synderegister.

F: Så må du fremover skrive til sidst [i brevet] at du i fremtiden kan ændre mening.

D: 'Med forbehold for fejl og mangler.'

F: Det kan vi ikke undgå. Lige så snart vi agerer på nettet, så bliver det suget og samlet op og vi vil kunne se os selv på Google ret hurtigt derefter. Og andre vil kunne finde os. Jeg synes det er meget sjovt. Jeg er faktisk også blevet kontaktet, af en klassekammerat, for ikke så længe siden. Som også havde fundet mig derigennem. Så det giver nogle nye muligheder. Også nogle muligheder for dem, der vil os det ondt. Heldigvis er der ikke så mange af dem.

B: Det der med at prøve at gemme sig. Nu da jeg var fængselsbetjent, der havde jeg nogle problemer med nogle af de stærke fanger, især rockerne og sådan nogle, som synes at jeg var en dum skid, fordi jeg passede mit arbejde. Så er der mange der siger: 'Har du ikke hemmelig adresse?' og sådan noget. Hvad fanden skulle det hjælpe? Så holder der bare en eller anden og venter, når jeg kører hjem og følger efter mig og finder ud af hvor jeg bor henne. Jeg tror ikke vi kan gemme os alligevel, så der er ikke nogen grund til at gøre sig store anstrengelser for det. Hvis der er nogen der vil det tilstrækkeligt meget, så kan de sagtens finde ud af hvem vi er og få vores CPR-nummer og alt muligt.

A: Det er mærkeligt med de e-mails. Nu får vi alle de der spam-mails.

B: Det er jo fordi at man kommer til at stikke næsen for langt frem og skrive sin adresse et eller andet sted, hvor man ikke skulle have gjort det.

C: Enten det eller også støder man ind i det faktum, at der er nogen der sælger lister over e-mail adresser, uden at have kigget på hvad de overhovedet får. 'Vil du købe den her adresse eller ej? Den eksisterer!' Det er simpelthen sådan nogle lange lister. Så er der også nogle, dem har jeg set, det er rene gæt. Jeg har en eller anden [e-mail] der bare er en bogstavkombination.

Og der kan du se at der er der gættet på, for den kan man ikke tro på. Der er nogen der har forsøgt at skjule sig, men så er de blevet ramt alligevel.

A: Der er nogen der spekulerer i sådan noget.

C: Men når man går den anden vej, så kan man vælge at have flere [e-mail adresser]. Jeg talte i går og fandt frem til at jeg har ti e-mail adresser. Jeg kan se at når der kommer noget på den ene adresse, så kan jeg have en idé om hvilken del af Internettet, det stammer fra. For det er kun nogen bestemte grupper, der har haft den adresse. På den måde er man jo på vej ind i noget identitetsstyring. Jeg opholder også indtil flere identiteter, alias, på forskellige steder på nettet, hvor man kan styre hvem der ved hvad, for du kan styre hvad du fortæller dem. Der sidder fx personer i Tyrkiet, der ved jeg eksisterer, og de kender et eller andet øgenavn, som de kender mig ved, de ved ikke hvad jeg hedder, men de ved hvilket land jeg kommer fra og det er også det. Hvor nemt vil de have ved at udnytte de informationer? Det er et spørgsmål om hvad du vælger at give dem af informationer. Alle mulige andre informationer har de ikke nogen jordisk chance for at få fat i, fordi de ved ikke de eksisterer.

B: Jeg kender også godt til det der med at have flere forskellige identiteter. Den dag at ham der sidder ovenpå [...]knappen får trykket på den og blandet hele lortet sammen. For de der adresser, de kan jo spores tilbage til dig. IP-adresserne og de kommer fra det samme sted fra. Hvis der er nogen der gider at bruge energien på det...

C: Det kan jeg sørge for at de ikke kan. Det vil tage mig omkring 3 millisekunder at gøre. Så er vi inde i et teknologikapløb; så finder de ud af at det kan spores alligevel og så videre.

B: Det kunne jo være at ham nede i Tyrkiet gerne ville vide hvem du er, så kunne han jo tage at spørge.

C: Så ville han jo også få flere oplysning. Jeg ved jo også nogen om ham. Jeg tror nok jeg ved hvor han arbejder.

B: Hvorfor fanden skulle han bruge en masse energi på finde ud af det, hvis du ikke vil fortælle ham det.

C: Umiddelbart har han ikke brug for oplysningerne. Det er derfor han ikke har spurgt om det. Der er mange der ikke spørger om oplysninger, det kunne være fordi de ikke har behov for dem. Det kan godt være at de kan få dem ad andre veje, men hvis de ikke spørger dig direkte, er de så interesserede i det? Når man sammenkører registre, kan man måske finde noget, men har folk behov for de oplysninger? Hvis folk har et legitimt behov for de oplysninger, så spørger de. Så kan du vælge om du vil give dem dem.

A: De skal ikke kontakte mig.

C: Nej, så kan du sige til dem, at det skal de ikke, og lade være med at give dem oplysningerne om hvordan de kan kontakte dig. Hvis de så bliver sure...

A: Kan jeg undgå at give dem private oplysninger?

C: Det kan du jo ved at lade være med at sende nogen mails.

A: Det ville være at holde mig uden for. [Alle griner]

B: Du kan jo få anonyme mailkontoer, der opløser sig selv i løbet af en time.

A: Det lyder svært.

C: Det er faktisk ikke særlig svært. Det er noget helt andet: Du indtaster adressen, adressen bliver oprettet, du modtager noget mail, og så bliver adressen, kontoen slettet efter x-antal timer.

F: Jeg synes spørgsmålet også er om staten skal have lov til at lave alle de her overvågninger og opsamle alle de her data.

C: På Internettet støder du hurtigt ind i det fænomen. Kan du begrænse dig til én stat?

F: Det kan du ikke, stat og kommune?

C: Du kan jo heller ikke begrænse dig til et land: Hvis du rejser med fly fra ét land til et andet, så kan du jo ikke begrænse dig til et land. Skal de to lande så også have lov til at snakke sammen?

F: Det er de jo nød til. Grunden til at vi skal samle al det her data op er pga af de systemer, der bliver udviklet, de bliver misbrugt. Vi vil gerne have alle goderne, vi vil gerne have en netbank, så vi slipper for at stå i kø hver lørdag nede på posthuset og skal betale alle vores regninger. Men netbanken gør også, at det er nemmere at bryde ind. Lige pludselig får vi digitale indbrud i vores netbanker. Det er vi jo så nød til at sikre os imod på en eller anden måde. Vi vil gerne betale regningerne hjemmefra, det er nemt og bekvemt og dejligt og vi slipper for at bruge en masse tid. Men der følger desværre også nogle andre børnesygdomme med - at der er nogen der gerne vil udnytte de her ting. Sådan er det jo hele vejen igennem. Vi vil også gerne surfe på Internettet og bruge alle de oplysningsmuligheder, der er for at hente ting og sager. Men det giver også pædofile mulighed for at lave databaser og misbruge vores børn. Sådan er det hver eneste gang der er nye ønsker om hvad vi gerne vil, så dukker der desværre nogen op, der gerne vil misbruge de her ting. Vi vil også gerne kunne køre sikkert på vejene alle sammen, desværre er der så nogen der synes det er sjovt af køre 240 og er fuldstændig ligeglade med at de har kørt nogen ned, de skrider bare fra det. Sådan er det bare, hele vejen igennem. Uanset om hvad vi taler om, også når ikke taler om teknologi. Der er altid nogen der misbruger tingene. Det er jo dem vi gerne vil smide et eller andet sted hen eller hjælpe, så vi alle sammen synes det er sjovt at være her. Det er jo sådan set det at det går ud på. Derfor mener jeg at det er vigtigt at staten kan opsamle al det her data omkring os. For det er det, der er formålet. Det er ikke at de skal se hvad fanden Fru Hansen sidder og laver, fordi det er fuldstændig lige gyldigt om der er nogen, der sidder og piller næse. Det handler om at vi kan få et samfund, og at vi kan få alle de her goder, vi gerne vil have. Men der følger desværre nogle andre ting med, og derfor biver vi nød til at suge al de her oplysninger om hvad vi laver, så de mennesker, der misbruger de her systemer, at de kan findes.

D: Men det er jo et fåtal, der misbruger systemerne, i forhold til dem der er clean og straight. Så hvorfor skal majoriteten leve under at blive overvåget i alle ender og kanter?

F: Det tror jeg at man skal vende sig til.

D: Promiller.

F: Jeg tror man skal vende sig til at have et mere overfladisk forhold til det og sige: 'Det er ikke fordi det er mig de skal kigge på. Det er fordi de skal finde dem, der misbruger det her. De er sku ligeglade med mig, så længe at jeg holder stien ren. Hvis ikke jeg gør det, så er det sku også i orden at de finder mig og gør noget ved det. Så er det fordi jeg skal hjælpes. Hvis jeg ikke holder stien ren, og render rundt og laver balade og kører stærkt på vejene og kører folk ned, så skal jeg da også hjælpes.

D: Der er meget big-brother is watching you.

F: Sådan kan du godt føle det. Min holdning er, at man skal have en meget overfladisk holdning til det her.

E: Det synes jeg bestemt ikke. Det er et spørgsmål om hvor meget politiet få adgang til. Det er svært når vi ikke tager udgangspunkt i en konkret sag, optrevling af et terrornetværk eller noget. Hvor godt et værktøj er de her overvågningsmekanismer til at finde frem til eller have en preventiv effekt til terrornetværk. Det er også lidt det, vi mangler i den her diskussion. For mig at se, så handler det om at skabe nogen skræmmebilleder, nogle angstbilleder, og så har vi nogle teknologier, der kan redde os. I stedet for at vi igen lægger teknologierne i hænderne på folk selv og gør sådan at vi selv skaber en god kontrol. Det er det jeg hele tiden siger, jeg synes det er virkelig problematisk.

F: Du kan jo ikke både få det ene og det andet. Så skal man lukke ned for det hele. Og så skal v lukke ned for det Internet der. Det bliver nok også bare en fuser [griner].

E: Nej. Vi har snakket om tre niveauer. Vi har snakket om regeringer, der går ind og henter data om os. Så er der kommercielle firmaer, der henter dataer med det formål at vide hvilke købsvaner vi har. Det er jeg flintrende ligeglad med. Så er der os selv, der ligger information ud om os selv og det har vi så heldigvis magt over hvad vi lægger ud og vi bliver mere og mere bevidste om at når vi lægger noget ud på nettet, så vil det være der altid. Det er tre meget forskellige ting. Det er ikke fordi jeg vil sige at Internettet ikke skal eksisterer, jeg synes at internettet er noget af det mest videunderlige der er sket. Og det er god mulighed for at udveksle information, for at tale med hinanden og for at kommunikere. Men jeg synes det er problematisk jo mere regeringen går ind. Internettet er et sted, der er ikke et medie. Hvis du ser Internettet som et sted ligesom når du ud på gaden, hvor mange ville bryde sig om at have en mand der cyklede efter sig med et kamera og filmede én, hver eneste sted man tog hen? Det gør man på internettet nu. Det synes jeg er problematisk.

B: Det der er den store forskel er at... Hvis nu der er en der cyklerefter alle med et kamera, ud over at de nok ville komme lidt til skade en gang i mellem, hvis bare det er alle oplysninger om alle, så er det i virkeligheden ligeegyldigt. Om det er noget du kan se ovre på den anden side af vejen, eller om det er nogen oplysninger, der ligger i en database, der er sådan set ligeegyldigt, så længe der er kontrol hvad det er man bruger de oplysninger til.

E: Det er rigtigt at det er meget meget vigtigt, at der er kontrol i den anden ende, men det stoler jeg ikke meget på at det bliver ved at være sådan.

A: Der er også noget psykologisk i det. Det ville ikke være rart, hvis der sad en her og tog billeder, mens du talte så sad jeg og tog billeder af dig. Det ville påvirke dig.

B: Det ville det nok, men det ville kun påvirke mig de første tre minutter.

A: Det er jeg ikke sikker på.

F: Det er også en lidt anden sag, for så sidder du og tager billeder af mig fx. Men det er fordi du vil et eller andet specielt med dem, måske. I det øjeblik at et kamera bare tager et offentligt rum, så tager det for det øjeblik at der skulle ske en eller anden situation med noget kriminelt. Så kan man gå tilbage og se: 'Her er han sku'. De sidder jo ikke og glør hele tiden efter hvad fanden vi render rundt og laver.

A: Vi kan ikke lide at der er nogen der lægger mærke til os. Det er ligesom det der med øjet, at han [gud] sidder deroppe og kigger ned og ser hvad du laver. Vi har aldrig brudt os om det.

G: Jeg havde én der slog min rude ud her forleden dag. Jeg ville sgu gerne have haft overvågning på. Det irriterer mig grænseløst at når man er afhængig af noget, at man så ikke kan have sine ting i fred. Der ville det have været fedt, at der have været overvågning. Det er helt banale ting. Men det er én af de gevinster, der kan være ved det, det er at man måske kan undgå sådan noget.

A: Hvor høj en pris vil du betale for det?

G: Jeg er ligeglad. Jeg har ikke noget imod overvågning. Men jeg vil gerne have sådan nogle gevinster her. Det generer mig grænseløst sådan nogle ting. Mere end det irriterer mig, at der står et kamera. Når det er der hele tiden, er det fuldstændig ligegyldigt.

F: Der er jo alligevel ikke nogen, der sidder og følger med i om du har været i Føtex tre gange i denne uge. Det er jo ikke det, der er spørgsmålet. Det der er spørgsmålet, er hvem der knalder den rude. Der kan man spole tilbage og så sige: 'Hov - det var ham her. Har vi et billede af ham i forvejen i en eller anden kriminel database? Nåhr det er ham der Ivan Larsen, han bor ude på den adresse, så kører vi ud og henter ham,'

A: Og sådan har vi det i dag. Sådan fungerer systemet. Så fanger man Ivan Larsen. Hvad gør man så ved ham? Man kan ikke gøre meget.

F: Det er jo så en ny sag.

A: Der er ikke blevet mindre grafitti i København de senere år.

B: Der er blevet mindre grafitti de steder, der er overvågning. Det er selvfølgelig det der, med at skubbe det et andet sted hen. Det er jo selvfølgelig også et mentallitetsspørgsmål om hvis man ikke har været med til at betale for noget, om man så bare kan ødelægge det. Det er jo en helt anden diskussion.

F: Når bankrøverne ikke kan bryde ind i bankerne, så begynder de at gå ind i dem, mens folk er der. Så det flytter sig selvfølgelig. Til nogen andre steder.

G: Nu taler man også om at man vil lave det præventivt. At man begynder at tage kriminaliteten før den sker. Så er vi ovre i 'Minority Report' [Spielburg film], hvor folk på baggrund af noget af noget bevismateriale, der peger på at de måske ville begå en handling, bliver arresteret. Det er ikke fordi jeg siger at Danmark vil se sådan ud. Vi har et specielt samfund, men det er de ting, jeg helst vil undgå. Jeg vil gerne holde på mine frihedsrettigheder.

F: Det er jo hele tiden et spørgsmål om hvor man selv vil sætte grænsen for brugen af de her data.

I: Jeg har et spørgsmål til jer, fordi jeg sidder og tænker at nogen af jer synes at det er helt i orden at blive filmet og nogen der er kritiske. Hvad gør man med dem, der ikke vil udsættes for de her teknologier i forhold til dem som gerne vil?

F: Så må de gå med sådan en plastik ting, der dækker deres ansigt. [alle griner]

B: Der er hætteforbud! [Mere grin] Det er jo svært når man tvinger folk til noget. Det er nemt nok, når der sidder et kamera ude på gadehjørnet, så må de sgu blive derhjemme, det er synd for dem. Det er selvfølgelig ikke særlig demokratisk eller venligt eller noget som helst over for dem.

F: Vi bestemmer hvem der skal sidde i vores folketing og skal afgøre de her ting. Så må vi pege på nogen, der enten synes det er forkert, eller synes det er rigtigt. På min datters skole har vi lige holdt afstemning om vi skulle lave tv-overvågning af cykelskurerne, fordi der var så forbandet meget hærværk op de der cykler. Det lavede vi som en afstemning og der var selvfølgelig nogen der var for og nogen der var imod, men flertallet var for og det der sket, er at der ikke er hærværk mod de cykler mere. Så er der formodentligt hærværk et andet sted, men det er i hvert fald ikke på ungerne cykler. Så det havde en effekt og beslutningen blev truffet ved en afstemning. Det er jo lidt det samme som når vi går til valg og giver vores mening tilkende gennem nogen politikere.

B: Der kunne man jo så tilbyde et cykelskur ved siden af, hvor der ikke var kamera-overvågning. [Generel latter] Så kunne man jo se hvor mange der ville holde der.

A: Jeg synes at det er en egoistisk holdning [...]

D: Noget jeg har lagt mærke er kommet tilbage til tv er Oplysning til Borgerne om Samfundet. Jeg kunne forestille mig at man brugte et indslag dér, for de fleste har i hvert fald tv. Så kunne man gå ind på kommunens hjemmeside, og så kunne man sige hvad man kunne stemme på, med forskellige sanktioner mht overvågning og sådan noget.

I: Så det er en anden form for demokrati du foreslår på det her område?

D: Ja, det er også fordi jeg har oplevet noget meget meget underligt. Jeg har engageret mig i de her tårnhøje huse her i indre by. Så var vi 200 mennesker, der blev indkaldt på Rådhuset sammen med Ritt Bjerregaard og Klaus Bondam. For det første blev det en retssag hvor ingen af de 200 borgere fik lov til at komme til orde. Senere skulle vi så gå i grupper, lige som her, og så fik vi at vide at vi slet ikke kunne pege på højhuse i Ørestaden, kun Vestamager og Indre By. Det var det ville undgå. Så udvandrede over halvdelen i protest. Så skrev vi bagefter til dem at det havde jo ikke meget med demokrati at gøre. Det svarede de ikke på. Vi skal passe på vores demokrati. Selvom de gerne vil have åbenhed på Rådhuset, så fungerer det ikke efter hensigten.

A: Jeg kan godt forstå jer på den ene måde. På den anden side er I jo også nogen frygtelige egoister. I tænker kun på det skide skur dér.

F: Ja. Hvad mener du?

A: Igen er det ligesom at vi som borgere bliver presset ind i nogle meget smalle holdninger, hvor vi tilgodeser vores eget, men hvad der ellers sker udenom, det er for svært. Det har vi ikke tid til. Vi kunne have taget en stor debat på skolen om hvorfor der er nogen der ødelægger det, og hvem er det egentlig, der gør det.

F: Det kunne man jo ikke finde ud af, for når man stillede nogen ud for at kigge, så var der ikke nogen. I det øjeblik, der ikke var nogen, der blev piftet cykler og hvad der ellers skete.

A: Lærerne kunne have taget det med i undervisningen. De kunne lave et undervisningsprojekt ud af det: 'Hvorfor bliver der ødelagt så meget - hvad er det for en mentalitet der er hos os?' og så videre.

F: Det havde også været gjort inden. Lige meget hjalp det. Så ender man et sted som her. Det var ikke fordi der ikke var prøvet noget andet. Det var vel sidste ud kald, sidste idé der kom på bordet. Det er konsekvensen af det her, vi bliver nødt til at lave overvågning.

G: Det udelukker jo ikke sammenhængen med undervisningen.

F: Nej, og der er jo ikke nogen registrering af de her børn. 'Peter var ikke i skole i fredags, så han har sgu nok pjækket.' På den måde, er der ikke nogen registrering af det. Kun i det øjeblik at der var noget. Det var også det vi blev enige om på det måde - det skulle kun bruges i det tilfælde at der var kriminalitet eller hærværk derude. Så kunne man spole tilbage og se hvem er det der har gjort det.

A: Man ved jo godt hvem det er. Skolepsykologen ved det og så videre.

F: Selvfølgelig, men man kan ikke dømme folk, hvis man ikke har nogen beviser.

C: Så skal man lægge på lur derude eller noget.

F: Vi skal jo heller ikke rende rundt og være politifolk på sådan en skole.

A: Hvad skal vi så være? Vi må jo ikke noget. Vi må jo ikke tage et barn i nakken. Det gjorde vi i min barndom. Så fik man en på kassen. Så gjorde man ikke det mere. Man må faktisk ikke noget. Så sætte man i stedet hele apparatet til.

B: Det er et grundlæggende problem i samfundet, at man ikke føler et medansvar for at tingene skal fungere og medansvar for at tingene er pæne og ordentlige og sikkert for alle. Det er vel et symptom på den tid vi lever i, hvor man er sig selv nærmest. Hvis ikke skraldespanden ligge og flyder foran ens egen dør, så er man egentlig ligeglad, for så lægger den et andetsteds og så må de selv rydde op. Folk smider affald ud af vinduet og hvad ved jeg. Det er jo fordi at vi er ligeglade med hinanden. Desværre.

A: Så er det jo der vi skal sætte ind.

F: Hvis alt var godt, så var der jo ikke nogen grund til overvågning. Så havde vi jo ikke behøvet den overvågning på skolen. Så havde vi jo ikke behøvet politifolk og al ting. Desværre så er det nødvendigt.

E: Er det nødvendigt? Vil det ændre noget? Vil verden blive anderledes på grund af overvågning? Vil vi få gjort kål på terrornetværk og uetiske handlinger? Det tror jeg ikke, jeg er meget meget enig med dig [A] om at man skal tage fat i problemet, og ikke sætte sin lid til at der er et overvågningskamera, eller at nogen logger information og så skal de nok finde frem til den forbryder.

F: Jeg mener heller ikke at man bare skal læne sig tilbage og så sige at nu er alting godt, for nu er der et overvågningskamera. I det øjeblik man får fat i de her, så skal de jo hjælpes, så de finder ud af at det er det forkerte at gøre. Så der skal selvfølgelig også sættes nogen ressourcer af til at hjælpe de her mennesker, det er ikke nok bare at lave overvågning i sig selv.

E: Jeg tror bare ikke jeg har den store lid til at de her sikkerhedsteknologier har den store effekt. Det skal være til en hvis balance, for jeg tror ikke det kan afhjælpe nogen problemer på nogen måde, i forhold til hvad der sker ude i verden.

B: Det kan ikke afhjælpe noget, det tror jeg du har ret i. Men det kan måske begrænse. Det kan gøre os mere bevidste om nogle ting. Det kan måske gøre at vi kan fokusere de ressourcer vi har de rigtige steder. På den måde, mener jeg godt vi kan bruge dem, men det er rigtig nok - nogen gange synes det at være lidt af en overdrivelse. Hvorfor gøre en hel masse ud af sikkerheden på et eller andet område, når det er sådan at man lige kan gå udenom og så aflevere et eller andet derovre. Man skal passe på med bare at gøre det, for at det skal se ud af noget. Det skal være noget man skal have gennemtænkt.

D: Jeg har svært ved at forstå, det er måske et sidespring, når man med Schengen-aftalen åbner alle grænser, enhver kan passere vores grænser, i det øjeblik du stiller dig ind i en lufthavn, eller som det her blev forslået på en metro- eller S-togsstation, så skal vi overvåges med fingeraftryk og sådan noget. Det hænger ligesom ikke rigtigt sammen.

A: Det er prisen for at ophæve grænsen.

B: Det er det jo lidt i virkeligheden. Når du sætter dig op i en flyver og flyver uden for Schengen, så skal du have den der grænsekontrol. Så er det jo ikke så meget fordi, hvor du er henne, så meget for at vide hvem der skal med flyveren. Det er for at kontrollere den samlede gruppe i flyveren. For at vide hvem der er.

D: Det givne eksempel, vi fik sendt hjem til os, handlede om to personer der henholdsvis kørte med et tog og tog et fly. Ville du [til B] bryde dig om at hvilken som helst vidste om du skulle fra a til b og hvor du i det hele taget skulle hen.

B: Jeg ville ikke have noget imod det, for det er ikke hvem som helst, der får det at vide. Der er jo ikke nogen der vil vide det. Hvem skulle det være? Jeg går hen og sætter fingeren på, og så kører det fuldstændig automatisk. Jeg behøver ikke at have billetten eller klippekortet oppe af lommen, jeg behøver ikke tænke på om det er vådt eller udløbet eller hvad der er. Den bliver bare trukket på min konto. Det ville jeg bare synes var genialt.

D: Det synes jeg simpelthen det er frastødende.

B: Hvem skulle være interesseret i at bruge en masse energi på at finde ud af hvor du nu har kørt i tog og har været henne.

D: Nej, det er muligt.

B: Det er ikke noget der betyder meget for mig.

F: Forestil dig hvor lang en liste over personer, der har kørt med det tog fra den ene station til den anden, tror du der er nogen der vil sidde og tæske igennem og du lige netop har kørt med det tog, og om du også var det i går. Det vil de altså kun, hvis de synes du har købt lidt for meget sprængstof på det sidste.

G: Tænk hvor billigt det ville blive at tage med DSB, når der ikke var nogen der kunne snyde sig til billetten.

I: Jeg har en par spørgsmål vi skal igennem, de allersidste. Vi har jo allerede brugt næsten en time på det. Jeg har et spørgsmål her, vi har berørt det. Der står: 'Hvem bør involveres i beslutninger om ny sikkerhedsteknologi?' Det er igen et spørgsmål til den demokratiske process, for det jo også det, der skal komme ud af det i sidste ende. Har I nogle meninger om det?

D: Borgerne. Netop som jeg foreslog før. Folkeafstemninger.

B: Det tror jeg også, men jeg tror også man skal passe på ikke at blive for specifik og sige: 'Sådan og sådan og vi har de her tre forskellige muligheder, det her kan vi gøre og det har de her konsekvenser - det her kan man gøre, det har de her konsekvenser.' Og så videre. Så kunne man få borgerne til at give en indikation af hvilken retning det er vi skal gå i. Men så tror jeg også, at 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.

D: Det tror jeg du har ret i, men jeg mener stadig at man skal spørge borgeren før man tager et så grundigt step ind i deres liv.

A: Det tror jeg også. Man skal måske gøre det på den her måde. Jeg ved ikke hvordan man skal hegne os ind [udvælge]. Nu blev vi trukket ud gennem folkeregisteret og det er så fint nok, og der var kaffe og blødt brød. Man skal være så bevidst om, at hvis denne udvikling kører videre uden borgerne er med, så sker der nogle ulykker. Eller også bliver vi bare fuldstændig sløve og siger at det har vi ikke noget forstand på, lad os bare køre det. Der tror jeg altså at politikerne skal ofre nogle penge. Lad os lave meget diskussion om hvad det er.

G: Det breder sig som ringe i vandet. Vi har siddet hele dagen til pauser og sådan noget og diskuteret på arbejdet, fordi jeg sagde at jeg skulle herind. Så det er en meget god måde. Det er ikke kun os, det er alle de cirkler som er med til at vende det. Det er også nogle sjove diskussioner i stedet for at snakke tv-programmer.

A: Jeg har også snakket med nogen om det.

F: Jeg tror ikke det skal være en folkeafstemning alene. Det skal man ikke basere det på, for der vil folk være for vævende og sige: 'Ej, det vil jeg helst ikke tage stilling til, så jeg siger bare nej.' Så kommer vi sgu ingen steder.

A: Demokrati er ikke afstemninger, demokrati er diskussion.

F: Derfor tror jeg at du [A] har fuldstændig ret. Man skal gøre sådan noget som man gør her. Man skal invitere en hel masse mennesker ind for at diskutere, hvorvidt man skal gøre de tiltag man har i tankerne eller ej. Frem for at gøre det med et ja-nej kryds.

A: Ligesom på Internettet, der er spalten ude til højre.

F: Så skal man, som du [B] er inde på, også have et panel af nogen som forsker i det, som har en anden indgangsvinkel til det. Ud fra alle de her synsvinkler, kan man så tage en beslutning.

I: Et andet spørgsmål, som jeg også har stående her, og som jeg heller ikke rigtigt har været rundt om, det er: 'Skal det stå frit for alle firmaer at udvikle, sælge og købe sikkerhedsteknologier?' Eller skal der være nogle begrænsninger for hvad man må udvikle og bruge?

F: Ej, det må du gerne sætte en stopper for. [Alle griner]

I: Det er jo faktisk én af pointerne med EU-regulativet, eller det vi sigter mod i sidste ende. Det er at EU skal kunne sige: 'Hvis i udvikler fx teknikker til data-sammenkørsel eller registrering, så må i kun udvikle teknikker, der går der og der til.' Eller man må kun markedsføre teknologier, der kan det og det og det. Så der er faktisk mulighed for at påvirke de her ting i en eller anden grad.

B: Du kan jo dårligt opstille grænser for hvad du må udvikle. Du kan jo ikke stille grænser for hvad for en tanke manden tænker, hvad det er for en god idé han får. Men du kan selvfølgelig sætte en grænse for, hvad det er at han må sælge og hvad han må markedsføre. Det skal man også helt klart gøre. Der skal man have en definition af hvilke ting, man mener falder inden for det område, og så skal man have en autoration, man kan miste, hvis man overskrider de her grænser.

A: Det synes jeg er det sværeste spørgsmål, for hvis vi siger nej i Danmark, så siger de måske ja i Kina. Det er ligesom med menneskekloning. Der er vi næsten alle sammen enige om, at det må vi ikke, men det kunne jo godt være at eller andet sted i verden, sidder de og pusler med det og så en dag [laver kliklyd med tungen]. Sådan er det også med sikkerhedsteknologier. Det er ikke til at styre. Men derfor skal man forsøge at styre det alligevel.

C: Du får en indirekte styring, for hvis du styrer på hvad folk må sælge, så hvis firmaet er interesseret i at tjene penge, hvorfor skulle de så forske i noget de ikke kan sælge og tjene penge på? Så får du en indirekte styring af hvad de forsker i og hvad de udvikler.

A: Skal de have lov til at lave små atombomber, man kan have med i sin håndtaske?

C: Hvis de kunne tjene penge på det, så ville de udvikle det. Nu kan de ikke tjene penge på det, fordi de ikke må sælge det, så udvikler de ikke i den retning. Så har du fået en indirekte styring, for du har ikke forbudt udviklingen, men har indirekte fået skubbet det i en retning.

[Alle taler i munden på hinanden]

A: [...] Al-Qaeda smider en beskidt bombe et eller andet sted.

C: Hvorfra skulle jeg vide om de gør det? Det kan godt være i det specifikke tilfælde der, der er det faktisk forbudt. Ellers, hvis firmaerne ikke kan sælge det, hvorfor skulle de så forsøge at udvikle det? De vil jo tjene penge.

A: Det kan være de er idealister.

C: Den slags folk eksisterer jo også.

A: Ja det gør de nemlig.

C: Så kommer du over imod at det ikke er et firma, der udvikler det, men en gruppe af mennesker, der ikke har til formål at tjene penge på det. Er det så et firma?

A: Sindssyge stakler.

C: Hvis de ikke har til formål at tjene penge, hvordan kan man så styre dem overhovedet? De gør det for deres egen skyld.

A: Eller en højere magt.

C: Dem kan man jo ikke styre med hvad de må sælge og ikke sælge.

A: Det skal helst ikke være for avanceret, det vi finder ud af, så bruger de det jo bare. Lad os holde det nede på...

F: Jeg tror ikke man kan styre det ret meget. Man kan selvfølgelig styre det ved at lovgive om hvad man må sælge og ikke sælge. Men selve udviklingen, kan man ikke sætte i båd, det vil blive udviklet. Så ender det alligevel med at man laver en eller anden regel med at så må man gerne udvikle, og man må også godt sælge det, men man må ikke bruge det. Du må også godt købe det, men du må ikke bruge det.

A: Kun til eget brug. [Alle griner]

C: Du har også den der side af det. Et eller andet specifikt, må du ikke udvikle. Hvad med en videreudvikling af det, det kan jo godt være at der er nogle fordele af det. Skal du så forbyde dem at udvikle den første ting, som de så kan udvikle videre på, og så finde et eller andet, der er meget brugbart?

B: Man kan ikke forbyde forskning.

C: Hvis du forbyder forskning, så får du måske hæmmet udviklingen til at komme frem til noget, der vil være til alles fordel. Det kan du jo ikke være sikker på, på forhånd.

A: Vi kan ikke en gang forhindre børneporno. Det er jo det.

C: Det kan du ikke, nej. For hvis du skulle have fat på det, så skulle du måske have forhindret udviklingen af fotografiapparater.

B: Det er lidt sent.

C: Det er én mulig videreudvikling af fotografiapparater.

I: Så tror jeg det er slut, med den almindelig diskussion, jeg har lige et par afrundende spørgsmål. Har I ændret holdning i dag, efter I har været til det her møde og sikkerhedsteknologi og privatliv? Eller har I bare argumenteret for jeres position, så godt som I kunne?

F: Jeg har ikke ændret holdning.

[Resten] Nej.

B: Når nogen melder sig til sådan noget, så er det jo fordi de har en holdning, og de er nok ikke nemme at rykke ved. [Alle griner]. Hvis du siger at det kun er tre procent der melder sig.

A: Vi kom for at vise vores holdning.

B: Nu skal vi fandeme nok vise de andre, hvad de skal mene. [Latter]

I: Godt. Er der noget I vil tilføje, så er det nu, sidste chance.

F: Jeg synes det har været fint at diskutere.

I: Fint. Så stopper jeg denne her [HD-recorderen].

5.4 Transcript of interview by UV

Indledning:

- Interviewer er markeret med I: og *kursiv*.
- [xxx] markerer udeladte stykker.

Interview:

Ulla: Sådan og den skal vist ligge på noget der var blødt. Sådan. Godt. Øh, det som vi er her for det er jo selvfølgelig at høre jeres holdninger. Så det gælder, det er ikke nogen test på teknisk viden. Øh, det er noget med hvad er jeres holdninger til det her. Og øh, det er også okay ikke at have nogen skrå sikre holdninger, men også at være søgende. Hvis det er der man er. Øh, Øh og vi kan starte med det første, øh, som er sådan et lidt åbent spørgsmål. Det er, jamen nu har I hørt på oplægsholderen og I har udfyldt spørgeskema og I har forhåbentlig også læst det informationsmateriale, altså de scenarier som I har fået tilsendt. Hvad er så hele jeres sådan overordnede indtryk af det her. Og I kan bare tale frit for leveren, øh, skyd med hvad som helst. Ja.

A: Jeg har undret mig over, at man går ud fra at der er en mistillid til overvågningssamfundet. Det har jeg undret mig meget over.

Ulla: Ja.

A: Altså jeg føler mig rigtig godt tilpas, hvis der er overvågning. Og jeg har også været i nogle situationer, hvor vi blev sådan overvåget, passet på. Det synes jeg var rigtig rart.

Ulla: Ja. Hvad, hvad var det for nogle situationer?

A: Det vil jeg ikke fortælle om.

Ulla: Nej, okay, det er helt i orden. Ja, ja. Ja, ja. Hvad var det så i vores materiale du synes, og sådan i oplægget du synes der er denne her mistillid til det her?

A: Ja, det synes jeg også. Ja, jeg har faktisk skrevet at, øh, jeg har skrevet nogle bemærkninger i materialet, hvor jeg egentlig undrer mig over, altså, øh, øh. Du nævnte det også lidt i starten.

Ulla: Ja. Ja. Ja ja jeg synes.

B: Men føler du dig fuldstændig overbevist om, at overvågning virker?

A: Det tør jeg overhovedet ikke udtale mig om.

B: Jamen fordi jeg har nemlig, altså hvis jeg sådan skal sige så, hvis man har prøvet at rejse i USA efter den 11. september ikke så har man, altså man skal jo møde flere timer før flyet går og man skal igennem meget meget omfattende sikkerhedstjek ikke og jeg tror jeg var igennem tre sikkerhedstjek sidst jeg var der ikke. Altså først det første og øh, så det andet og så blev vi tilfældigvis som udlænding udvalgt til en anden gang security også. Det viser sig så kun at være udlændinge der blev udvalgt til det, for så slap de for retssager fra amerikanere hvis de stod og tog på dem. Så det kan man jo så sige, at det var en fejl at I ved det. Man gør..... Så er det jo så heldigt at hvis man har et pas (...). Der, da slog det mig at øh, det er jo til, i en lufthavn er det jo til at komme til ikke. Altså, det er sådan et enkelt sted hvor du kommer ind og du kommer næsten igennem sådan en trakt, der ender i et fly. Så, så i efteråret var jeg nede på den der xxxbanegård, der ligger i Madrid. Kan I huske der hvor der blev sprængt bomber den 11. marts. Og det var jo fuldstændig lige så åbent som det altid har været. Altså det var jo genopbygget, man kunne overhovedet ikke se at der var sket noget, altså det var genopbygget. Og øh, folk kunne komme og gå, ind fra gader og alle mulige niveauer og skifte fra tog til tog. Der slog det mig bare, at, at det er jo lige så farligt der. Det er lige så nemt, den dag i dag at tage en bombe med i det tog og sprænge den. Præcis det samme som der blev lavet, øh, den 11. marts. Men det er jo helt uoverskueligt, hvis man skulle til at sikkerhedstjekke, altså, alle de pendlere der skal på arbejde, der skal skifte tog, på den der hovedbanegård. Det er jo fuldstændig, altså det slår mig bare, at det er sådan lidt tilfældigt at så vælger man lufthavne, fordi der er det ligesom praktisk muligt at lave noget, noget sikkerhed. Men, hvis nu man også f.eks. forestiller sig at man skulle gennem de samme sikkerhedstjek i vores S-tog system. Så ville folk jo aldrig komme frem til arbejde. Altså hvis du skulle have kigget den mappe igennem, hver gang du steg på på Østerport station.

A: Jamen synes du så ikke der er nogle gode forslag til hvordan man kan rejse og komme hurtigt igennem?

B: Se, der vil det jo, hvis du har, hvis du har, alene Ringbanen her øh, der kører 100.00 om dagen.

A: Ja.

B: Hvis alle de mennesker skulle sikkerhedstjekket, selvom hvis man gjorde det meget meget strømlinet og meget meget effektivt, så ville det jo ta tid.

A: Jo, men tager jo også tid at du stempler din billet. Nu ikke, hvis du kører med billet.

B: Altså så vil du gøre billetten til sådan et sikkerheds.

A: Det ku man måske gøre ja.

B:

A: Altså jeg vil jeg er bare bange for. Altså det du snakker om er jo blot et teknisk problem, der skal løses.

C: Man skal vel også overveje om, om, om det er det værd.

B: Altså. Ja det er klart. Du kan jo vende den om og sige, at, at hvis man er terrorist, jamen så skal vi jo sikre alt. Alt forsyning. Du kan jo hælde bakterier ned i vandet, der kan slå os alle sammen ihjel. Altså, der er jo masser af muligheder for, og lave det. Og terroristerne er jo heller ikke dumme. De kender jo også at man nu vil ha, følge deres øh, øh, deres telefoner. De finder jo på noget nyt hele tiden. Altså, så vi kan jo blive ved i en uendelighed. Jo jeg ser faren, og jeg synes at.

A: Nej, det tror jeg ikke. Jeg tror ikke du kan blive ved.

C: Jooo.

B: Sådan har det jo været altid. Lige siden at man startede menneskeligheden. Forbrydere kan jo altid finde på et eller andet. Men der hvor jeg ser den store fare det er jo, at det eneste.

A: Altså jeg synes stadig at man hørt om positive øh, afklaringer af både forbrydelser og indfangning af vestgående terrorister.

B: Nu siger du opklaring, jo jo. Når du opklarer noget, så finder de jo på nogle nye fremgangsmåder.

A: et er jo lige meget. Altså så er det med til at udvikle teknologien i det hele taget. Det er jo også positivt.

C: Men du skal tænke den anden vej også. Altså sige, prøv nu og tænk et politisk system, som begynder at kontrollere alt hvad vi foretager os.

A: Ja...

C: Så varer det jo altså ikke ret længe inden vi ikke, hvis man vil misbruge det altså. Hvis, hvis vi nu tænker Hitler for eksempel. Han vil jo kunne styre os alle sammen. Vi kan jo ikke.

A: Nej, det tror jeg altså ikke.

C: Det er jo ganske enkelt

A: Nej, det er en følgeslutning du kommer med dér.

D: Det er lige præcis den største problematik omkring den her sikkerhedsteknologi. Det er simpelthen det der med, at vi bliver. Det kan proppes sammen i en eller anden database og så

ligger der bare en eller anden totalprofil på mig. Og det synes jeg er meget skræmmende og jeg synes at det bliver jeg endnu mere utryg over end at en eller anden terrorist kommer med en bombe. Mmmm, hvor jeg også tænker hvem er det der skal sidde og øh, registrere de der data. Bare noget helt banalt som et aktivt kamera. Hvem skal sidde med det? Hvad, hvad for et sikkerhedstjek skal man give den person? Øh, fordi vedkommende får jo nogle oplysninger som, jo så også kan misbruges. Øh, så. Hele vejen igennem, når jeg har læst om det her, så, så har jeg hele tiden set det som som det sværeste. Det sværeste dilemma det er, at hvem er det der skal have adgang til alle de her dataer der kommer frem omkring mig og borgerne.

B: Man kan også samle så mange data så man ikke, så det ikke. Der skal jo også være en hvis mening med tingene ikke. Du kan jo også få bunket så mange data sammen at du overhovedet ikke kan overskue mængden af data ikke. Altså.

D: Lige præcis. Altså. Du kan bare google dig selv ikke.

Ha ha ha.

Ulla: Inden vi kommer ind i diskussionen sådan for meget om fordel og ulempe, for den skal vi nok få, øh, så skal jeg lige høre, hvad er er andre første håndsindtryk? Hvad tænker I sådan umiddelbart?

E: Jeg synes vi er på vej til at få for meget af øh, jeg synes det går ud over min privatsikkerhed. Helt sikkert. Så det kan jeg, det fremgår også sådan som jeg har svaret. Nu har jeg selv været ansat i Kommunedata, hvor vi lavede, øh, social systemer. Og hvor der var en skarp grænse imellem systemet. Man kunne ikke engang sende det til en anden kommune. Og det syntes jeg var fint. Og efterhånden så kan man samle alle data op og det bryder jeg mig ikke om.

A: Hvad hvad kan du, jamen altså, ja medmindre du har.

E: Jamen jeg har ikke gjort noget forkert. Jamen jeg har ikke gjort noget forkert.

A: Jeg kan ikke forstå hvad det er du.

E: Jo det bryder jeg mig ikke om. Banken begynder også at skrive ud om om om de må give det til den forsikring som øh som de nu har osv. Og det siger jeg ja til fordi jeg selv har en forsikring der, men jeg synes nok at der er en grænse på det. Altså sikkerhedsmæssigt øh, øh, altså, øh, vi har i vores egen vej der har vi et system hvor vi øh kan, når der kommer en tyv så kan vi se hvilket hus den går ind i. Men øh, og det er så syv huse vi har koblet sammen. Jamen det synes jeg er ok. Nå ok. Men øh, men øh der er altså en grænse for øh, hvad jeg vil overvåges med. Og jeg har ikke gjort noget kriminelt og min familie heller ikke.

A: Nej nej.

Ulla: Øh ja, og der er. Jeg har øh. Der er et par stykker der ikke sagt noget og dem tager vi lige først.

F: Øh jeg synes øhTeknologisk Råd fra middle east og fra Afrika og ja jeg synes det her her arbejde, det er ikke kun danskere ser skal arbejde med det Teknologisk råd ja. Jeg synes altså udlændinge skal.

Ulla: Jamen synes du det er et problem?

F: Nej øh, det Teknologisk Råd arbejde øh, det kommer udlændinge mennesker, ikke danske mennesker kommer her. Øh, som fra Somalia for eksempel. Jeg håber arbejde med teknologisk Råd ja. Ja. Ja. Jeg ikke forstå nu her. Jeg håber tager øh kursus som det er.

Ulla: Så det er interessant at arbejde med?

F: Ja, ja. Og jeg synes det kommer også udlændinge. Ja. ja.

Ulla: Det er sådan dit første indtryk. Ja, jeg synes. Ja.

G: Ja. Ja. Jamen altså jeg er nok lidt mere sådan til tanken om, at altså den der tanke om at du kan overvåge. Altså den der kan hvad hedder det, der kan udfolde sig til det uendelige og der er ikke grænser for hvad man kan gøre. Altså, det er den der S-togs mission, hvor alle skal

trykke, hvad hedder det, fingeraftryk af inden man stiger ombord. Det kan du i princippet godt gøre, men altså det er de der sådan langsigtede konsekvenser der er fuldstændig skræmmende og tænke på og og jeg, når man sidder og læser sådan et stykke papir her, det der spørgeskema så synes jeg nærmest man, man øh har på fornemmelsen at der er sådan en teknologi forældelse i hele i hele spørgeskemaet. Altså, altså. Hvis man læser ned og svarer på, og læser på ned og ser hvad jeg har svaret på så, man har næsten svært ved at svare det er skidt fordi man bliver præsenteret for det som om det er et gode. Det er meget skævt spørgsmål. Øh, og øh, man ved hele EU vinkelen på at informationerne og hele den, hvor glade de er for det. Altså siger jeg, jeg er meget bekymret øh, også hvad i forhold til sådan sådan en session har, hvilken sammenhæng den bliver sat ind i. Nu er, man frygter jo, lige her har man jo så fundet en eller anden vis øh, øh skepsis overfor informationsteknologier og anvendelsen af det. Men, men sådan i det politiske billede kan sådan nogle møder her, sådan nogle borgermøder sådan meget hurtig få karakter af sådan populistisk udtræk af hvad er det lige nu og her er er spillere. Hvad er det der er let for mig? For jeg sidder her som loyldig borger. Det er nemt for mig og sige jamen bare registrer det hele og 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 én. Også selvom det ikke er i en eller anden øh, i et kriminelt øjemed. Jamen simpelthen bare for at i et tilfælde hvor man pludselig gør, at den her registrering kan gå hen og blive et problem. Og, og hvad så? Det, altså det synes jeg simpelthen er problemet. Men udover alle grænser. Øh.

A: Har du tænkt på, øh, hvor meget der skal til af tid, hvis nogen de gad grave ned og, og, ja for eksempel lytte til den der båndoptagelse og registrere hvad du havde sagt. Hvis der var nogen der gad gå selv dig i den grad. Jamen hele det her overvågningsperspektiv. Jamen hvad vil det ikke kræve af tid og ressourcer? Det er jo fuldstændig latterligt. Det vil jo ta et helt liv ikke altså.

G: Det er jo heller den vurdering du foretager med hensyn til informationsteknologi. Der registrerer du jo ikke, eller der interesserer du dig ikke for den enkelte information. Nej du interesserer dig for den enkelte information, når den viser sig at være relevant og så tager du udgangspunkt i den lille bitte information som egentlig på det daværende tidspunkt da den blev registreret nok kunne være nok så uinteressant, men fordi man lige pludselig identificerer den som værende interessant, så kan du lige pludselig gå tilbage og støtte alle mulige andre irrelevante informationer sammen og koble det op på en person, som så lige pludselig kan sidde der i øh helt u utilsigtet og have fået den her nye profil som en eller anden big brother kan sidde og stykke sammen. Og det synes jeg simpelthen er er så skræmmende som noget kan være.

A: Tror du ikke at han vil blive opdaget på en eller anden måde? Eller af. Nej det. Øh.

G: Nej det er det der er hele tanken bag informationsteknologien det er jo ikke, altså, det er jo, der er kun den begrænsning som dem der har systemet sætter. Der er ikke nogen begrænsning i

den måde du kan anvende det, andet end hvis der er nogle magthavere. Og det er dem vi sidder nu og skal påvirke. Nogle magthavere der, hvad hedder det nu, der langt hen af vejen sidde og øh, skal sidde og træffe beslutninger om hvor langt man må gå i sådan noget informationsovervågning.

Ulla: Ja og måske producenter.

G: Ja og producenter.

A: Jeg kan slet ikke forestille mig, at der var nogen der gad interessere sig for og manipulere med mig.

G: Jamen det er ikke det at manipulere. Det er at sammenstykke tilfældige informationer.

A: Ja, ja.

G: Og lige pludselig så bliver det. Altså for eksempel hvad hedder det.

A: Jeg er sikker på at det vil blive afsløret.

G: Jamen nej. Det er ikke det at blive afsløret. Eksemplet er jo nu, her allerede med de elektroniske patientjournaler som man begynder at indføre i Danmark, hvor man begynder og øh, øh koble forskellige registre på forskellige sygehuse sammen til et stort register.

A: Det vil da være dejligt at det endelig sker.

G: Ja ja, men nu, så kan man så forestille sig, hvad så hvor i det tilfælde hvor du så som barn har, som barn har, som ungt menneske har væltet på en øh fodboldbane og slået dit knæ. Helt tilfældigt. Og glemmer så at få det registreret det hos forsikringen fordi det gør lige lidt ondt dér. Så når du så bliver ældre hvad hedder det og begynder at arbejde og får et arbejde hvor du

skal gå meget øh, som postbud og så lige pludselig vælter som postbud på din cykel og dit knæ går i stykker. Så kan det risikere, at du ikke engang kan få din arbejdsskade-forsikring fordi du som ung kan forsikrings-selskabet gå tilbage og kigge. Jamen da havde du en skade. Du var på skadestuen.

A: Ved du hvad jeg synes det er så langt ude med sådan nogle undtagelser dér. Jeg ville finde en løsning. Tage et nyt job.....

Ulla: Jeg bliver nød til at stoppe jer nu. Det er rigtig dejlige diskussioner, men dels går det ikke at tale i munden på hinanden og dels øh har vi nu taget en åben runde. Nu begynder jeg at snævre lidt mere ind på nogle mere specifikke spørgsmål som jeg vil bede jer om at forholde jer til ret konkret. I har, der er kommet nogle forskellige udmeldinger om det materiale, som vi har øh, har brugt her til i dag, hvor hvor der er én som er sådan mere er det er meget negativt over for for teknologierne og hvor der er en anden der siger at spørgeskemaet kan være lidt forførende ikke. Øh. Er der andre sådan konkrete kommentarer til øh det materiale der er blevet udleveret?

C: Jeg har nu ikke tænkt på det sådan specielt positivt eller negativt. Men jeg opfattede det sådan relativt neutralt altså.

Ulla:

A: Okay. Jamen det var det da også, men jeg bringer bare øh terminologien der er brugt, så synes jeg at at man skal bruge den både lige for og imod ikke øh.

Ulla: Ja. Godt.

G: Men jeg kommentere på hvorfor du synes det er så positivt. Er det ikke det at man overfor et en forsamling er fuldstændig ukyndige på sådan et område her? Fremdrage så mange eksempler på ting og teknologier. Som teknologier er et positivt ord i sig selv i den her moderne verden vi lever i her. Ej det er jo ikke rigtigt. Joo, teknologi er i det moderne videnssamfund og så har det en positiv klang. Altså ting der.

A: Nej, det er bestemt ikke for alle i den her sammenhæng. Nej, men okay så men så. Så hvad hedder det oplister man så så mange teknologier, så begynder man sådan okay, så skal du da i hvert fald differentiere inden for den mængde der, det vil sige du kan ikke sige altså, der er ikke et spørgsmål der siger hvad så med dem alle sammen? Hvad synes du så med dem? Synes du så det generelt er et problem? Nej, du bliver bedt om at forholde dig til de enkelte specifik og så sker der automatisk en differentiering. Ergo er der en af dem der kommer til at fremstå som værende bedre og mere acceptabel end den anden. Altså vel at mærke øh, selvom de måske alle sammen var noget skidt. Men der sker en differentiering og der er noget der bliver bedre og du har kun de der fem kategorier at opstille på og du kommer til at at at . Jeg mener der er en positivt ladet effekt.

Ulla: Ja. Inden vi tager alle kommentarerne med. Øh skal jeg lige høre. Hvad synes I om scenarierne?

A: Jeg synes de er sådan lidt barnlige. Ja.

Ulla: På hvilken måde? Ja. Måden de er skrevet på eller beskrevet på? Eller er det.

A: Jamen jeg vil, jeg finder mig overhovedet ikke provokeret af historierne øh, jeg synes det er øh, jeg synes. Jamen jeg er jo altså meget for alt det her overvågningssystem. Men.

B: Det er skabelon agtigt. Jeg kan slet ikke forstå de undskyldninger der er for at være imod det. Det kan jeg ikke. Øhm. Ah. Jeg kan ikke forstå den angst for at registrere. Fordi altså. Jeg har oplevet samfundet på en helt anden måde. Jeg har ikke oplevet misbrug af mennesker. Jeg har tværtimod man hjælper mennesker i samfundet også hvis man oplever et eller andet negativt omkring. Og det er derfor jeg. Jeg skal have nogle skrappere øh hvad skal man sige dilemmaer for at blive provokeret. øh Ja. For at ændre min mening.

B: Du kan da vel ikke mene at vi skal være enige. Vi skal have lov til at komme med vores meninger hver især sådan har jeg opfattet det. Scenariet her. Jeg tror klart vi har forstået min mening også, men øh, men altså jeg synes det er nogle glimrende spørgsmål. Man kan altid man kan altid sidde og synes man måske ku svare på en lidt anden måde eller ikke lige helt forstod baggrunden bag. Men jeg synes generelt var det et rigtig godt spørgeskema. Og øh, jeg synes også de der scenarier er ganske udemærkede.

C: Tror du ikke scenarierne.

B: Nå jo scenarierne er også ganske udemærkede. ja ja.

D: De fik i hvert fald sat knald på refleksionerne. Ja. Helt sikkert.

Ulla: Det er ihvertfald et af formålene kan man sige.

D: Men hvor jeg hele tiden når jeg læser det her eller øh har læst om det også hele tiden tænker på hvor reel er den her terrortrussel? Hvor jeg tænker på journalistikken altså. Vor fjerde statsmagt øh der hele tiden bomber os med den der angst for terror ikke. Og det kan jeg jo ikke lade være at have med i mine tanker når jeg læser de her ting og når jeg forholder mig til de spørgsmål. Øh. Jeg synes de var fine i forhold til og få refleksionen i gang ikke.

B: Altså det jeg savner noget det det er det der altså jeg studsede meget over de der ressourcer. Nu var jeg i Skotland i sommer og så sådan et overvågningscenter. I Glasgow har man vist tre. Hvor de sidder med sådan nogle skærme på samtlige banegårde. Og det her det er også de der shopping arkader der er rundt om og parkeringsplads og sådan. Og der sad så konstant fem og fyre mand. På det jeg så. Altså døgnbemanding der så på de der skærme. Og øh så spurgte jeg dem kan I dokumentere at der virker? Kan I simpelthen dokumentere at det her det er pengene værd? I får fra, nærmest. Det ku de jo ikke. Altså det er jo kolossalt med ressourcer man man bruger på det her. Det synes jeg så ikke altså man tager for meget øh fat på i de der spørgeskema med ressource. Fordi man ved jo også at de der gammel østeuropæiske lande, de brød jo sammen under de der kontrolsystemer. Hvor til sidst hver tredje borger var involveret i at kontrollere ikke. Og øh de andre borgere. Så øh et eller andet sted er du jo altså nødt til at finde altså selvom man kan sige det. Altså jeg tror heller ikke der sidder nogen og vil os alle sammen til livs og hvis de kan finde et eller andet onskabsfuldt ved os og så videre. Det tror jeg sådan set ikke. Jeg sidder bare og tænker på kan vi blive ved at antage nye folk og hvis de skal ha, altså der skal jo sidde nogen og kigge på kameraet ellers er det jo ikke noget værd. Altså der skal jo sidde nogen og altså jeg synes altså man skal altså. Står det mål med øh og så ligger der jo også noget mistro i det. Altså som du også er inde på hvor man bygger sådan en mistro op mod hinanden ved kameraet.

A: Jeg ser det anderledes. Jeg ser det som at man bygger en beskyttelse op af individet. Og jeg føler mig rigtig godt tilpas ved at der er nogen der gider tage hånd i hanke og passe på mig. Sådan ser jeg det.

B: Uanset hvor meget man bruger på det?

A: Det må det må folk der har forstand på det ta stilling til og også.

B: Du har forstand på det.

A: Du er jo skatteyder, du betaler til det. Nej, jeg har mine områder som jeg synes

B: Ej altså Du skal da bestemme om pengene skal bruges til overvågning eller eller lægge ny asfalt på vejene altså eller et bedre....

Ulla: Vi er inde i en diskussion om fordele og ulemper nu og det er fint fordi det skal vi også.

E: Jeg vil gerne sige noget om om de her det oplæg. Jeg synes altså ikke det er eksakt nok. Jeg synes kun at det der står rigtig eksakt om Det andet det synes jeg sådan er en la la la historie. Den er ikke eksakt nok for mig. Nej. Og jeg har læst den igennem to gange for at tænke ej ej det kan I ikke mene. Altså det kun jeg ha sat en femten-årig til at læse det her. Det er ikke det er ikke eksakt nok for mig.

Ulla: Historien er for barnagtigt?

E: For barnagtig ja.

Ulla: Scenarierne er for barnagtige?

E: Ja det synes jeg. Men heldigvis så har I jo beskrevet øh alt hvad det er. Og det er lige før at jeg kunne nøjes med det. Ja.

Ulla: Så du havde ikke behøvet historierne?

E: Nej. Det behøvede jeg bestemt ikke.

Ulla: Godt, så går vi lige over til fordele og ulemper og vi er allerede godt igang med den diskussion. Øh, måske skulle vi lige prøve og tage øh nogle af de positive muligheder først. Så vil du sikkert protestere og sige jamen. Ha ha ha. Det er rigtig godt at få alle synspunkterne frem. Og der er, det glemte jeg jo at sige måske men der er ikke noget der er rigtigt og forkert. Alle holdninger har lige gyldighed her. Øh, hvad synes I er de største positive muligheder ved sikkerhedsteknologier? Altså hvilke teknologier synes I bedst om? Hvis I synes om nogle af dem og og hvorfor? Vil du sige starte?

F: Øh, fordi øh jeg synes i Danmark der har ikke terrorist. Nej. Jeg synes jeg der kommer terrorist ind i Danmark.

Ulla: Der er ikke terrorister i Danmark?

F: Ja. Jeg synes øh øh der har måske en million udlændinge i Danmark.

Ulla: Så mange tror jeg ikke der er. Hvor mange er det der er?

F: Det synes jeg. Ja. Jeg synes altså øh øh jeg har Danmark en kriminalitet en kriminalitet. Jeg synes Danmark jeg tager fra Somalia fra Kenya fra hele her i Danmark. Fra Iran og kontrollere. Iran Irak. Kontrollerer. Arab og Afrika. Jeg synes der er.

Ulla: Så det du siger der er ikke, det er i forvejen meget kontrolleret?

F: Kontrolleret ja. Ja. Øh og for eksempel fra Iran fra Irak fra Palæstina fra øh.

Ulla: Er det jeg hører dig sige er det at.

F: Fra Somalia det er stort samfund.

Ulla: Man kontrollerer en særlig gruppe. Er det det du siger?

F: Ja. Ja. Ja.

Ulla: At man ikke kontrollerer svenskere og nordmænd og amerikanere.

F: Ja ja jeg mener ja. Og at og at. Det er Europa sammen ja. Okay, så kontrollerer hele Europa ja og så USA her.

Ulla: Mmm. Men når vi så taler om sikkerhedsteknologier.

F: Bedst her i Danmark.

Ulla: Ja, men synes de har et godt formål eller synes du at de er besværlige og ikke til nogen nytte eller noget andet?

F: Nej nej nej det er det kontrollerer hele Europa ja. But first det tager ude fra Danmark. Det udland bor i Danmark. Ja iransk to og tredive og fem. København to og fem ja. Og Århus to øh. Ålborg to ja og ti mennesker fra Iran.

Ulla: Du taler om at der er ikke så mange udlændinge.

F: Nej. Jeg tager for eksempel Iran to. Fra Afghanistan to fra Irak to fra Palæstina to. Det kontrollerer arbejde med tolv teknologier og her ja.

Ulla: Jeg er ikke helt med på hvad du mener.

D: Altså du mener som deltager i det her.

F: Ja ja der er. Du forstå måske der er mennesker der kontrollerer. Kriminelle. Normalt arbejde her Teknologisk Råd her.

Ulla: Øh, jeg er ikke helt med på hvad du siger.

F: Ja. Fordi at øh jeg ikke kommer jeg synes at terrorist i Danmark. Du tager her.

Ulla: Er det bedre at inkludere? Ja. Og ta folk med ind.

F: Ja ja.

Ulla: Okay.

F: Ja. Jeg synes. I stedet for alle teknologier. Ja ja. Okay.

Ulla: Så man skal i stedet inddrage folk lidt mere?

F: Ja ja.

Ulla: Okay. Godt, så fik vi det på plads. Ja. Er der andre der har synspunkter på positive øh. Ja det har du jo. Ja.

A: Nå ja men jeg kan da give nogle konkrete eksempler, hvis man har interesse i det. Ja. . Øh et af mine børn øh blev overfaldet en gang og det blev registreret hos politiet og fotograferet på

hospitalet og alt mulig. Og så måtte jeg læse i avisen om et andet sted om et lignende overfald og så ringede vi til politiet og spurgte om om de havde tænkt på sammenhængen der fordi beskrivelsen af den måde overfaldene var var så enslydig. Nej det var, det havde de ikke. De havde nemlig ikke på det tidspunkt fået lov til at sammenkøre med registre. Og det gjorde mig enormt vred. Og alene sådan en historie det har gjort at jeg har haft det sådan selvfølgelig skal registrene sammenkøres. I dag måtte jeg køre ud på et hospital og hente nogle røntgenbilleder og en om om hvad hedder det et stykke papir hvor der stod at min svigermor skal ind og opereres. Det var blevet sendt forkert rundt man benytter gammeldags post system og ikke sammenkører hospitalets ting. De kunne med få tryk have sendt den henvisning ud til det hospital hvor hun hører til. Jeg har måtte køre København rundt for som postbud fordi de om fordi ikke lige kunne gøre det hurtigt. Så jeg håber at der hurtigst muligt kommer en masse sammenkøringer for at effektivisere arbejdsgangen bare inden for hospitalsvæsenet og det vil også gøre det hele meget nemmere.

D: Lige præcis det konkrete eksempel det kan du selv om lave accept på at det bliver samlet alt sammen.

Ulla: Så det bliver individuelle beslutninger.

D: Det gør det ja. Måske ikke lige røntgenbillederne fordi det ved jeg ikke om man kan faxe eller hvad pokker man kan med om alt det andet det kan du få samlet.

G: Jamen det har da ikke noget med sikkerhedsteknologier at gøre.

A: Nej. Men der er nogle mennesker der er i mod at man sammenkører registrer.

G: Det har noget at gøre med at hvert sygehus har sit eget system. Det har jo ikke kunne enes om det og København har måtte skrotte.

A: Jamen det er jo sammenkøring af sammenkøring af registeret ikke.

G: Det er kun det der er problemet i det altså de kan ikke rent teknologisk gøre det. De har måtte opgive det.

D: Men diskussionen går jo på om det er med vores accept eller ej. Altså.

Ulla: Men så kunne jeg godt tænke mig at spørge nu har jer der har udtrykt nogle forbeholdne holdninger til teknologierne er der nogen, skelner i mellem teknologierne? Er der nogen I anser for mere relevante end andre?

D: Ja. Altså jeg har siddet og tænkt af de seks stykker der blev øh oplæst er der et par stykker som jeg sagtens kan leve med. Ja. Altså jeg kan for eksempel sagtens leve med passiv overvågning. Øh, hvor det er sådan nogle kameraer der bare kører, hvor der ikke sidder nogen og kigger, men at det bliver båndet ikke. Det vil jeg rent personligt sagtens kunne leve med. Jeg vil også kunne leve med en scanner. Altså det har jeg heller ikke nogen problemer med.

Ulla: Men vil du kunne leve med det overalt? Eller ville der være nogle områder hvor du ikke.

D: Arh måske ikke i badeanstalten til omklædningsrum og hvor det er sådan inden for min intimsfære. Der ville jeg ikke bryde mig om det. Der var blandt andet et spørgsmål om når man køber tøj. Hvad er det sådan et. Et prøverum. Det ville jeg ikke synes var okay.

B: Der er jo ellers kommercielle muligheder i det. Ja. Ha ha ha.

D: Men alle mulige andre steder det har jeg ingen.

Ulla: Hvad med barer og offentlige kontorer?

D: Det ville ikke genere mig en hylende fis men det skulle være. Men jeg sku ha være hundrede fem og tyve tusinde procent sikker på at det ville kun blive gennemkigget i det øjeblik der var sket en eller anden form for øh kriminell aktivitet.

Ulla: Ja.

C: For så lige, prøv så lige at forstil jer. Nu det ikke fordi jeg er nogen fan af Morten Messerschmidt der var i Tivoli her den anden dag her. Og lavede et eller andet eller lavede han ikke noget. Men i sådan et tilfælde der.

D: Det er rigtigt.

C: Når sådan en mand sidder dér, hvor usympatisk manden end er, så øh, så altså så lige pludselig så kan han sidde der i et festlig lag og drikke øl og lave sådan en eller anden hilsen til en eller anden.

B: Det var oven i købet for sjov.

C: Nå undskyld for sjov. Så lige pludselig så fordi der er kamera, altså i scenariet over det hele. Jamen så den her mand, som har en, som sidder med et passivt kamera. Så vil man jo kunne finde frem til det passive kamera der bare har stået og kigget ned på ham hele den dag. Og lavede han den eller lavede han ikke den.

B: De kan jo også frikende ham. Jamen det, ja ja.

C: Men men men øh, altså.

B: Han ville jo nok være glad for at der havde været et kamera det tilfælde.

C: Jamen det ved jeg ikke. Altså, det kan være. Men tanken om at du hele tiden vil være vil, du vil aldrig nogensinde kunne stille spørgsmål tegn om hvad er det du lavede på et givent tidspunkt. Der vil altid være en et en record på dig. Det synes jeg da er totalt skræmmende.

D: Dybest set så synes jeg også det r det der er det største dilemma fordi at stadigvæk, hvem er det der skal have øh adgang til de oplysninger. Men stadigvæk så synes jeg der er nogle forhold hvor.

C: Jamen der er jo et generelt problem i forhold til alle teknologier. Det er præcis hvad altså. Det er fint nok og det er jo også det de skriver her. Jamen hvis du altid er helt sikkert 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 fange the bad guys, jamen så er det måske, så kan vi måske begynde at sige, jamen så kan det godt være. Problemet er bare at det kan du bare aldrig nogensinde være sikker på. Der vil altid være nogen som vi.

B: Man kan jo se den positive side af, uanset hvad øh, af sådan noget overvågningsteknologi hvad enten det er overvågningskamera eller de biometri, jamen det er jo at man kan opklare forbrydelse. Man kan . Det er jo den positive effekt af det.

C: Jamen det er rigtigt men altså. Hvor langt vil du så gå for at få opklaret.

B: Ja ja. Og det kan du sige. Men man kan jo så sige at hvor. Der er vel et håb om at det også virker præventivt. Jamen at hvis man ved at Jomfru Ane gade er overvåget så lader man være med at stikke folk ned. Men det tror jeg nu ikke fordi det er jo som regel ikke særlig planlagt. nej øh ha ha. Så det tror jeg altså ikke, at det vil virke særlig præventivt.

C: Hvor stor skal forbrydelsen så være? Det er jo også spørgsmålet. Altså det er jo også bare en grænse som vi kan flytte frem og tilbage. Når man først har registreret at alting er registreret og filmet på film jamen altså. Er det mord er det chok, er det indbrud, ja måske. Er det biltyveri, ja måske. Er det, hvor lang tid, er det det en marsbar nede i kiosken er øh det er det når du kysser naboens kæreste øh.

B: Det er vel ikke ulovligt. Nej nej. Ha ha ha.

C: Vi er helt enige. Det bliver registreret. Men du er stadigvæk, det er stadigvæk på det dokumenteret, der er stadigvæk nogen.

B: Jeg tvivler lidt på at politiet kan få adgang til at sidde og.

C: Det er jo ikke det der er spørgsmålet. Det er altså det er der.

A: Jamen altså vi behøver vel ikke aftale hvad der er tilladt og hvad der ikke er.

C: Jamen for lige at nævne det positive i altså for eksempel altså der er automatisk trafikkontrol som jo også har været meget diskuteret ikke. Men øh. Det gælder også overvågning og kontrol. Det er i lige så høj grad. Altså overvågning når du kører rundt. Og så får du en bøde ikke. Det er jo også overvågning. Men da synes jeg da at det er acceptabelt.

G: Det synes jeg faktisk ikke.

Ha ha ha.

B: Jamen altså. I Schweiz har man det sådan så hvis du kører ud i et kryds der er rødt ikke så bliver du klippet, så bliver du fotograferet.

G: Ja det har vi da også i Danmark mange steder.

C: Nej. Jo det har vi. Vi har vist opgivet det herhjemme.

G: I Århus der knipser de stadigvæk.

C: Gør de det? Ja okay, men i hvert fald det virker ikke så vidt jeg ved.

G: I Århus der klipser de jo stadigvæk hvis du kører overfor rødt. Du får et lille knips i hovedet hver gang du kører på alle indfaldsvejene.

C: Er det rigtigt? Ja men altså.

Ulla: Ja du ville sige noget.

C: Ja, jeg vil jo sige det at at at når teknologien først findes, så kan vi iøvrigt protestere og gøre ved alt det vil vil, men det er jo indført og det kører og vi kan lige så godt. Kan I huske dengang hvor personnumrene kom frem.

Ulla: Ja.

C: Det skulle uh registrere og vi måtte ikke. Og nu kommer der breve hvor personnummeret står oppe i ruden og jeg ved ikke hvad og banker of forsikringsselskaber og alt muligt. Vi kan lige så godt indse at det er der og det bliver der og det kommer til at køre videre. Men men , jeg er stadigvæk ikke enig i at vi skal overvåges på kryds og tværs alle steder. Fordi det er fint nok ,så længe vi gør som det skal og det gør vi jo heldigvis alle sammen. De fleste af os da i hvert fald rimelig meget ikke. Men men du kan godt se. Nu kan vi overvåge. Se jeg har jo en flok sælgere der kører rundt ikke og de kan sådan, jeg kan sidde og se hvor de kører hen ikke. Og den dag jeg har noget imod en af dem og gerne vil have ham ud af porten ikke, så kan jeg jo bare sidde og holde øje med at han lige drejer forkert et sted og så hej hvor kører du hen. Du kørte ikke, hvad laver du der. Ud af klappen med dig ikke. Altså misbruget ligger der og og og og øh den er tæt på ikke altså.

B: I gamle dage havde man jo fundet en anden årsag til at fyre ham.

C: Ja ja altså det er jo rigtig nok. Men det ændrer jo ikke noget ved, at. Det hænger jo sammen alt sammen. Nu var det jo bare et simpelt eksempel kan man sige ikke. Men vi kan jo alle sammen samle oplysninger om, at det som du sagde før. At du kan samle sammen og så kan du altså pege på noget.

A: Jeg synes da stadigvæk at det er vigtigt at skelne imellem de der forskellige. Fordi altså der har da nogen jeg helt klart vil kunne leve med og også lever med i dag altså. Bare derinde hvor vi sad i salen, der sidder nogle store skilte, hvor der står overvågning. Hvis I lige så det. Det ved jeg ikke om I så.

C: Det lagde jeg ikke mærke til.

A: Nej. Nå, der kan du bare se. Ha ha. Øh så var der nogle af dem hvor jeg har det helt fint med at det der kan jeg sagtens leve med. Hvor der er nogle af dem hvor jeg absolut over hovedet ikke kan forestille mig eller slet ikke vil have noget med at gøre.

Ulla: Kan du give et par eksempler på på begge dele? Nu har du nævnt.

A: Jeg har nævnt for eksempel den passive overvågning øhm, men med nogle gradueringer og scanning, scanning vil altså. Jeg vil være så ligeglad med om hvis jeg gik igennem Østerport station at øh jeg lige blev blokket op på en eller anden mannequin dukke og de kunne se at jeg ikke havde nogle bomber på mig og sådan noget. Det ville ikke røre mig overhovedet. Og så synes jeg faktisk den der e-call ting var rigtig smart, men den forudsætter at man selv kan vælge og sætte den til. Altså jeg synes det handler meget om det der med at øh kunne vælge ikke vælge. Men selvfølgelig i forhold til det der med scanning og passiv overvågning. Men f.eks. biometri det skal væk, få det væk.

Ulla: Det står du af på?

A: Fuldstændig. Ja, jeg synes det er grotesk.

E: Ja, når du siger det du kan vælge e-call jamen så hjælper det jo ikke for terroristerne, de vælger det jo fra så ikke.

A: Jamen jeg ser e-call som en mulighed for hvis du kører galt eller et eller andet.

E: Ja men du sagde man selv skulle kunne vælge og der var et spørgsmål om man om mak skulle kunne vælge om man ville have det eller ej.

G: Det er vel fordi du ser den her teknologi som værende noget som kan hjælpe dig i din hverdag. Jamen, jeg er sådan set mindre eller ligeglad med hvordan det xxx. Politiet skal fange terrorister og og så hvis jeg ikke. E-call lyder som en meget fin idé, hvis jeg sådan skulle.

A: Ja, men det er sådan jeg ser det.

E: Det synes jeg også når vi går over til ulykke, men nu var der så en graduering ikke, men man kunne også vælge at man selv vil have det ikke. Det vil jeg nok foretrække.

G: Det vil jeg også.

Ulla: Var der i nogle tilfælde hvor du godt kunne leve med nogle teknologier?

B: Jo, men sagtens for det bliver vi nødt til altså, ganske enkelt fordi det er jo, når det er der så bliver det brugt. Ingen tvivl om det og jeg er da enig med dig i der sagde det med det passiv overvågning altså, det ville jeg ikke have noget imod. Hvor man kan gå ind bagefter og tjekke og se. Det så man jo også i London, at man jo også kunne finde.

C: Men de, men det ændrer jo ingen ting.

B: Det forhindrer ikke at det sker, men du kan forhindre at, du kan bagefter opklare og måske finde dem der har været skyld i måske. Men altså, selvfølgelig er det er og selvfølgelig skal det være det. Der er da også masser af ting. E-call er da genialt hvis man selv kan aktivere det ikke.

A: Mmm.

B: Altså, der er da mange ting der er rigtig smarte ikke, og det og det skal vi bare leve med. Det er da helt okay.

Ulla: Hvad hvad siger du er der ingen eller flere af de her teknologier som du synes er positive?

F: Øh, for udlændinge?

Ulla: For alle. Ja.

Ulla: Både udlændinge og ikke udlændinge altså. Ja ja. Overvågning synes du det er okay.

F: Ja. Ja. Ja.

Ulla: Hvad med det der med biometri? At man skal kunne genkende sig på sin tommelfinger?

F: Ja, det er en god ide.

Ulla: Det er også en god idé?

F: Det er en god idé. Ja ja Det er fint. Ja. Godt. Både i lufthavne og.

Ulla: Alle steder?

F: Ja det ja.

Ulla: Hvad på togstationen?

F: Ja, lufthavnen først ja.

Ulla: Lufthavnen er det vigtigste?

F: Ja. Ja, det er lufthavnen.

Ulla: Ja okay, godt. Ja. Øh, Så skal jeg lige høre øh, hvem skal egentlig træffe beslutninger om øh hvilke nogle sikkerhedsteknologier vi skal have og hvor?

G: Vi skal nok ikke overlade det til sådan et voxpop panel, som vi er en del af. Nej, det er de folkevalgte i tæt samarbejde med med folk kan der kan tænke nogle lidt større tanker end som sådan almindelige mennesker, altså filosoffer og og etikere ja. Fordi der er altså der er der er behov for i sådan en sammenhæng at tænke at tænke større tanker end bare den umiddelbare effekt af hvad sådan en overvågningsteknologi kan have af betydning for mig lige nu her i min egen hverdag. Lige nu her når jeg kører i min bil eller kører mit kort igennem en maskine. Altså det her det er jo altså nogle ting der kan sådan generelt have betydning for hvordan et samfund udvikler sig. Altså så vi er helt nede der hvor hvor hvor der er generelle ting i samfundet, som som øh ja skal tænkes ind i en sammenhæng og der er der desværre ikke almindelige mennesker der kan altså kan.

C: Altså simpelthen en elitær tankegang.

G: Ja det skal. XXX

A: Virkelig kloge folk. Ha ha ha.

C: Jamen jeg synes da ikke, der kan da være mennesker der har lige så meget ret som en eller anden skvadderpande af en filosof, der er på Århus Universitet altså efter min opfattelse.

A: Ja, har siddet og gloet i en bog i tredive år. ja. Ha ha .

C: Nej nej. Jeg kan faktisk ikke se at der er nogen der er mere kvalificeret end én og egentlig kan man komme frygtelig galt afsted med at have nogen der har mere kvalificerede meninger end andr.

G: Jamen altså jeg er helt, altså det er jo så.

Ulla: Men du nævnte politikkerne, synes du politikkerne skal gøre det alene? Ene og alene eller skal de gøre det i samarbejde med.

C: Jamen man kan også kaste det ud til en folkeafstemning for min skyld altså.

B: Jamen vi skal da have en god offentlig debat i det ikke altså. Ja og så har vi jo en bred valgt folketing der afspejler befolkningen jo et eller andet sted ikke så så så . Efter en bred debat kunne det være rimeligt at politikkerne traf beslutningerne. Det er jo. Det er jo vores demokrati, det er jo hele vores basis bygger på jo.

Ulla: Du nikker, er du enig?

F: Ja. Ja. Politikere. Ja. Ja.

E: Det er jeg ikke helt. Nej, jamen jeg holder lidt med dig. Der skal være nogle specialister som sådan giver som ligesom tager specialister ind til andre ting i Folketinget, så vil jeg gerne have en runde med nogle der har forstand på det. Så vil jeg gerne have både dem der skal lave det teknologisk set og dem der har mere forstand på det end os der sidder her.

C: Altså det er aldrig gået godt hvor teknologiindustrien skal ud og.

A: Der skal lovgives.

G: Altså vi har jo i Danmark allerede et etisk råd og sådan noget. Der er en grund til at vi har sådan nogle ting. Fordi folkevalgte politikere har ikke en kina mands chance for at tænke så store tanker at med respekt.

C: Så kan de jo rådgive dem.

G: Ja. Ja formelt set vil det jo altid være politikerne der skal sidde og træffe beslutninger om det i et eller andet parlament sammenhæng, men øh men jeg vil da være meget bekymret for hvis det ville være politikere ud fra sådan en eller anden populær betragtning som sådan sad og traf beslutninger om sådan nogle ting som kan have så vidtrækkende konsekvenser for hvordan det er at være menneske i et samfund. Det synes jeg simpelthen ikke.

C: Jamen vi er jo alle sammen mennesker i et samfund. XXXXX

G: Jamen det her det er jo virkelig noget man kommer til at vedrøre alle i det øjeblik man indfører sådan nogle teknologier i sådan et i en bred forstand. Så derfor øh altså der er man i i mange årtusinder i Europa været så heldige at basere sig på folk de har kunne tænke lidt større tanker, der har været hvad hedder det formålet at sætte tingene i en sammenhæng og det er i denne her sammenhæng filosoffer og etikere. Og endnu engang det er ikke fordi jeg hverken den eller den anden.

C: Har har du også nævnt præsterne?

G: Ja nej, men altså.

C: Det skal jo være, man bliver jo nødt til at lave en debat først og der kan dine folk jo komme ind og vi kan jo alle sammen give vores besyv med i en debat som vi jo for så vidt også gør her. Som jo er en del her og så kan man sige når den debat har kørt i et stykke tid så er det jo i sidste ende selvfølgelig politikerne der træffer beslutningerne. Altså som vi jo selv har valgt.

Ulla: Ja, hvad siger du?

A: Jamen diskussionen den kommer jo til at køre i medierne.

G: Ja, og det er kvalificerende eller hvad?

D: Det er en garanti for mange spændende og...

C: Vi skal jo alle sammen give et bidrag også.

A: Det er jo lige præcis det, det er jo ikke enten eller.

C: Sevfølgelig skal vi da det.

Ulla: Ja. Hvordan tror I man kan styre udviklingen af de her teknologier? Har I nogle forslag til det? Hvordan det her skal gøres?

A: Altså hvis der er et eller andet som gør rigtig ondt, som ikke er godt så er jeg sikker på at det også kommer frem og så bliver det også fjernet igen.

C: Det er jo et massivt pres, der vil jo hele tiden altså når folk er utrygge som der jo er mange mennesker der er ikke så vil der jo hele tiden være nogle der vil opfinde og der er jo sikkert nye øh øh metoder og meninger og appellere og prøve at gøre tingene bedre og bedre.

G: Jeg tror ikke bare det er teknologien det er også politikerne der sider og ønsker sådan nogle ting her altså det er jo politikerne der har presset på at vi får de informationsovervågningssystemer vi har nu her altså. Hvor dine penge overføres bliver overvåget og bliver systematiseret og bliver tjekket altså banker skal nu selv altså alle de betalinger vi foretager skal simpelthen klassificeres efter en risikovurdering øh, velvidende, altså det ved vi ikke, det er borgere.

C: Det kan jo anmeldes hvis det er mistænkeligt.

G: Også i den almindelige terrorbekæmpelse ud over bare hvidvaskning øh altså. Når du går ned nu her og betaler på et girokort. Tidligere kunne du bare gå ned og betale på et girokort, det er slut nu, det kan du ikke længere. Nu skal du legitimere dig med billedlegitimation, fordi de skal ved siden af indtaste informationer om hvem er det der foretager denne her betaling nu her. Og det indgår i en stor database som man sidder i EUROPOL og overvåger Alle de betalinger der overgår eller foretages. Altså på tværs af.

A: Jamen det er da godt nok.

G: Ja, men jeg siger bare.

A: Jeg har da også hørt om en der der øh, blev ringet op fordi der skete nogle uregelmæssigheder på vedkommendes hævekort og det blev de opdagede så det blev misbrugt og var blevet kopieret.

Ulla: Men skal.

A: Og det var da rigtig godt.

G: Jamen det jo noget du har det kan du jo aktivt gå ned og bede din bank om at sige, altså npr der er nogen der misbruger dit hævekort eller sådan noget. Så må du godt.

A: Ja det var da dejligt.

G: Men det er det er fint det er noget du aktivt kan tilmelde dig og lave i forholdet hvis din bank siger kan du ikke lige hjælpe mig med at overvåge at der ikke kommer overtræk på den her konto nu her.

A: Det var ikke overtræk, det var misbrug. Det var så beløb der blev trukket lige så langsomt fra kontoen, det blev opdaget af banken. Det var oprigtig dejligt.

Ulla: Men kan vi og skal vi som samfund prøve på at styre udviklingen af de her teknologier? Måske også hvad producenterne gerne vil lave?

C: Ja ja, det mener jeg vi skal prøve at styre det helt klart. Bestemt bestemt. Du ser jo en radikal styring.

B: Du bliver nødt til at se på renten ik, neej. Det er ligesom at forhindre atombomben. 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 et sted hvor den ikke skulle være. Ja. Og sådan vil det også være med teknologien her.

Ulla: Så det jeg hører jer sige det er noget med at producenterne forsøger at producere og så må man træde i bremsen ind i mellem.

C: Jeg tror hvis der er et publikum, et købedygtigt publikum i forhold til politikere eller øh, flyselskaber, togselskaber, hvis der er nogen der vil købe, så er der også nogle der vil fremstille. Sådan fungerer markedet.

B: Helt sikkert helt sikkert ja.

D: Det der er vigtigt det er jo at stille spørgsmål om hvad er fordelene og hvad er ulemperne ikke.

Ulla: Mmm. Men skal.

D: Det er jo sådan en markant øh.

Ulla: Skal politikerne gå ind og lægge nogle begrænsninger på hvad man må.

G: I hvert fald i det øjeblik det er anvendt. Altså i det øjeblik det bliver flyttet fra at være at være en produktudvikling, det er jo lidt svært at begrænse hvad folk de sidder og tænker af kreative tanker og blandet nogle ting sammen i et eller andet øh baglokale i en fabriksal. Det kan man det er svært at regulere. Men i det øjeblik noget af det her teknologi kommer ud og møder den almindelige borger i det her samfund og bliver sat i anvendelse og der begynder at blive opbygget et eller andet register bagved. Jamen så synes jeg simpelthen bare at der skal

være total kontrol med hvad der foregår og hvad der bliver registreret og hvornår og hvor meget og hvem der har adgang til det. Hele vejen rundt.

C: Jeg synes også der skal en dommerkendelse til altså.

G: Men også bare at sætte det i gang altså.

C: Ja hvis man sætter det i gang skal der en dommerkendelse til.

B: Du kan bare se hvordan det var i halvtredserne og tresserne. Der hvor PET overvågede eller telefonaflyttede venstreorienterede i Danmark uden dommertilladelse. Så altså det kører jo og teknologi er der og så bliver den brugt og misbrugt. Også af lovgiverne altså også.

C: Derfor kan det jo godt være ulovligt og og...

D: Jeg synes også det er vigtigt hvem der har adgang til det ikke. Det var lige, der var lige en der sagde et eller andet med den der GPS ikke, øh, den utro hustru der lige får smidt sådan en ind i handskerummet øhm, hvor at så begynder jeg at overvåge dig og du begynder at overvåge ham og sådan noget så så så jeg synes i hvert fald at det er utrolig vigtigt også at der er meget meget meget meget stor kontrol med hvem der har adgang til det her sikkerhedsteknologi.

C: Det kan jo da ikke forhindre dig hvis det er billigt nok.

D: Nej nej , det er jeg godt klar over men jeg.

G: Det er vigtigt ikke bare at give los og bare sige jamen det er lige gyldigt. Det er meget meget vigtigt. Man kan jo altid.

C: Man kan godt sige at det er ulovligt men jeg tror det.

Ulla: Vi øh ja skal desværre til at runde af nu. Vi har kun små fem minutter til tilbage til at. Vi har jo næsten kun skimmet overfladen ikke. Vi er ikke rigtigt eller der var mange flere ting vi godt kunne diskutere, men jeg kunne godt tænke mig at vi sluttede af med en disciplineret runde ha ha ha ha. Hvor hver især kommer lige ganske ganske kort siger om øh, øh om dagens møde har ændret jeres holdning til sikkerhedsteknologier og i må også godt lige sige hvis der er et eller andet i har på hjertet som I ikke synes I har fået ud endnu. Så skal vi køre den her vej igen? Nej, vi kører den her vej.

E: Det kan vi godt. Jeg har ikke fået noget nyt og det har jeg også skrevet og øh jeg tror min holdning er nøjagtig den samme som den var inden.

Ulla: Ja. Og hvis du skulle summe det op?

E: Jamen jeg synes det har været spændende nok at være med i dag, hvis det er sådan noget du gerne vil vide.

Ulla: Nej det var det egentlig ikke, det var din holdning til teknologierne.

E: Den er at jeg er bange for for for meget overvågning og jeg holder meget på privatlivets fred.

Ulla: Godt, jamen tak skal du ha.

B: Jamen jeg har fuldstændig samme holdning som dig også bekymret over det og og jeg har ikke ændret holdning i løbet af dagen. Det har været meget interessant diskussion altså jeg synes det har været okay, meget fint, men jeg er også nervøs for det.

G: Ja. Ja, jeg må sige at jeg har faktisk, jeg arbejder i en branche hvor vi faktisk bruger sådan noget her og bruger meget tid på det og det fylder meget i mit arbejde det her og da jeg kom her faktisk var mere positiv over for det end jeg er nu her. Jeg faktisk blevet meget opmærksom på de der potentielle, altså når man lige pludselig bryder om og alle kan sidde med sin egen lille ting her og begynder at lægge tingene sammen og kan se at se det store altså

hvad betyder det her for samfundet og hvad betyder det for individet i det samfund vi lever i og hvad betyder det også for den samfundsudvikling at altså bare den mistro der er i samfundet hvis man begynder at udvikle og bruge sådan nogle teknologier. Den den bekymring om og sammenhæng af de forskellige teknologier den havde jeg faktisk ikke før. Hvor jeg sad meget og kiggede på mit eget lille snævre område øh, hvor der altså ingeniør set er mange fordele. Og jeg sidder hver dag på vegne af et stort foretagende og argumenterer for det overfor politikere og alle mulige andre og synes det er temmelig godt i den sammenhæng, men tingene sat sammen i det store billede, så begynder jeg at blive meget bekymret især når jeg og det er derfor at jeg siger at når man så ser det i en sammenhæng her hvor det har, mener jeg fået en karakter af teknologi forelskelse hvor hvor det bærer karakter af at nu har vi det og vi har en 11. september og vi skal have et eller andet og vi har noget valgt det er bare et spørgsmål om hvordan vi skal prioritere det . Hvilken rækkefølge er det vi skal implementere de her ting i samfundet, fordi der er ingen tvivl om at politikerne de er pisse bange for at ende i 11. september og de er villige til at bruge hvad som helst for at undgå det og det synes jeg er bekymrende.

Ulla: Tak. Ha ha.

F: Jeg synes øh, forstå, teknologisk råd først og bagefter måske jeg håber at at arbejde. Arbejde med sådan noget, ja.

Ulla: Har du ændret holdning fra du kom til du nu.

F: Ja jaja.

Ulla: Er du blevet mere positiv over for teknologierne?

F: Ja, ja.

Ulla: Okay. Godt tak.

F: Og tak for det her.

Ulla: Ja, selv tak. Ja. Det er din tur.

A: Ta lige ham først, jeg skal lige tænke over det. Ja.

Ulla: Er der nogen der vil ja. Værsgod.

C: Jeg vil godt. Altså jeg har ikke ændret øh ret meget holdning, altså jeg har stadigvæk, min største bekymring er at man bruger en helvedes masse penge på det her teknologi og øh bygger en masse op til ingen verdens nytte fordi det giver falsk tryghed og så videre og man kan sige at teknologien i sig selv tror jeg ikke spiller så afgørende en rolle for man kan jo se at i tredivernes Tyskland, det var jo ganske udmærket overvågning og ganske udmærket registre øh, der kunne man faktisk finde ud af det uden teknologien og øh det var jo ikke så sjovt at skrive, den gang man skrev i registrene og fik at vide at det blev så brugt senere ikke altså så jeg tror sgu ikke at det har så meget med teknologi at gøre. Jeg er bare bange for at man i de her år også lidt som du siger også under indtryk af nogle terroraktioner og sådan noget kan bruge en helvedes masse penge og sætte en helvedes masse folk i sving med det uden at man egentlig vinder ret meget med det. Hvorimod hvis man fik mere ud af at rette nogle flere kryds ud så færre folk kørte galt så og så videre altså.

Ulla: Tak. Ja, så er det.

A: Ja, jeg er helt klar. Ja. Øhm, altså jeg ,de film og og og hvad skal vi sige referater, historier hvor der er blevet brugt overvågning og hvor man har kunne bruge det med henblik på at opklare øh forbrydelser og måske fange terrorister der er sluppet fra stedet det det gør at jeg er meget positiv indstillet over for teknologi øh hvis bare man kan stoppe øh drabet på en lille gruppe mennesker ved hjælp af en masse teknologi så vil jeg være lykkelig. Tænk hvis der var noget nogen jeg kendte eller nogen i min familie. Men så er der en ting jeg vil tilføje til alt det der og det var faktisk da du sagde og det er at øh der er noget specielt ved Danmark. Nogen steder i Danmark og det er der er nogle steder hvor man taler sammen og hvor man holder øje med hinanden. Og det skal vi på en eller anden måde have med. Fordi det tror jeg også er forebyggende mod terrorister og det er da ikke, det står ingen steder. Jeg mener ikke at der er kommunikation nok i Danmark.

Ulla: Nej.

B: Det har du fuldstændig ret i. Det er den mest effektive måde.

A: Og så ville man ikke blive frist, hvis man hvis man snakkede med hinanden så ville man ikke blive fristet til at misbruge en GPS'er til at fyre en medarbejder. Så ville man sige det lige ud til ham, at du bliver fyret fordi at du har gjort et eller andet. Whatever ikke, men hvis man snakkede mere sammen, så lige det aspekt synes jeg skal på en eller anden måde, det skal hives ind i det hele ikke. Ja, og så kunne man jo måske også få nogle flere diskussioner der gik lidt dybere og få manet nogle spørgsmål i jorden eller få nogle andre ting fremhævet som man så fik undersøgt til gengæld fordi man siger jeg er smadder bange for det her vil I ikke godt undersøge det så det ikke bliver misbrugt? Det, men det vil jo kræve at vi har tid og råderum til at kommunikere.

Ulla: Det var en ny pointe i slutrunden. Tak for det.

D: Ja. Ja, og da kan jeg da kun tilslutte mig dig og sige at det var den vigtigste pointe. Lige præcis det der med og gå i debat med hinanden og tage os af hinanden og holde samtaler og så videre. Øh, men ændring af synspunkt altså jeg har jo fra starten været meget bekymret omkring sikkerhedsteknologi øh og mit synspunkt har ikke ændret sig. Jeg synes stadigvæk at jeg kan se dilemmaet imellem at i nogle tilfælde er det hensigtsmæssigt med den der overvågning blandt andet øh et lille barn der bliver slået ihjel, der var jo blandt Mia der som man fandt via mobiltelefonen. Der synes jeg at jo det har sin berettigelse. Men stadig synes jeg det er utrolig vigtigt hvem det er der får adgangen til og hvordan man får adgang til de oplysninger der nu engang ligger i forhold til overvågning.

Ulla: Tak. Det var okay. Nu er vi færdige. Du blev færdig? Ha hahaa. Jamen så vil jeg gerne sige tak for jeres gode bidrag og g øh ivrige debat villighed eller hvad det hedder ja, det har været en rigtig fornøjelse. Skal vi derind igen? Ja.

Annex 6 Frequency tables

6.1 Frequencies

q1sex

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	14	51,9	51,9	51,9
	female	13	48,1	48,1	100,0
	Total	27	100,0	100,0	

q2age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	21	1	3,7	3,7	3,7
	25	1	3,7	3,7	7,4
	28	1	3,7	3,7	11,1
	30	2	7,4	7,4	18,5
	31	1	3,7	3,7	22,2
	34	2	7,4	7,4	29,6
	35	1	3,7	3,7	33,3
	36	1	3,7	3,7	37,0
	42	1	3,7	3,7	40,7
	47	3	11,1	11,1	51,9
	49	1	3,7	3,7	55,6
	50	2	7,4	7,4	63,0
	53	1	3,7	3,7	66,7
	57	1	3,7	3,7	70,4
	59	2	7,4	7,4	77,8
	60	1	3,7	3,7	81,5
	61	2	7,4	7,4	88,9
	65	1	3,7	3,7	92,6
	69	1	3,7	3,7	96,3
	71	1	3,7	3,7	100,0
Total		27	100,0	100,0	

q3household Persons in household ink self

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 1	6	22,2	22,2	22,2
2	13	48,1	48,1	70,4
3	3	11,1	11,1	81,5
4 or more	5	18,5	18,5	100,0
Total	27	100,0	100,0	

q4childre

	Frequency	Percent	Valid	Cumulative Percent
Valid yes	20	74,1	74,1	74,1
no	7	25,9	25,9	100,0
Total	27	100,0	100,0	

q5childhome1 No children

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	11	40,7	40,7	40,7
yes	16	59,3	59,3	100,0
Total	27	100,0	100,0	

q5childhome2 14 or younger

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	74,1	74,1	74,1
yes	7	25,9	25,9	100,0
Total	27	100,0	100,0	

q5childhome3 15 or older

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	23	85,2	85,2	85,2
yes	4	14,8	14,8	100,0
Total	27	100,0	100,0	

q6edu

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 2	1	3,7	3,7	3,7
3	3	11,1	11,1	14,8
4	2	7,4	7,4	22,2
5	4	14,8	14,8	37,0
6	8	29,6	29,6	66,7
7	9	33,3	33,3	100,0
Total	27	100,0	100,0	

q7occupstring

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Civil engineer	4	14,8	14,8	14,8
Designer	1	3,7	3,7	18,5
Graphic designer	1	3,7	3,7	22,2
Graphic designer, manager	1	3,7	3,7	25,9
Hospital porter	1	3,7	3,7	29,6
Journalist	1	3,7	3,7	33,3
Laborant	1	3,7	3,7	37,0
Manager of marketing	1	3,7	3,7	40,7
Nurse	1	3,7	3,7	44,4
Pensionist	1	3,7	3,7	48,1
Planner	1	3,7	3,7	51,9
Political consultant	1	3,7	3,7	55,6
Project assistant	1	3,7	3,7	59,3
Research consultant	1	3,7	3,7	63,0
Self employed	1	3,7	3,7	66,7
Student	1	3,7	3,7	70,4
Student, Interviewer	1	3,7	3,7	74,1
Teacher	3	11,1	11,1	85,2
Technician	1	3,7	3,7	88,9
Translator, Student	1	3,7	3,7	92,6
Unemployed	1	3,7	3,7	96,3
Warder	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q8district

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Metro	22	81,5	81,5	81,5
Provincial town	4	14,8	14,8	96,3
Rural	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q9phone

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	21	77,8	77,8	77,8
at least once a week	5	18,5	18,5	96,3
less than once a month	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q10email

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	18	66,7	66,7	66,7
at least once a week	8	29,6	29,6	96,3
at least once a month	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q11internet

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	22	81,5	81,5	81,5
at least once a week	4	14,8	14,8	96,3
at least once a month	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q12publictransport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	2	7,4	7,4	7,4
at least once a week	6	22,2	22,2	29,6
at least once a month	6	22,2	22,2	51,9
less than once a month	11	40,7	40,7	92,6
never	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q13plane

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid more than 5 times a year	5	18,5	18,5	18,5
3-5 times a year	3	11,1	11,1	29,6
1-2 times a year	12	44,4	44,4	74,1
less than 1 time a year	6	22,2	22,2	96,3
never	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q14car

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid at least once a day	14	51,9	51,9	51,9
at least once a week	3	11,1	11,1	63,0
less than once a month	7	25,9	25,9	88,9
never	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q15general The security of society is absolutely dependent on the development and use of new security technologies

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	7,4	7,4	7,4
partly agree	12	44,4	44,4	51,9
neither agree nor disagree	4	14,8	14,8	66,7
partly disagree	6	22,2	22,2	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	3	11,1	11,1	11,1
partly agree	13	48,1	48,1	59,3
neither agree nor disagree	5	18,5	18,5	77,8
partly disagree	4	14,8	14,8	92,6
completely disagree	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	7,4	7,4	7,4
partly agree	9	33,3	33,3	40,7
neither agree nor disagree	2	7,4	7,4	48,1
partly disagree	8	29,6	29,6	77,8
completely disagree	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q18general When security technology is available, we might just as well make use of it

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	7,4	7,4	7,4
partly agree	10	37,0	37,0	44,4
neither agree nor disagree	1	3,7	3,7	48,1
partly disagree	8	29,6	29,6	77,8
completely disagree	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q19general Privacy should not be violated without reasonable suspicion of criminal intent

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	9	33,3	33,3	33,3
partly agree	10	37,0	37,0	70,4
neither agree nor disagree	3	11,1	11,1	81,5
partly disagree	2	7,4	7,4	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	7	25,9	25,9	25,9
partly agree	12	44,4	44,4	70,4
neither agree nor disagree	3	11,1	11,1	81,5
partly disagree	2	7,4	7,4	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q21general New security technologies are likely to be abused by governmental agencies

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	4	14,8	14,8	14,8
partly agree	11	40,7	40,7	55,6
neither agree nor disagree	6	22,2	22,2	77,8
partly disagree	3	11,1	11,1	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q22general New security technologies are likely to be abused by criminals

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	10	37,0	37,0	37,0
partly agree	14	51,9	51,9	88,9
neither agree nor disagree	1	3,7	3,7	92,6
partly disagree	1	3,7	3,7	96,3
completely disagree	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q23biom1 Facial characteristics

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	63,0	63,0	63,0
yes	10	37,0	37,0	100,0
Total	27	100,0	100,0	

q23biom2 Fingerprints

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	14	51,9	51,9	51,9
yes	13	48,1	48,1	100,0
Total	27	100,0	100,0	

q23biom3 Iris recognition

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	13	48,1	48,1	48,1
yes	14	51,9	51,9	100,0
Total	27	100,0	100,0	

q23biom4 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	15	55,6	55,6	55,6
yes	12	44,4	44,4	100,0
Total	27	100,0	100,0	

q23biom5 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q24biom1 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	70,4	70,4	70,4
	yes	8	29,6	29,6	100,0
	Total	27	100,0	100,0	

q24biom2 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	40,7	40,7	40,7
	yes	16	59,3	59,3	100,0
	Total	27	100,0	100,0	

q24biom3 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	81,5	81,5	81,5
	yes	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q24biom4 Border

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	48,1	48,1	48,1
	yes	14	51,9	51,9	100,0
	Total	27	100,0	100,0	

q24biom5 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	74,1	74,1	74,1
	yes	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

q24biom6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	74,1	74,1	74,1
	yes	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

q24biom7 Other private service

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	96,3	96,3	96,3
	yes	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q24biom8 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q24biom9 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	25,9	25,9	25,9
	partly agree	4	14,8	14,8	40,7
	neither agree nor disagree	4	14,8	14,8	55,6
	partly disagree	3	11,1	11,1	66,7
	completely disagree	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	25,9	25,9	25,9
	partly agree	6	22,2	22,2	48,1
	neither agree nor disagree	5	18,5	18,5	66,7
	partly disagree	4	14,8	14,8	81,5
	completely disagree	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q27visual1 Store

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	33,3	33,3	33,3
	yes	18	66,7	66,7	100,0
	Total	27	100,0	100,0	

q27visual2 Dressing room

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	85,2	85,2	85,2
	yes	4	14,8	14,8	100,0
	Total	27	100,0	100,0	

q27visual3 Central bus and train station

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	2	7,4	7,4	7,4
	yes	25	92,6	92,6	100,0
	Total	27	100,0	100,0	

q27visual4 Bank

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	2	7,4	7,4	7,4
	yes	25	92,6	92,6	100,0
	Total	27	100,0	100,0	

q27visual5 Airport

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	27	100,0	100,0	100,0

q27visual6 Stadium and crowded

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	25,9	25,9	25,9
	yes	20	74,1	74,1	100,0
	Total	27	100,0	100,0	

q27visual7 All public

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	74,1	74,1	74,1
yes	7	25,9	25,9	100,0
Total	27	100,0	100,0	

q27visual8 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q27visual9 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q28visual How do you feel about the number of CCTV cameras in public spaces in general?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid there should be more	11	40,7	47,8	47,8
the number is appropriate	11	40,7	47,8	95,7
there should be less	1	3,7	4,3	100,0
Total	23	85,2	100,0	
Missing d.k.	4	14,8		
Total	27	100,0		

q29visual1 School

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	24	88,9	88,9	88,9
yes	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q29visual2 Central bus and train station

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	74,1	74,1	74,1
yes	7	25,9	25,9	100,0
Total	27	100,0	100,0	

q29visual3 Airport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	2	7,4	7,4	7,4
yes	25	92,6	92,6	100,0
Total	27	100,0	100,0	

q29visual4 Shopping mall

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	25	92,6	92,6	92,6
yes	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q29visual5 Public buildings

	Frequency	Percent
Missing 99	27	100,0

q29visual6 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	25	92,6	92,6	92,6
yes	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q29visual7 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q30visual1 Reveal everything

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	24	88,9	88,9	88,9
yes	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q30visual2 Mannequin projection

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	9	33,3	33,3	33,3
yes	18	66,7	66,7	100,0
Total	27	100,0	100,0	

q30visual3 Body heat, sweat & heart rate

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q30visual4 Metal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	18,5	18,5	18,5
	yes	22	81,5	81,5	100,0
	Total	27	100,0	100,0	

q30visual5 Luggage x-ray

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	1	3,7	3,7	3,7
	yes	26	96,3	96,3	100,0
	Total	27	100,0	100,0	

q30visual6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q30visual7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q31visual CCTV surveillance makes me feel more secure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	3,7	3,7	3,7
	partly agree	12	44,4	44,4	48,1
	neither agree nor disagree	9	33,3	33,3	81,5
	partly disagree	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q32visual CCTV surveillance infringes my privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid partly agree	12	44,4	44,4	44,4
neither agree nor disagree	7	25,9	25,9	70,4
partly disagree	4	14,8	14,8	85,2
completely disagree	4	14,8	14,8	100,0
Total	27	100,0	100,0	

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	9	33,3	33,3	33,3
partly agree	11	40,7	40,7	74,1
neither agree nor disagree	6	22,2	22,2	96,3
partly disagree	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q34local1 Terrorists and criminals w court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	6	22,2	22,2	22,2
yes	21	77,8	77,8	100,0
Total	27	100,0	100,0	

q34local2 Any w/o court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	23	85,2	85,2	85,2
yes	4	14,8	14,8	100,0
Total	27	100,0	100,0	

q34local3 Emergency

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	25,9	25,9	25,9
yes	20	74,1	74,1	100,0
Total	27	100,0	100,0	

q34local4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	96,3	96,3	96,3
	yes	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q34local5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q35local1 Terrorists and criminals w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	14,8	16,0	16,0
	yes	21	77,8	84,0	100,0
	Total	25	92,6	100,0	
Missing	System	2	7,4		
Total		27	100,0		

q35local2 Any w/o court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	88,9	88,9	88,9
	yes	3	11,1	11,1	100,0
	Total	27	100,0	100,0	

q35local3 Stolen vehicles

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	29,6	29,6	29,6
	yes	19	70,4	70,4	100,0
	Total	27	100,0	100,0	

q35local4 Speeding

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	63,0	63,0	63,0
	yes	10	37,0	37,0	100,0
	Total	27	100,0	100,0	

q35local5 Automatic accident reporting

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	7	25,9	25,9	25,9
yes	20	74,1	74,1	100,0
Total	27	100,0	100,0	

q35local6 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	26	96,3	96,3	96,3
yes	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q35local7 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q36local Should eCall automatically be installed in all new cars?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	7	25,9	25,9	25,9
yes but possible to deactivate	5	18,5	18,5	44,4
no, optional	14	51,9	51,9	96,3
no, never	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q37local The possibility of locating all mobile phones is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	12	44,4	44,4	44,4
partly agree	5	18,5	18,5	63,0
partly disagree	4	14,8	14,8	77,8
completely disagree	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	11	40,7	40,7	40,7
partly agree	11	40,7	40,7	81,5
neither agree nor disagree	2	7,4	7,4	88,9
partly disagree	1	3,7	3,7	92,6
completely disagree	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q39local The possibility of locating all cars is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	10	37,0	37,0	37,0
partly agree	9	33,3	33,3	70,4
neither agree nor disagree	1	3,7	3,7	74,1
partly disagree	3	11,1	11,1	85,2
completely disagree	4	14,8	14,8	100,0
Total	27	100,0	100,0	

40local The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	7	25,9	25,9	25,9
partly agree	10	37,0	37,0	63,0
neither agree nor disagree	3	11,1	11,1	74,1
partly disagree	6	22,2	22,2	96,3
completely disagree	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q41data1 Prevention of terrorism

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	63,0	63,0	63,0
yes	10	37,0	37,0	100,0
Total	27	100,0	100,0	

q41data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	22,2	22,2	22,2
	yes	21	77,8	77,8	100,0
	Total	27	100,0	100,0	

q41data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	74,1	74,1	74,1
	yes	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

q41data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	18,5	18,5	18,5
	yes	22	81,5	81,5	100,0
	Total	27	100,0	100,0	

q41data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q41data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	88,9	88,9	88,9
	yes	3	11,1	11,1	100,0
	Total	27	100,0	100,0	

q41data7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	96,3	96,3	96,3
	yes	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q42data1 Prevention of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	74,1	74,1	74,1
	yes	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

q42data2 Investigation of terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	25,9	25,9	25,9
	yes	20	74,1	74,1	100,0
	Total	27	100,0	100,0	

q42data3 Prevention of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	77,8	77,8	77,8
	yes	6	22,2	22,2	100,0
	Total	27	100,0	100,0	

q42data4 Investigation of crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	6	22,2	22,2	22,2
	yes	21	77,8	77,8	100,0
	Total	27	100,0	100,0	

q42data5 Commercial

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q42data6 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	85,2	85,2	85,2
	yes	4	14,8	14,8	100,0
	Total	27	100,0	100,0	

q42data7 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	26	96,3	96,3	96,3
yes	1	3,7	3,7	100,0
Total	27	100,0	100,0	

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	2	7,4	7,4	7,4
partly agree	9	33,3	33,3	40,7
neither agree nor disagree	1	3,7	3,7	44,4
partly disagree	6	22,2	22,2	66,7
completely disagree	9	33,3	33,3	100,0
Total	27	100,0	100,0	

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	12	44,4	44,4	44,4
partly agree	3	11,1	11,1	55,6
neither agree nor disagree	3	11,1	11,1	66,7
partly disagree	7	25,9	25,9	92,6
completely disagree	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q45data Scanning of and combining data from different databases containing personal information is privacy infringing

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	12	44,4	44,4	44,4
partly agree	5	18,5	18,5	63,0
neither agree nor disagree	4	14,8	14,8	77,8
partly disagree	5	18,5	18,5	96,3
completely disagree	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q46data Scanning of and combining data from different databases is a good tool for police to prevent terror

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	4	14,8	14,8	14,8
partly agree	9	33,3	33,3	48,1
neither agree nor disagree	4	14,8	14,8	63,0
partly disagree	4	14,8	14,8	77,8
completely disagree	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q47data Databases being used for something else than the original purpose is a serious privacy problem

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	14	51,9	51,9	51,9
partly agree	7	25,9	25,9	77,8
neither agree nor disagree	3	11,1	11,1	88,9
partly disagree	1	3,7	3,7	92,6
completely disagree	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q48wire1 Prevention and investigation of terrorism w court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	5	18,5	18,5	18,5
yes	22	81,5	81,5	100,0
Total	27	100,0	100,0	

q48wire2 Prevention and investigation of terrorism w/o court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	20	74,1	74,1	74,1
yes	7	25,9	25,9	100,0
Total	27	100,0	100,0	

q48wire3 Prevention and investigation of crime w court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	4	14,8	14,8	14,8
yes	23	85,2	85,2	100,0
Total	27	100,0	100,0	

q48wire4 Prevention and investigation of crime w/o court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	22	81,5	81,5	81,5
yes	5	18,5	18,5	100,0
Total	27	100,0	100,0	

q48wire5 Commercial

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q48wire6 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	25	92,6	92,6	92,6
yes	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q48wire7 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	27	100,0	100,0	100,0

q49wire What methods of eavesdropping is acceptable?

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid all communication lines	2	7,4	7,7	7,7
persons that suspect is expected to contact	6	22,2	23,1	30,8
suspects	16	59,3	61,5	92,3
totally unacceptable	2	7,4	7,7	100,0
Total	26	96,3	100,0	
Missing d.k.	1	3,7		
Total	27	100,0		

q50wire Eavesdropping is a good tool for police investigation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	40,7	40,7	40,7
	partly agree	8	29,6	29,6	70,4
	neither agree nor disagree	4	14,8	14,8	85,2
	partly disagree	3	11,1	11,1	96,3
	completely disagree	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q51wire Eavesdropping is a serious violation of privacy

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	10	37,0	37,0	37,0
	partly agree	6	22,2	22,2	59,3
	neither agree nor disagree	4	14,8	14,8	74,1
	partly disagree	6	22,2	22,2	96,3
	completely disagree	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q52protect1 Anonymous calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	77,8	77,8	77,8
	yes	6	22,2	22,2	100,0
	Total	27	100,0	100,0	

q52protect2 Encryption programmes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	48,1	48,1	48,1
	yes	14	51,9	51,9	100,0
	Total	27	100,0	100,0	

q52protect3 Identity management

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	70,4	70,4	70,4
	yes	8	29,6	29,6	100,0
	Total	27	100,0	100,0	

q52protect4 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	26	96,3	96,3	96,3
yes	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q52protect5 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	17	63,0	63,0	63,0
yes	10	37,0	37,0	100,0
Total	27	100,0	100,0	

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	10	37,0	37,0	37,0
partly agree	7	25,9	25,9	63,0
neither agree nor disagree	4	14,8	14,8	77,8
partly disagree	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid partly agree	9	33,3	33,3	33,3
neither agree nor disagree	6	22,2	22,2	55,6
partly disagree	9	33,3	33,3	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q55dilem1 Accept registration of travel and fingerprints

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	23	85,2	85,2	85,2
yes	4	14,8	14,8	100,0
Total	27	100,0	100,0	

q55dilem2 Accept only if template

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	88,9	88,9	88,9
	yes	3	11,1	11,1	100,0
	Total	27	100,0	100,0	

q55dilem3 Accept only if deleted

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	81,5	81,5	81,5
	yes	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q55dilem4 Accept only if not exclusive

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	55,6	55,6	55,6
	yes	12	44,4	44,4	100,0
	Total	27	100,0	100,0	

q55dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	48,1	48,1	48,1
	yes	14	51,9	51,9	100,0
	Total	27	100,0	100,0	

q55dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	96,3	96,3	96,3
	yes	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q56dilem1 Accept database and biometrics

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q56dilem2 Accept naked machine

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q56dilem3 Accept sweat, body heat and heart rate scanning

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q56dilem4 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q56dilem5 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	92,6	92,6	92,6
	yes	2	7,4	7,4	100,0
	Total	27	100,0	100,0	

q57dilem1 Accept all consequences

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	92,6	92,6	92,6
	yes	2	7,4	7,4	100,0
	Total	27	100,0	100,0	

q57dilem2 Accept only low rate of false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	70,4	70,4	70,4
	yes	8	29,6	29,6	100,0
	Total	27	100,0	100,0	

q57dilem3 Accept only no false positives

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q57dilem4 Accept only in exposed places

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	63,0	63,0	63,0
	yes	10	37,0	37,0	100,0
	Total	27	100,0	100,0	

q57dilem5 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	74,1	74,1	74,1
	yes	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

q57dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q58dilem1 Accept all access for counter terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	81,5	81,5	81,5
	yes	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q58dilem2 Accept only if anonymous and w court order

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	37,0	37,0	37,0
	yes	17	63,0	63,0	100,0
	Total	27	100,0	100,0	

q58dilem3 Never

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	81,5	81,5	81,5
	yes	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q58dilem4 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q59dilem1 Accept locate car to prevent crime or terrorism

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	55,6	55,6	55,6
	yes	12	44,4	44,4	100,0
	Total	27	100,0	100,0	

q59dilem2 Accept speeding tickets

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	92,6	92,6	92,6
	yes	2	7,4	7,4	100,0
	Total	27	100,0	100,0	

q59dilem3 Accept register all movements

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	88,9	88,9	88,9
	yes	3	11,1	11,1	100,0
	Total	27	100,0	100,0	

q59dilem4 Accept only accidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q59dilem5 Accept only if voluntary

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	40,7	40,7	40,7
	yes	16	59,3	59,3	100,0
	Total	27	100,0	100,0	

q59dilem6 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	27	100,0	100,0	100,0

q60dilem1 Accept calling cards

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q60dilem2 Accept encryption

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	40,7	40,7	40,7
	yes	16	59,3	59,3	100,0
	Total	27	100,0	100,0	

q60dilem3 Accept Internet anonymity - bomb

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	66,7	66,7	66,7
	yes	9	33,3	33,3	100,0
	Total	27	100,0	100,0	

q60dilem4 Accept Internet anonymity - child pornography

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	81,5	81,5	81,5
	yes	5	18,5	18,5	100,0
	Total	27	100,0	100,0	

q60dilem5 Never

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	77,8	77,8	77,8
yes	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q60dilem6 d.k.

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	23	85,2	85,2	85,2
yes	4	14,8	14,8	100,0
Total	27	100,0	100,0	

q61dilem1 Accept exclusion of refusers from public service

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	21	77,8	77,8	77,8
yes	6	22,2	22,2	100,0
Total	27	100,0	100,0	

q61dilem2 Accept exclusion of unable from public service

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	24	88,9	88,9	88,9
yes	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q61dilem3 Accept refusers are impended when public transport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	19	70,4	70,4	70,4
yes	8	29,6	29,6	100,0
Total	27	100,0	100,0	

q61dilem4 Accept unable are impended when public transport

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid no	24	88,9	88,9	88,9
yes	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q61dilem5 Accept no consequences for refusers

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q61dilem6 Accept no consequences for unabled

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	59,3	59,3	59,3
	yes	11	40,7	40,7	100,0
	Total	27	100,0	100,0	

q61dilem7 d.k.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	85,2	85,2	85,2
	yes	4	14,8	14,8	100,0
	Total	27	100,0	100,0	

62demo Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	13	48,1	48,1	48,1
	partly agree	9	33,3	33,3	81,5
	neither agree nor disagree	1	3,7	3,7	85,2
	partly disagree	4	14,8	14,8	100,0
	Total	27	100,0	100,0	

q63demo The subject of security and privacy is so complicated that it makes no sense to include the general public in discussions of this issue

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	partly agree	3	11,1	11,1	11,1
	neither agree nor disagree	5	18,5	18,5	29,6
	partly disagree	6	22,2	22,2	51,9
	completely disagree	13	48,1	48,1	100,0
	Total	27	100,0	100,0	

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	13	48,1	48,1	48,1
partly agree	12	44,4	44,4	92,6
neither agree nor disagree	1	3,7	3,7	96,3
completely disagree	1	3,7	3,7	100,0
Total	27	100,0	100,0	

q65demo It is important that private companies involved in producing security technologies are also entitled to be heard when important decisions on security and privacy are made

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	4	14,8	14,8	14,8
partly agree	11	40,7	40,7	55,6
neither agree nor disagree	5	18,5	18,5	74,1
partly disagree	4	14,8	14,8	88,9
completely disagree	3	11,1	11,1	100,0
Total	27	100,0	100,0	

q66demo In relation to significant decisions on the use of security technologies, it is imperative that alternative solutions are elucidated and included in the debate

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid completely agree	20	74,1	74,1	74,1
partly agree	5	18,5	18,5	92,6
neither agree nor disagree	2	7,4	7,4	100,0
Total	27	100,0	100,0	

q67suggest Collection of personal data from unsuspecting individuals must be anonymous until identification is authorized by court order

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid high importance	20	74,1	80,0	80,0
some importance	3	11,1	12,0	92,0
not important at all	2	7,4	8,0	100,0
Total	25	92,6	100,0	
Missing d.k.	2	7,4		
Total	27	100,0		

q68suggest Only authorized personnel can have access to collected personal data

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	25	92,6	92,6	92,6
	some importance	2	7,4	7,4	100,0
	Total	27	100,0	100,0	

q69suggest Prior to implementing, new security technologies must be checked for privacy impact

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	19	70,4	70,4	70,4
	some importance	7	25,9	25,9	96,3
	little importance	1	3,7	3,7	100,0
	Total	27	100,0	100,0	

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	12	44,4	48,0	48,0
	some importance	6	22,2	24,0	72,0
	little importance	5	18,5	20,0	92,0
	not important at all	2	7,4	8,0	100,0
	Total	25	92,6	100,0	
Missing	d.k.	2	7,4		
Total		27	100,0		

q71end Have you changed your attitude towards security technologies in general in the course of completing this questionnaire?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes, more positive	1	3,7	4,0	4,0
	yes, more worried	6	22,2	24,0	28,0
	no	18	66,7	72,0	100,0
	Total	25	92,6	100,0	
Missing	d.k.	2	7,4		
Total		27	100,0		

eduISCED97

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid lower secondary level of education	1	3,7	3,7	3,7
upper secondary level of education	5	18,5	18,5	22,2
first stage of tertiary education	21	77,8	77,8	100,0
Total	27	100,0	100,0	

eduISCED97binary Tertiary

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Shorter than tertiary	6	22,2	22,2	22,2
Tertiary	21	77,8	77,8	100,0
Total	27	100,0	100,0	

AgeBinary Age over and under 50

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid 18-49	15	55,6	55,6	55,6
50+	12	44,4	44,4	100,0
Total	27	100,0	100,0	

PhoneBinary Daily

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Less	6	22,2	22,2	22,2
Daily	21	77,8	77,8	100,0
Total	27	100,0	100,0	

EmailBinary Daily

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Less	9	33,3	33,3	33,3
Daily	18	66,7	66,7	100,0
Total	27	100,0	100,0	

InternetBinary Daily

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Less	5	18,5	18,5	18,5
Daily	22	81,5	81,5	100,0
Total	27	100,0	100,0	

PublicBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	25	92,6	92,6	92,6
	Daily	2	7,4	7,4	100,0
	Total	27	100,0	100,0	

CarBinary Daily

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	13	48,1	48,1	48,1
	Daily	14	51,9	51,9	100,0
	Total	27	100,0	100,0	

PlaneBinary Less than once a year

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 times a year or more	20	74,1	74,1	74,1
	Less than 1 time a year	7	25,9	25,9	100,0
	Total	27	100,0	100,0	

PublicBinary2 Weekly

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	19	70,4	70,4	70,4
	at least once a week	8	29,6	29,6	100,0
	Total	27	100,0	100,0	

CarBinary2 Weekly

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	10	37,0	37,0	37,0
	at least once a week	17	63,0	63,0	100,0
	Total	27	100,0	100,0	

6.2 Cross tables

Crosstabs

15general The security of society is absolutely dependent on the development and use of new security technologies * q1sex Crosstabulation

				q1sex		Total
				male	female	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	1	1	2	
		% within q1sex	7,1%	7,7%	7,4%	
	partly agree	Count	7	5	12	
		% within q1sex	50,0%	38,5%	44,4%	
	neither agree nor disagree	Count	1	3	4	
		% within q1sex	7,1%	23,1%	14,8%	
	partly disagree	Count	2	4	6	
		% within q1sex	14,3%	30,8%	22,2%	
	completely disagree	Count	3	0	3	
		% within q1sex	21,4%	,0%	11,1%	
Total	Count	14	13	27		
	% within q1sex	100,0%	100,0%	100,0%		

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q1sex Crosstabulation

				q1sex		Total
				male	female	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	0	3	3	
		% within q1sex	,0%	23,1%	11,1%	
	partly agree	Count	8	5	13	
		% within q1sex	57,1%	38,5%	48,1%	
	neither agree nor disagree	Count	2	3	5	
		% within q1sex	14,3%	23,1%	18,5%	
	partly disagree	Count	4	0	4	
		% within q1sex	28,6%	,0%	14,8%	
	completely disagree	Count	0	2	2	
		% within q1sex	,0%	15,4%	7,4%	
Total	Count	14	13	27		
	% within q1sex	100,0%	100,0%	100,0%		

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q1sex Crosstabulation

			q1sex		Total
			male	female	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	0	2	2
		% within q1sex	,0%	15,4%	7,4%
	partly agree	Count	4	5	9
		% within q1sex	28,6%	38,5%	33,3%
	neither agree nor disagree	Count	2	0	2
		% within q1sex	14,3%	,0%	7,4%
	partly disagree	Count	5	3	8
		% within q1sex	35,7%	23,1%	29,6%
	completely disagree	Count	3	3	6
		% within q1sex	21,4%	23,1%	22,2%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

q18general When security technology is available, we might just as well make use of it * q1sex Crosstabulation

			q1sex		Total
			male	female	
q18general When security technology is available, we might just as well make use of it	completely agree	Count	0	2	2
		% within q1sex	,0%	15,4%	7,4%
	partly agree	Count	5	5	10
		% within q1sex	35,7%	38,5%	37,0%
	neither agree nor disagree	Count	0	1	1
		% within q1sex	,0%	7,7%	3,7%
	partly disagree	Count	5	3	8
		% within q1sex	35,7%	23,1%	29,6%
	completely disagree	Count	4	2	6
		% within q1sex	28,6%	15,4%	22,2%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * q1sex Crosstabulation

			q1sex		Total
			male	female	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	3	6	9
		% within q1sex	21,4%	46,2%	33,3%
	partly agree	Count	7	3	10
		% within q1sex	50,0%	23,1%	37,0%
	neither agree nor disagree	Count	2	1	3
		% within q1sex	14,3%	7,7%	11,1%
	partly disagree	Count	2	0	2
		% within q1sex	14,3%	,0%	7,4%
	completely disagree	Count	0	3	3
		% within q1sex	,0%	23,1%	11,1%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q1sex Crosstabulation

			q1sex		Total
			male	female	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	4	3	7
		% within q1sex	28,6%	23,1%	25,9%
	partly agree	Count	6	6	12
		% within q1sex	42,9%	46,2%	44,4%
	neither agree nor disagree	Count	2	1	3
		% within q1sex	14,3%	7,7%	11,1%
	partly disagree	Count	2	0	2
		% within q1sex	14,3%	,0%	7,4%
	completely disagree	Count	0	3	3
		% within q1sex	,0%	23,1%	11,1%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q1sex Crosstabulation

			q1sex		Total
			male	female	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	1	3	4
		% within q1sex	7,1%	23,1%	14,8%
	partly agree	Count	8	3	11
		% within q1sex	57,1%	23,1%	40,7%
	neither agree nor disagree	Count	3	3	6
		% within q1sex	21,4%	23,1%	22,2%
	partly disagree	Count	1	2	3
		% within q1sex	7,1%	15,4%	11,1%
	completely disagree	Count	1	2	3
		% within q1sex	7,1%	15,4%	11,1%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q1sex Crosstabulation

			q1sex		Total
			male	female	
q22general New security technologies are likely to be abused by criminals	completely agree	Count	7	3	10
		% within q1sex	50,0%	23,1%	37,0%
	partly agree	Count	6	8	14
		% within q1sex	42,9%	61,5%	51,9%
	neither agree nor disagree	Count	0	1	1
		% within q1sex	,0%	7,7%	3,7%
	partly disagree	Count	1	0	1
		% within q1sex	7,1%	,0%	3,7%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	7,7%	3,7%
Total		Count	14	13	27
		% within q1sex	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	1	1	2
		% within AgeBinary Age over and under 50	6,7%	8,3%	7,4%
	partly agree	Count	7	5	12
		% within AgeBinary Age over and under 50	46,7%	41,7%	44,4%
	neither agree nor disagree	Count	2	2	4
	% within AgeBinary Age over and under 50	13,3%	16,7%	14,8%	
	partly disagree	Count	4	2	6
		% within AgeBinary Age over and under 50	26,7%	16,7%	22,2%
	completely disagree	Count	1	2	3
		% within AgeBinary Age over and under 50	6,7%	16,7%	11,1%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	2	1	3
		% within AgeBinary Age over and under 50	13,3%	8,3%	11,1%
	partly agree	Count	8	5	13
		% within AgeBinary Age over and under 50	53,3%	41,7%	48,1%
	neither agree nor disagree	Count	0	5	5
	% within AgeBinary Age over and under 50	,0%	41,7%	18,5%	
	partly disagree	Count	4	0	4
		% within AgeBinary Age over and under 50	26,7%	,0%	14,8%
	completely disagree	Count	1	1	2
		% within AgeBinary Age over and under 50	6,7%	8,3%	7,4%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count % within AgeBinary Age over and under 50	0 ,0%	2 16,7%	2 7,4%
	partly agree	Count % within AgeBinary Age over and under 50	5 33,3%	4 33,3%	9 33,3%
	neither agree nor disagree	Count % within AgeBinary Age over and under 50	2 13,3%	0 ,0%	2 7,4%
	partly disagree	Count % within AgeBinary Age over and under 50	5 33,3%	3 25,0%	8 29,6%
	completely disagree	Count % within AgeBinary Age over and under 50	3 20,0%	3 25,0%	6 22,2%
Total		Count % within AgeBinary Age over and under 50	15 100,0%	12 100,0%	27 100,0%

q18general When security technology is available, we might just as well make use of it * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q18general When security technology is available, we might just as well make use of it	completely agree	Count % within AgeBinary Age over and under 50	1 6,7%	1 8,3%	2 7,4%
	partly agree	Count % within AgeBinary Age over and under 50	5 33,3%	5 41,7%	10 37,0%
	neither agree nor disagree	Count % within AgeBinary Age over and under 50	1 6,7%	0 ,0%	1 3,7%
	partly disagree	Count % within AgeBinary Age over and under 50	3 20,0%	5 41,7%	8 29,6%
	completely disagree	Count % within AgeBinary Age over and under 50	5 33,3%	1 8,3%	6 22,2%
Total		Count % within AgeBinary Age over and under 50	15 100,0%	12 100,0%	27 100,0%

19general Privacy should not be violated without reasonable suspicion of criminal intent * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	5	4	9
		% within AgeBinary Age over and under 50	33,3%	33,3%	33,3%
	partly agree	Count	6	4	10
		% within AgeBinary Age over and under 50	40,0%	33,3%	37,0%
	neither agree nor disagree	Count	3	0	3
	% within AgeBinary Age over and under 50	20,0%	,0%	11,1%	
	partly disagree	Count	1	1	2
		% within AgeBinary Age over and under 50	6,7%	8,3%	7,4%
	completely disagree	Count	0	3	3
		% within AgeBinary Age over and under 50	,0%	25,0%	11,1%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

20general It is uncomfortable to be under surveillance, even though you have no criminal intent * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	4	3	7
		% within AgeBinary Age over and under 50	26,7%	25,0%	25,9%
	partly agree	Count	7	5	12
		% within AgeBinary Age over and under 50	46,7%	41,7%	44,4%
	neither agree nor disagree	Count	2	1	3
	% within AgeBinary Age over and under 50	13,3%	8,3%	11,1%	
	partly disagree	Count	1	1	2
		% within AgeBinary Age over and under 50	6,7%	8,3%	7,4%
	completely disagree	Count	1	2	3
		% within AgeBinary Age over and under 50	6,7%	16,7%	11,1%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	2	4
		% within AgeBinary Age over and under 50	13,3%	16,7%	14,8%
	partly agree	Count	7	4	11
		% within AgeBinary Age over and under 50	46,7%	33,3%	40,7%
	neither agree nor disagree	Count	3	3	6
	% within AgeBinary Age over and under 50	20,0%	25,0%	22,2%	
	partly disagree	Count	2	1	3
		% within AgeBinary Age over and under 50	13,3%	8,3%	11,1%
	completely disagree	Count	1	2	3
		% within AgeBinary Age over and under 50	6,7%	16,7%	11,1%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		Total
			18-49	50+	
q22general New security technologies are likely to be abused by criminals	completely agree	Count	6	4	10
		% within AgeBinary Age over and under 50	40,0%	33,3%	37,0%
	partly agree	Count	8	6	14
		% within AgeBinary Age over and under 50	53,3%	50,0%	51,9%
	neither agree nor disagree	Count	0	1	1
	% within AgeBinary Age over and under 50	,0%	8,3%	3,7%	
	partly disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	6,7%	,0%	3,7%
	completely disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	8,3%	3,7%
Total		Count	15	12	27
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count % within eduISCED97binary Tertiary	1 16,7%	1 4,8%	2 7,4%
	partly agree	Count % within eduISCED97binary Tertiary	2 33,3%	10 47,6%	12 44,4%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	0 ,0%	4 19,0%	4 14,8%
	partly disagree	Count % within eduISCED97binary Tertiary	3 50,0%	3 14,3%	6 22,2%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 14,3%	3 11,1%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror *edulSCED97binary Tertiary Crosstabulation

			edulSCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count % within edulSCED97binary Tertiary	1 16,7%	2 9,5%	3 11,1%
	partly agree	Count % within edulSCED97binary Tertiary	3 50,0%	10 47,6%	13 48,1%
	neither agree nor disagree	Count % within edulSCED97binary Tertiary	1 16,7%	4 19,0%	5 18,5%
	partly disagree	Count % within edulSCED97binary Tertiary	1 16,7%	3 14,3%	4 14,8%
	completely disagree	Count % within edulSCED97binary Tertiary	0 ,0%	2 9,5%	2 7,4%
Total	Count % within edulSCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count % within eduISCED97binary Tertiary	0 0,0%	2 9,5%	2 7,4%
	partly agree	Count % within eduISCED97binary Tertiary	3 50,0%	6 28,6%	9 33,3%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	0 0,0%	2 9,5%	2 7,4%
	partly disagree	Count % within eduISCED97binary Tertiary	2 33,3%	6 28,6%	8 29,6%
	completely disagree	Count % within eduISCED97binary Tertiary	1 16,7%	5 23,8%	6 22,2%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

**q18general When security technology is available, we might just as well make use of it *
eduISCED97binary Tertiary Crosstabulation**

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q18general When security technology is available, we might just as well make use of it	completely agree	Count % within eduISCED97binary Tertiary	0 0,0%	2 9,5%	2 7,4%
	partly agree	Count % within eduISCED97binary Tertiary	2 33,3%	8 38,1%	10 37,0%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	1 16,7%	0 ,0%	1 3,7%
	partly disagree	Count % within eduISCED97binary Tertiary	2 33,3%	6 28,6%	8 29,6%
	completely disagree	Count % within eduISCED97binary Tertiary	1 16,7%	5 23,8%	6 22,2%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

**q19general Privacy should not be violated without reasonable suspicion of criminal intent *
 eduISCED97binary Tertiary Crosstabulation**

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count % within eduISCED97binary Tertiary	4 66,7%	5 23,8%	9 33,3%
	partly agree	Count % within eduISCED97binary Tertiary	0 ,0%	10 47,6%	10 37,0%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	1 16,7%	2 9,5%	3 11,1%
	partly disagree	Count % within eduISCED97binary Tertiary	1 16,7%	1 4,8%	2 7,4%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 14,3%	3 11,1%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

**q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
 eduISCED97binary Tertiary Crosstabulation**

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count % within eduISCED97binary Tertiary	3 50,0%	4 19,0%	7 25,9%
	partly agree	Count % within eduISCED97binary Tertiary	2 33,3%	10 47,6%	12 44,4%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	1 16,7%	2 9,5%	3 11,1%
	partly disagree	Count % within eduISCED97binary Tertiary	0 ,0%	2 9,5%	2 7,4%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 14,3%	3 11,1%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

**q21general New security technologies are likely to be abused by governmental agencies *
eduISCED97binary Tertiary Crosstabulation**

			eduISCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count % within eduISCED97binary Tertiary	0 ,0%	4 19,0%	4 14,8%
	partly agree	Count % within eduISCED97binary Tertiary	4 66,7%	7 33,3%	11 40,7%
	neither agree nor disagree	Count % within eduISCED97binary Tertiary	1 16,7%	5 23,8%	6 22,2%
	partly disagree	Count % within eduISCED97binary Tertiary	1 16,7%	2 9,5%	3 11,1%
	completely disagree	Count % within eduISCED97binary Tertiary	0 ,0%	3 14,3%	3 11,1%
Total	Count % within eduISCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%	

q22general New security technologies are likely to be abused by criminals * eduLSCED97binary Tertiary Crosstabulation

			eduLSCED97binary Tertiary		Total
			Shorter than tertiary	Tertiary	
q22general New security technologies are likely to be abused by criminals	completely agree	Count % within eduLSCED97binary Tertiary	1 16,7%	9 42,9%	10 37,0%
	partly agree	Count % within eduLSCED97binary Tertiary	4 66,7%	10 47,6%	14 51,9%
	neither agree nor disagree	Count % within eduLSCED97binary Tertiary	0 ,0%	1 4,8%	1 3,7%
	partly disagree	Count % within eduLSCED97binary Tertiary	1 16,7%	0 ,0%	1 3,7%
	completely disagree	Count % within eduLSCED97binary Tertiary	0 ,0%	1 4,8%	1 3,7%
Total		Count % within eduLSCED97binary Tertiary	6 100,0%	21 100,0%	27 100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * q4children Crosstabulation

			q4children		Total
			yes	no	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count % within q4children	2 10,0%	0 ,0%	2 7,4%
	partly agree	Count % within q4children	9 45,0%	3 42,9%	12 44,4%
	neither agree nor disagree	Count % within q4children	2 10,0%	2 28,6%	4 14,8%
	partly disagree	Count % within q4children	5 25,0%	1 14,3%	6 22,2%
	completely disagree	Count % within q4children	2 10,0%	1 14,3%	3 11,1%
Total		Count % within q4children	20 100,0%	7 100,0%	27 100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q4children Crosstabulation

			q4children		Total
			yes	no	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count	1	2	3
		% within q4children	5,0%	28,6%	11,1%
	partly agree	Count	11	2	13
		% within q4children	55,0%	28,6%	48,1%
	neither agree nor disagree	Count	4	1	5
		% within q4children	20,0%	14,3%	18,5%
	partly disagree	Count	3	1	4
		% within q4children	15,0%	14,3%	14,8%
	completely disagree	Count	1	1	2
		% within q4children	5,0%	14,3%	7,4%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

7general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q4children Crosstabulation

			q4children		Total
			yes	no	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	2	0	2
		% within q4children	10,0%	,0%	7,4%
	partly agree	Count	7	2	9
		% within q4children	35,0%	28,6%	33,3%
	neither agree nor disagree	Count	2	0	2
		% within q4children	10,0%	,0%	7,4%
	partly disagree	Count	5	3	8
		% within q4children	25,0%	42,9%	29,6%
	completely disagree	Count	4	2	6
		% within q4children	20,0%	28,6%	22,2%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

**q18general When security technology is available, we might just as well make use of it * q4children
Crosstabulation**

			q4children		Total
			yes	no	
q18general When security technology is available, we might just as well make use of it	completely agree	Count	1	1	2
		% within q4children	5,0%	14,3%	7,4%
	partly agree	Count	10	0	10
		% within q4children	50,0%	,0%	37,0%
	neither agree nor disagree	Count	0	1	1
		% within q4children	,0%	14,3%	3,7%
	partly disagree	Count	5	3	8
		% within q4children	25,0%	42,9%	29,6%
	completely disagree	Count	4	2	6
		% within q4children	20,0%	28,6%	22,2%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

**q19general Privacy should not be violated without reasonable suspicion of criminal intent * q4children
Crosstabulation**

			q4children		Total
			yes	no	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	7	2	9
		% within q4children	35,0%	28,6%	33,3%
	partly agree	Count	6	4	10
		% within q4children	30,0%	57,1%	37,0%
	neither agree nor disagree	Count	2	1	3
		% within q4children	10,0%	14,3%	11,1%
	partly disagree	Count	2	0	2
		% within q4children	10,0%	,0%	7,4%
	completely disagree	Count	3	0	3
		% within q4children	15,0%	,0%	11,1%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

**q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
q4children Crosstabulation**

			q4children		Total
			yes	no	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	4	3	7
		% within q4children	20,0%	42,9%	25,9%
	partly agree	Count	11	1	12
		% within q4children	55,0%	14,3%	44,4%
	neither agree nor disagree	Count	2	1	3
		% within q4children	10,0%	14,3%	11,1%
	partly disagree	Count	1	1	2
		% within q4children	5,0%	14,3%	7,4%
	completely disagree	Count	2	1	3
		% within q4children	10,0%	14,3%	11,1%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

**q21general New security technologies are likely to be abused by governmental agencies * q4children
Crosstabulation**

			q4children		Total
			yes	no	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	2	4
		% within q4children	10,0%	28,6%	14,8%
	partly agree	Count	10	1	11
		% within q4children	50,0%	14,3%	40,7%
	neither agree nor disagree	Count	5	1	6
		% within q4children	25,0%	14,3%	22,2%
	partly disagree	Count	1	2	3
		% within q4children	5,0%	28,6%	11,1%
	completely disagree	Count	2	1	3
		% within q4children	10,0%	14,3%	11,1%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

**q22general New security technologies are likely to be abused by criminals * q4children
Crosstabulation**

			q4children		Total
			yes	no	
q22general New security technologies are likely to be abused by criminals	completely agree	Count	9	1	10
		% within q4children	45,0%	14,3%	37,0%
	partly agree	Count	9	5	14
		% within q4children	45,0%	71,4%	51,9%
	neither agree nor disagree	Count	0	1	1
		% within q4children	,0%	14,3%	3,7%
	partly disagree	Count	1	0	1
		% within q4children	5,0%	,0%	3,7%
	completely disagree	Count	1	0	1
		% within q4children	5,0%	,0%	3,7%
Total		Count	20	7	27
		% within q4children	100,0%	100,0%	100,0%

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	1	1	2
		% within q5childhome1 No children	9,1%	6,3%	7,4%
	partly agree	Count	6	6	12
		% within q5childhome1 No children	54,5%	37,5%	44,4%
	neither agree nor disagree	Count	0	4	4
		% within q5childhome1 No children	,0%	25,0%	14,8%
	partly disagree	Count	4	2	6
		% within q5childhome1 No children	36,4%	12,5%	22,2%
	completely disagree	Count	0	3	3
		% within q5childhome1 No children	,0%	18,8%	11,1%
Total		Count	11	16	27
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror	completely agree	Count % within q5childhome1 No children	1 9,1%	2 12,5%	3 11,1%
	partly agree	Count % within q5childhome1 No children	6 54,5%	7 43,8%	13 48,1%
	neither agree nor disagree	Count % within q5childhome1 No children	0 ,0%	5 31,3%	5 18,5%
	partly disagree	Count % within q5childhome1 No children	3 27,3%	1 6,3%	4 14,8%
	completely disagree	Count % within q5childhome1 No children	1 9,1%	1 6,3%	2 7,4%
Total		Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count % within q5childhome1 No children	2 18,2%	0 ,0%	2 7,4%
	partly agree	Count % within q5childhome1 No children	2 18,2%	7 43,8%	9 33,3%
	neither agree nor disagree	Count % within q5childhome1 No children	2 18,2%	0 ,0%	2 7,4%
	partly disagree	Count % within q5childhome1 No children	3 27,3%	5 31,3%	8 29,6%
	completely disagree	Count % within q5childhome1 No children	2 18,2%	4 25,0%	6 22,2%
Total		Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%

18general When security technology is available, we might just as well make use of it * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q18general When security technology is available, we might just as well make use of it	completely agree	Count % within q5childhome1 No children	1 9,1%	1 6,3%	2 7,4%
	partly agree	Count % within q5childhome1 No children	5 45,5%	5 31,3%	10 37,0%
	neither agree nor disagree	Count % within q5childhome1 No children	0 ,0%	1 6,3%	1 3,7%
	partly disagree	Count % within q5childhome1 No children	1 9,1%	7 43,8%	8 29,6%
	completely disagree	Count % within q5childhome1 No children	4 36,4%	2 12,5%	6 22,2%
Total		Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%

19general Privacy should not be violated without reasonable suspicion of criminal intent * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count % within q5childhome1 No children	4 36,4%	5 31,3%	9 33,3%
	partly agree	Count % within q5childhome1 No children	3 27,3%	7 43,8%	10 37,0%
	neither agree nor disagree	Count % within q5childhome1 No children	1 9,1%	2 12,5%	3 11,1%
	partly disagree	Count % within q5childhome1 No children	1 9,1%	1 6,3%	2 7,4%
	completely disagree	Count % within q5childhome1 No children	2 18,2%	1 6,3%	3 11,1%
Total		Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%

**q20general It is uncomfortable to be under surveillance, even though you have no criminal intent *
q5childhome1 No children Crosstabulation**

			q5childhome1 No children		Total
			no	yes	
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count % within q5childhome1 No children	1 9,1%	6 37,5%	7 25,9%
	partly agree	Count % within q5childhome1 No children	7 63,6%	5 31,3%	12 44,4%
	neither agree nor disagree	Count % within q5childhome1 No children	1 9,1%	2 12,5%	3 11,1%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	2 12,5%	2 7,4%
	completely disagree	Count % within q5childhome1 No children	2 18,2%	1 6,3%	3 11,1%
Total	Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%	

q21general New security technologies are likely to be abused by governmental agencies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count % within q5childhome1 No children	1 9,1%	3 18,8%	4 14,8%
	partly agree	Count % within q5childhome1 No children	6 54,5%	5 31,3%	11 40,7%
	neither agree nor disagree	Count % within q5childhome1 No children	2 18,2%	4 25,0%	6 22,2%
	partly disagree	Count % within q5childhome1 No children	0 ,0%	3 18,8%	3 11,1%
	completely disagree	Count % within q5childhome1 No children	2 18,2%	1 6,3%	3 11,1%
Total	Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%	

q22general New security technologies are likely to be abused by criminals * q5childhome1 No children Crosstabulation

			q5childhome1 No children		Total
			no	yes	
q22general New security technologies are likely to be abused by criminals	completely agree	Count % within q5childhome1 No children	5 45,5%	5 31,3%	10 37,0%
	partly agree	Count % within q5childhome1 No children	4 36,4%	10 62,5%	14 51,9%
	neither agree nor disagree	Count % within q5childhome1 No children	0 ,0%	1 6,3%	1 3,7%
	partly disagree	Count % within q5childhome1 No children	1 9,1%	0 ,0%	1 3,7%
	completely disagree	Count % within q5childhome1 No children	1 9,1%	0 ,0%	1 3,7%
Total		Count % within q5childhome1 No children	11 100,0%	16 100,0%	27 100,0%

Crosstabs

q24biom2 Airport * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		Total
			1-2 times a year or more	Less than 1 time a year	
q24biom2 Airport	no	Count % within PlaneBinary Less than once a year	8 40,0%	3 42,9%	11 40,7%
	yes	Count % within PlaneBinary Less than once a year	12 60,0%	4 57,1%	16 59,3%
Total		Count % within PlaneBinary Less than once a year	20 100,0%	7 100,0%	27 100,0%

Crosstabs

q56dilem1 Accept database and biometrics * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		Total
			1-2 times a year or more	Less than 1 time a year	
q56dilem1 Accept database and biometrics	no	Count	11	7	18
		% within PlaneBinary Less than once a year	55,0%	100,0%	66,7%
	yes	Count	9	0	9
		% within PlaneBinary Less than once a year	45,0%	,0%	33,3%
Total		Count	20	7	27
		% within PlaneBinary Less than once a year	100,0%	100,0%	100,0%

Crosstabs**q24biom5 Central bus and train station * PublicBinary Daily Crosstabulation**

			PublicBinary Daily		Total
			Less	Daily	
q24biom5 Central bus and train station	no	Count	18	2	20
		% within PublicBinary Daily	72,0%	100,0%	74,1%
	yes	Count	7	0	7
		% within PublicBinary Daily	28,0%	,0%	25,9%
Total		Count	25	2	27
		% within PublicBinary Daily	100,0%	100,0%	100,0%

Crosstabs**q55dilem1 Accept registration of travel and fingerprints * PublicBinary Daily Crosstabulation**

			PublicBinary Daily		Total
			Less	Daily	
q55dilem1 Accept registration of travel and fingerprints	no	Count	21	2	23
		% within PublicBinary Daily	84,0%	100,0%	85,2%
	yes	Count	4	0	4
		% within PublicBinary Daily	16,0%	,0%	14,8%
Total		Count	25	2	27
		% within PublicBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q35local1 Terrorists and criminals w court order * CarBinary Daily Crosstabulation

				CarBinary Daily		Total
				Less	Daily	
q35local1 Terrorists and criminals w court order	no	Count		0	4	4
		% within CarBinary Daily		,0%	28,6%	16,0%
	yes	Count		11	10	21
		% within CarBinary Daily		100,0%	71,4%	84,0%
Total	Count			11	14	25
	% within CarBinary Daily			100,0%	100,0%	100,0%

q35local2 Any w/o court order * CarBinary Daily Crosstabulation

				CarBinary Daily		Total
				Less	Daily	
q35local2 Any w/o court order	no	Count		13	11	24
		% within CarBinary Daily		100,0%	78,6%	88,9%
	yes	Count		0	3	3
		% within CarBinary Daily		,0%	21,4%	11,1%
Total	Count			13	14	27
	% within CarBinary Daily			100,0%	100,0%	100,0%

q35local3 Stolen vehicles * CarBinary Daily Crosstabulation

				CarBinary Daily		Total
				Less	Daily	
q35local3 Stolen vehicles	no	Count		4	4	8
		% within CarBinary Daily		30,8%	28,6%	29,6%
	yes	Count		9	10	19
		% within CarBinary Daily		69,2%	71,4%	70,4%
Total	Count			13	14	27
	% within CarBinary Daily			100,0%	100,0%	100,0%

q35local4 Speeding * CarBinary Daily Crosstabulation

				CarBinary Daily		Total
				Less	Daily	
q35local4 Speeding	no	Count		9	8	17
		% within CarBinary Daily		69,2%	57,1%	63,0%
	yes	Count		4	6	10
		% within CarBinary Daily		30,8%	42,9%	37,0%
Total	Count			13	14	27
	% within CarBinary Daily			100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q35local5 Automatic accident reporting	no	Count	5	2	7
		% within CarBinary Daily	38,5%	14,3%	25,9%
	yes	Count	8	12	20
		% within CarBinary Daily	61,5%	85,7%	74,1%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q36local Should eCall automatically be installed in all new cars? * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q36local Should eCall automatically be installed in all new cars?	yes	Count	3	4	7
		% within CarBinary Daily	23,1%	28,6%	25,9%
	yes but possible to deactivate	Count	3	2	5
		% within CarBinary Daily	23,1%	14,3%	18,5%
	no, optional	Count	6	8	14
		% within CarBinary Daily	46,2%	57,1%	51,9%
	no, never	Count	1	0	1
		% within CarBinary Daily	7,7%	,0%	3,7%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q39local The possibility of locating all cars is privacy infringing * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	3	7	10
		% within CarBinary Daily	23,1%	50,0%	37,0%
	partly agree	Count	5	4	9
		% within CarBinary Daily	38,5%	28,6%	33,3%
	neither agree nor disagree	Count	1	0	1
		% within CarBinary Daily	7,7%	,0%	3,7%
	partly disagree	Count	2	1	3
		% within CarBinary Daily	15,4%	7,1%	11,1%
	completely disagree	Count	2	2	4
		% within CarBinary Daily	15,4%	14,3%	14,8%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	8	7	15
		% within CarBinary Daily	61,5%	50,0%	55,6%
	yes	Count	5	7	12
		% within CarBinary Daily	38,5%	50,0%	44,4%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem2 Accept speeding tickets	no	Count	11	14	25
		% within CarBinary Daily	84,6%	100,0%	92,6%
	yes	Count	2	0	2
		% within CarBinary Daily	15,4%	,0%	7,4%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem3 Accept register all movements	no	Count	12	12	24
		% within CarBinary Daily	92,3%	85,7%	88,9%
	yes	Count	1	2	3
		% within CarBinary Daily	7,7%	14,3%	11,1%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem4 Accept only accidents	no	Count	7	9	16
		% within CarBinary Daily	53,8%	64,3%	59,3%
	yes	Count	6	5	11
		% within CarBinary Daily	46,2%	35,7%	40,7%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem5 Accept only if voluntary	no	Count	6	5	11
		% within CarBinary Daily	46,2%	35,7%	40,7%
	yes	Count	7	9	16
		% within CarBinary Daily	53,8%	64,3%	59,3%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary Daily Crosstabulation

			CarBinary Daily		Total
			Less	Daily	
q59dilem6 d.k.	no	Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%
Total		Count	13	14	27
		% within CarBinary Daily	100,0%	100,0%	100,0%

Crosstabs**q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * PhoneBinary Daily Crosstabulation**

				PhoneBinary Daily		Total
				Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	0	2	2	
		% within PhoneBinary Daily	,0%	9,5%	7,4%	
	partly agree	Count	3	6	9	
		% within PhoneBinary Daily	50,0%	28,6%	33,3%	
	neither agree nor disagree	Count	1	0	1	
	% within PhoneBinary Daily	16,7%	,0%	3,7%		
	partly disagree	Count	1	5	6	
		% within PhoneBinary Daily	16,7%	23,8%	22,2%	
	completely disagree	Count	1	8	9	
		% within PhoneBinary Daily	16,7%	38,1%	33,3%	
Total		Count	6	21	27	
		% within PhoneBinary Daily	100,0%	100,0%	100,0%	

q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	1	1	2
		% within EmailBinary Daily	11,1%	5,6%	7,4%
	partly agree	Count	1	8	9
		% within EmailBinary Daily	11,1%	44,4%	33,3%
	neither agree nor disagree	Count	0	1	1
	% within EmailBinary Daily	,0%	5,6%	3,7%	
	partly disagree	Count	5	1	6
		% within EmailBinary Daily	55,6%	5,6%	22,2%
	completely disagree	Count	2	7	9
		% within EmailBinary Daily	22,2%	38,9%	33,3%
Total		Count	9	18	27
		% within EmailBinary Daily	100,0%	100,0%	100,0%

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary	completely agree	Count	0	2	2
		% within InternetBinary Daily	,0%	9,1%	7,4%
	partly agree	Count	0	9	9
		% within InternetBinary Daily	,0%	40,9%	33,3%
	neither agree nor disagree	Count	0	1	1
	% within InternetBinary Daily	,0%	4,5%	3,7%	
	partly disagree	Count	3	3	6
		% within InternetBinary Daily	60,0%	13,6%	22,2%
	completely disagree	Count	2	7	9
		% within InternetBinary Daily	40,0%	31,8%	33,3%
Total		Count	5	22	27
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within PhoneBinary Daily	3 50,0%	9 42,9%	12 44,4%
	partly agree	Count % within PhoneBinary Daily	0 ,0%	3 14,3%	3 11,1%
	neither agree nor disagree	Count % within PhoneBinary Daily	0 ,0%	3 14,3%	3 11,1%
	partly disagree	Count % within PhoneBinary Daily	2 33,3%	5 23,8%	7 25,9%
	completely disagree	Count % within PhoneBinary Daily	1 16,7%	1 4,8%	2 7,4%
Total	Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%	

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within EmailBinary Daily	4 44,4%	8 44,4%	12 44,4%
	partly agree	Count % within EmailBinary Daily	1 11,1%	2 11,1%	3 11,1%
	neither agree nor disagree	Count % within EmailBinary Daily	2 22,2%	1 5,6%	3 11,1%
	partly disagree	Count % within EmailBinary Daily	1 11,1%	6 33,3%	7 25,9%
	completely disagree	Count % within EmailBinary Daily	1 11,1%	1 5,6%	2 7,4%
Total	Count % within EmailBinary Daily	9 100,0%	18 100,0%	27 100,0%	

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count % within InternetBinary Daily	2 40,0%	10 45,5%	12 44,4%
	partly agree	Count % within InternetBinary Daily	1 20,0%	2 9,1%	3 11,1%
	neither agree nor disagree	Count % within InternetBinary Daily	1 20,0%	2 9,1%	3 11,1%
	partly disagree	Count % within InternetBinary Daily	1 20,0%	6 27,3%	7 25,9%
	completely disagree	Count % within InternetBinary Daily	0 ,0%	2 9,1%	2 7,4%
Total	Count % within InternetBinary Daily	5 100,0%	22 100,0%	27 100,0%	

Crosstabs

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count % within PhoneBinary Daily	1 16,7%	11 52,4%	12 44,4%
	partly agree	Count % within PhoneBinary Daily	3 50,0%	2 9,5%	5 18,5%
	neither agree nor disagree	Count % within PhoneBinary Daily	1 16,7%	3 14,3%	4 14,8%
	partly disagree	Count % within PhoneBinary Daily	1 16,7%	4 19,0%	5 18,5%
	completely disagree	Count % within PhoneBinary Daily	0 ,0%	1 4,8%	1 3,7%
Total	Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%	

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count % within EmailBinary Daily	3 33,3%	9 50,0%	12 44,4%
	partly agree	Count % within EmailBinary Daily	1 11,1%	4 22,2%	5 18,5%
	neither agree nor disagree	Count % within EmailBinary Daily	4 44,4%	0 ,0%	4 14,8%
	partly disagree	Count % within EmailBinary Daily	0 ,0%	5 27,8%	5 18,5%
	completely disagree	Count % within EmailBinary Daily	1 11,1%	0 ,0%	1 3,7%
Total	Count % within EmailBinary Daily	9 100,0%	18 100,0%	27 100,0%	

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count % within InternetBinary Daily	2 40,0%	10 45,5%	12 44,4%
	partly agree	Count % within InternetBinary Daily	1 20,0%	4 18,2%	5 18,5%
	neither agree nor disagree	Count % within InternetBinary Daily	2 40,0%	2 9,1%	4 14,8%
	partly disagree	Count % within InternetBinary Daily	0 ,0%	5 22,7%	5 18,5%
	completely disagree	Count % within InternetBinary Daily	0 ,0%	1 4,5%	1 3,7%
Total	Count % within InternetBinary Daily	5 100,0%	22 100,0%	27 100,0%	

Crosstabs

**q47data Databases being used for something else than the original purpose is a serious privacy problem
PhoneBinary Daily Crosstabulation**

			PhoneBinary Daily		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within PhoneBinary Daily	1 16,7%	13 61,9%	14 51,9%
	partly agree	Count % within PhoneBinary Daily	2 33,3%	5 23,8%	7 25,9%
	neither agree nor disagree	Count % within PhoneBinary Daily	1 16,7%	2 9,5%	3 11,1%
	partly disagree	Count % within PhoneBinary Daily	1 16,7%	0 ,0%	1 3,7%
	completely disagree	Count % within PhoneBinary Daily	1 16,7%	1 4,8%	2 7,4%
Total		Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%

**q47data Databases being used for something else than the original purpose is a serious privacy problem
EmailBinary Daily Crosstabulation**

			EmailBinary Daily		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within EmailBinary Daily	6 66,7%	8 44,4%	14 51,9%
	partly agree	Count % within EmailBinary Daily	1 11,1%	6 33,3%	7 25,9%
	neither agree nor disagree	Count % within EmailBinary Daily	1 11,1%	2 11,1%	3 11,1%
	partly disagree	Count % within EmailBinary Daily	0 ,0%	1 5,6%	1 3,7%
	completely disagree	Count % within EmailBinary Daily	1 11,1%	1 5,6%	2 7,4%
Total		Count % within EmailBinary Daily	9 100,0%	18 100,0%	27 100,0%

q47data Databases being used for something else than the original purpose is a serious privacy problem * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count % within InternetBinary Daily	5 100,0%	9 40,9%	14 51,9%
	partly agree	Count % within InternetBinary Daily	0 ,0%	7 31,8%	7 25,9%
	neither agree nor disagree	Count % within InternetBinary Daily	0 ,0%	3 13,6%	3 11,1%
	partly disagree	Count % within InternetBinary Daily	0 ,0%	1 4,5%	1 3,7%
	completely disagree	Count % within InternetBinary Daily	0 ,0%	2 9,1%	2 7,4%
Total		Count % within InternetBinary Daily	5 100,0%	22 100,0%	27 100,0%

Crosstabs

q51wire Eavesdropping is a serious violation of privacy * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within PhoneBinary Daily	2 33,3%	8 38,1%	10 37,0%
	partly agree	Count % within PhoneBinary Daily	2 33,3%	4 19,0%	6 22,2%
	neither agree nor disagree	Count % within PhoneBinary Daily	1 16,7%	3 14,3%	4 14,8%
	partly disagree	Count % within PhoneBinary Daily	1 16,7%	5 23,8%	6 22,2%
	completely disagree	Count % within PhoneBinary Daily	0 ,0%	1 4,8%	1 3,7%
Total		Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%

q51wire Eavesdropping is a serious violation of privacy * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within EmailBinary Daily	4 44,4%	6 33,3%	10 37,0%
	partly agree	Count % within EmailBinary Daily	0 ,0%	6 33,3%	6 22,2%
	neither agree nor disagree	Count % within EmailBinary Daily	2 22,2%	2 11,1%	4 14,8%
	partly disagree	Count % within EmailBinary Daily	2 22,2%	4 22,2%	6 22,2%
	completely disagree	Count % within EmailBinary Daily	1 11,1%	0 ,0%	1 3,7%
Total		Count % within EmailBinary Daily	9 100,0%	18 100,0%	27 100,0%

q51wire Eavesdropping is a serious violation of privacy * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count % within InternetBinary Daily	2 40,0%	8 36,4%	10 37,0%
	partly agree	Count % within InternetBinary Daily	1 20,0%	5 22,7%	6 22,2%
	neither agree nor disagree	Count % within InternetBinary Daily	1 20,0%	3 13,6%	4 14,8%
	partly disagree	Count % within InternetBinary Daily	1 20,0%	5 22,7%	6 22,2%
	completely disagree	Count % within InternetBinary Daily	0 ,0%	1 4,5%	1 3,7%
Total		Count % within InternetBinary Daily	5 100,0%	22 100,0%	27 100,0%

Crosstabs

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within PhoneBinary Daily	1 16,7%	9 42,9%	10 37,0%
	partly agree	Count % within PhoneBinary Daily	3 50,0%	4 19,0%	7 25,9%
	neither agree nor disagree	Count % within PhoneBinary Daily	1 16,7%	3 14,3%	4 14,8%
	partly disagree	Count % within PhoneBinary Daily	1 16,7%	5 23,8%	6 22,2%
Total		Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within EmailBinary Daily	6 66,7%	4 22,2%	10 37,0%
	partly agree	Count % within EmailBinary Daily	2 22,2%	5 27,8%	7 25,9%
	neither agree nor disagree	Count % within EmailBinary Daily	1 11,1%	3 16,7%	4 14,8%
	partly disagree	Count % within EmailBinary Daily	0 ,0%	6 33,3%	6 22,2%
Total		Count % within EmailBinary Daily	9 100,0%	18 100,0%	27 100,0%

**q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy *
InternetBinary Daily Crosstabulation**

			InternetBinary Daily		Total
			Less	Daily	
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count % within InternetBinary Daily	4 80,0%	6 27,3%	10 37,0%
	partly agree	Count % within InternetBinary Daily	1 20,0%	6 27,3%	7 25,9%
	neither agree nor disagree	Count % within InternetBinary Daily	0 ,0%	4 18,2%	4 14,8%
	partly disagree	Count % within InternetBinary Daily	0 ,0%	6 27,3%	6 22,2%
Total		Count % within InternetBinary Daily	5 100,0%	22 100,0%	27 100,0%

Crosstabs

**q58dilem1 Accept all access for counter terrorism * PhoneBinary Daily
Crosstabulation**

			PhoneBinary Daily		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count % within PhoneBinary Daily	4 66,7%	18 85,7%	22 81,5%
	yes	Count % within PhoneBinary Daily	2 33,3%	3 14,3%	5 18,5%
Total		Count % within PhoneBinary Daily	6 100,0%	21 100,0%	27 100,0%

q58dilem1 Accept all access for counter terrorism * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count	7	15	22
		% within EmailBinary Daily	77,8%	83,3%	81,5%
	yes	Count	2	3	5
		% within EmailBinary Daily	22,2%	16,7%	18,5%
Total		Count	9	18	27
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q58dilem1 Accept all access for counter terrorism	no	Count	4	18	22
		% within InternetBinary Daily	80,0%	81,8%	81,5%
	yes	Count	1	4	5
		% within InternetBinary Daily	20,0%	18,2%	18,5%
Total		Count	5	22	27
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q34local1 Terrorists and criminals w court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q34local1 Terrorists and criminals w court order	no	Count	1	5	6
		% within PhoneBinary Daily	16,7%	23,8%	22,2%
	yes	Count	5	16	21
		% within PhoneBinary Daily	83,3%	76,2%	77,8%
Total		Count	6	21	27
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local2 Any w/o court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q34local2 Any w/o court order	no	Count	4	19	23
		% within PhoneBinary Daily	66,7%	90,5%	85,2%
	yes	Count	2	2	4
		% within PhoneBinary Daily	33,3%	9,5%	14,8%
Total		Count	6	21	27
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local3 Emergency * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q34local3 Emergency	no	Count	3	4	7
		% within PhoneBinary Daily	50,0%	19,0%	25,9%
	yes	Count	3	17	20
		% within PhoneBinary Daily	50,0%	81,0%	74,1%
Total		Count	6	21	27
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local4 Never * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q34local4 Never	no	Count	6	20	26
		% within PhoneBinary Daily	100,0%	95,2%	96,3%
	yes	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,8%	3,7%
Total		Count	6	21	27
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local5 d.k. * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		Total
			Less	Daily	
q34local5 d.k. no	Count	6	21	27	
	% within PhoneBinary Daily	100,0%	100,0%	100,0%	
Total	Count	6	21	27	
	% within PhoneBinary Daily	100,0%	100,0%	100,0%	

Crosstabs**q52protect1 Anonymous calling cards * PhoneBinary Daily Crosstabulation**

				PhoneBinary Daily		Total
				Less	Daily	
q52protect1 Anonymous calling cards	no	Count	4	17	21	
		% within PhoneBinary Daily	66,7%	81,0%	77,8%	
	yes	Count	2	4	6	
		% within PhoneBinary Daily	33,3%	19,0%	22,2%	
Total		Count	6	21	27	
		% within PhoneBinary Daily	100,0%	100,0%	100,0%	

Crosstabs**q37local The possibility of locating all mobile phones is privacy infringing * PhoneBinary Daily Crosstabulation**

			PhoneBinary Daily		Total
			Less	Daily	
q37local The possibility of locating all mobile phones is privacy infringing	completely agree	Count	2	10	12
		% within PhoneBinary Daily	33,3%	47,6%	44,4%
	partly agree	Count	1	4	5
		% within PhoneBinary Daily	16,7%	19,0%	18,5%
partly disagree	Count	0	4	4	
	% within PhoneBinary Daily	,0%	19,0%	14,8%	
completely disagree	Count	3	3	6	
	% within PhoneBinary Daily	50,0%	14,3%	22,2%	
Total		Count	6	21	27
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q52protect2 Encryption programmes * EmailBinary Daily Crosstabulation

			EmailBinary Daily		Total
			Less	Daily	
q52protect2 Encryption programmes	no	Count	4	9	13
		% within EmailBinary Daily	44,4%	50,0%	48,1%
	yes	Count	5	9	14
		% within EmailBinary Daily	55,6%	50,0%	51,9%
Total		Count	9	18	27
		% within EmailBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q52protect3 Identity management * InternetBinary Daily Crosstabulation

			InternetBinary Daily		Total
			Less	Daily	
q52protect3 Identity management	no	Count	3	16	19
		% within InternetBinary Daily	60,0%	72,7%	70,4%
	yes	Count	2	6	8
		% within InternetBinary Daily	40,0%	27,3%	29,6%
Total		Count	5	22	27
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Crosstabs

q24biom5 Central bus and train station * PublicBinary2 Weekly Crosstabulation

			PublicBinary2 Weekly		Total
			less than once a week	at least once a week	
q24biom5 Central bus and train station	no	Count	12	8	20
		% within PublicBinary2 Weekly	63,2%	100,0%	74,1%
	yes	Count	7	0	7
		% within PublicBinary2 Weekly	36,8%	,0%	25,9%
Total		Count	19	8	27
		% within PublicBinary2 Weekly	100,0%	100,0%	100,0%

Crosstabs

q35local1 Terrorists and criminals w court order * CarBinary2 Weekly Crosstabulation

				CarBinary2 Weekly		Total
				less than once a week	at least once a week	
q35local1 Terrorists and criminals w court order	no	Count	0	4	4	
		% within CarBinary2 Weekly	,0%	25,0%	16,0%	
	yes	Count	9	12	21	
		% within CarBinary2 Weekly	100,0%	75,0%	84,0%	
Total		Count	9	16	25	
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%	

q35local2 Any w/o court order * CarBinary2 Weekly Crosstabulation

				CarBinary2 Weekly		Total
				less than once a week	at least once a week	
q35local2 Any w/o court order	no	Count	10	14	24	
		% within CarBinary2 Weekly	100,0%	82,4%	88,9%	
	yes	Count	0	3	3	
		% within CarBinary2 Weekly	,0%	17,6%	11,1%	
Total		Count	10	17	27	
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%	

q35local3 Stolen vehicles * CarBinary2 Weekly Crosstabulation

				CarBinary2 Weekly		Total
				less than once a week	at least once a week	
q35local3 Stolen vehicles	no	Count	2	6	8	
		% within CarBinary2 Weekly	20,0%	35,3%	29,6%	
	yes	Count	8	11	19	
		% within CarBinary2 Weekly	80,0%	64,7%	70,4%	
Total		Count	10	17	27	
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%	

q35local4 Speeding * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q35local4 Speeding	no	Count	7	10	17
		% within CarBinary2 Weekly	70,0%	58,8%	63,0%
	yes	Count	3	7	10
		% within CarBinary2 Weekly	30,0%	41,2%	37,0%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary2 Weekly Crosstabulation

				CarBinary2 Weekly		Total
				less than once a week	at least once a week	
q35local5 Automatic accident reporting	no	Count	3	4	7	
		% within CarBinary2 Weekly	30,0%	23,5%	25,9%	
	yes	Count	7	13	20	
		% within CarBinary2 Weekly	70,0%	76,5%	74,1%	
Total		Count	10	17	27	
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%	

Crosstabs

q36local Should eCall automatically be installed in all new cars? * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q36local Should eCall automatically be installed in all new cars?	yes	Count % within CarBinary2 Weekly	2 20,0%	5 29,4%	7 25,9%
	yes but possible to deactivate	Count % within CarBinary2 Weekly	3 30,0%	2 11,8%	5 18,5%
	no, optional	Count % within CarBinary2 Weekly	5 50,0%	9 52,9%	14 51,9%
	no, never	Count % within CarBinary2 Weekly	0 ,0%	1 5,9%	1 3,7%
Total		Count % within CarBinary2 Weekly	10 100,0%	17 100,0%	27 100,0%

Crosstabs

q39local The possibility of locating all cars is privacy infringing * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q39local The possibility of locating all cars is privacy infringing	completely agree	Count % within CarBinary2 Weekly	3 30,0%	7 41,2%	10 37,0%
	partly agree	Count % within CarBinary2 Weekly	4 40,0%	5 29,4%	9 33,3%
	neither agree nor disagree	Count % within CarBinary2 Weekly	0 ,0%	1 5,9%	1 3,7%
	partly disagree	Count % within CarBinary2 Weekly	1 10,0%	2 11,8%	3 11,1%
	completely disagree	Count % within CarBinary2 Weekly	2 20,0%	2 11,8%	4 14,8%
Total		Count % within CarBinary2 Weekly	10 100,0%	17 100,0%	27 100,0%

Crosstabs

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	7	8	15
		% within CarBinary2 Weekly	70,0%	47,1%	55,6%
	yes	Count	3	9	12
		% within CarBinary2 Weekly	30,0%	52,9%	44,4%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem2 Accept speeding tickets	no	Count	9	16	25
		% within CarBinary2 Weekly	90,0%	94,1%	92,6%
	yes	Count	1	1	2
		% within CarBinary2 Weekly	10,0%	5,9%	7,4%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem3 Accept register all movements	no	Count	10	14	24
		% within CarBinary2 Weekly	100,0%	82,4%	88,9%
	yes	Count	0	3	3
		% within CarBinary2 Weekly	,0%	17,6%	11,1%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem4 Accept only accidents	no	Count	4	12	16
		% within CarBinary2 Weekly	40,0%	70,6%	59,3%
	yes	Count	6	5	11
		% within CarBinary2 Weekly	60,0%	29,4%	40,7%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem5 Accept only if voluntary	no	Count	5	6	11
		% within CarBinary2 Weekly	50,0%	35,3%	40,7%
	yes	Count	5	11	16
		% within CarBinary2 Weekly	50,0%	64,7%	59,3%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary2 Weekly Crosstabulation

			CarBinary2 Weekly		Total
			less than once a week	at least once a week	
q59dilem6 d.k.	no	Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%
Total		Count	10	17	27
		% within CarBinary2 Weekly	100,0%	100,0%	100,0%

6.3 Recoding

To be able to compare education between countries, we have chosen to create a second education variable in accordance with the ISCED-97 standard as presented in “Classifying Educational Programmes – Manual for ISCED-97 Implementation in OECD Countries – 1999 Edition - OECD”.

For the cross-tabulations, we have chosen to create binary variables out of age and education, car, e-mail etc. instead of using three or more subgroups. The simple reason is the small datasets – if the statistics gets too detailed, it is impossible to make any useful interpretations of the results.

Accordingly the grouping has been done with three things in mind: 1) To construct groups which have an analytical value, e.g. young/old – high education/low education. 2) To construct groups with enough respondents to make comparison possible. 3) To create groups that are internationally comparable. This means we have tried to identify thresholds for the groups that can be shared by all countries involved.

The groups used in the cross tabulations:

Crosstabs

- Sex: Male / Female
- Age: 50 and above / 49 and below
- Education: Tertiary / non-tertiary
- Children: Yes / no
- Children at home: Yes / no

- Airplane: 1-2 times a year or more / less
- Public: Daily (Also weekly / less for Denmark and Germany)*
- Car: Daily / less (Also weekly / less for Germany)*
- Mobile: Daily / less
- E-mail: Daily / less

- Internet: Daily / less

* We have made additional groupings of these variables, as too few people fit into the 'daily' category in these countries.

6.4 Syntax / SPSS

recoding

```
RECODE
  eduISCED97
  (5 thru 6=1) (ELSE=0) INTO eduISCED97binary .
VARIABLE LABELS eduISCED97binary 'Tertiary'.
EXECUTE .
```

```
RECODE
  q2age
  (17 thru 49=0) (50 thru 90=1) (MISSING=Copy) INTO AgeBinary .
VARIABLE LABELS AgeBinary 'Age over and under 50'.
EXECUTE .
```

```
RECODE
  q9phone q10email q11internet q12publictransport q14car
  (1=1) (2 thru 5=0) INTO PhoneBinary EmailBinary InternetBinary PublicBinary CarBinary
.
VARIABLE LABELS PhoneBinary 'Daily' /EmailBinary 'Daily' /InternetBinary 'Daily'
/PublicBinary 'Daily' /CarBinary 'Daily'.
EXECUTE .
```

```
RECODE
  q12publictransport q14car
  (1 thru 2=1) (3 thru 5=0) INTO PublicBinary2 CarBinary2 .
VARIABLE LABELS PublicBinary2 'Weekly' /CarBinary2 'Weekly'.
EXECUTE .
```

```
RECODE
  q13plane
  (4 thru 5=1) (1 thru 3=0) INTO PlaneBinary .
VARIABLE LABELS PlaneBinary 'Less than once a year'.
EXECUTE .
```

crosstabs general attitude

```
CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q1sex
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .
```

```
CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY AgeBinary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
  /COUNT ROUND CELL .
```

```
CROSSTABS
  /TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY eduISCED97binary
  /FORMAT= AVALUE TABLES
  /CELLS= COUNT COLUMN
```

/COUNT ROUND CELL .

CROSSTABS

/TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q4children
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q15general q16general q17general q18general q19general q20general q21general
q22general BY q5childhome1
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLUMN
/COUNT ROUND CELL .

crosstabs 2

CROSSTABS

/TABLES=q24biom2 BY PlaneBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q56dilem1 BY PlaneBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q24biom5 BY PublicBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q55dilem1 BY PublicBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q35local1 q35local2 q35local3 q35local4 q35local5 BY CarBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q36local BY CarBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q39local BY CarBinary
/FORMAT= AVALUE TABLES

/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q59dilem1 q59dilem2 q59dilem3 q59dilem4 q59dilem5 q59dilem6 BY CarBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q43data BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q44data BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q45data BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q47data BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q51wire BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q53protect BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q58dilem1 BY PhoneBinary EmailBinary InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS

/TABLES=q34local1 q34local2 q34local3 q34local4 q34local5 BY PhoneBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q52protect1 BY PhoneBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q37local BY PhoneBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q52protect2 BY EmailBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q52protect3 BY InternetBinary
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

crosstabs DK & DE extra car and public

CROSSTABS
/TABLES=q24biom5 BY PublicBinary2
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q35local1 q35local2 q35local3 q35local4 q35local5 BY CarBinary2
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q36local BY CarBinary2
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q39local BY CarBinary2
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

CROSSTABS
/TABLES=q59dilem1 q59dilem2 q59dilem3 q59dilem4 q59dilem5 q59dilem6 BY CarBinary2
/FORMAT= AVALUE TABLES
/CELLS= COUNT COLOUMN
/COUNT ROUND CELL .

Annex 7 Comments from the questionnaire (in Danish)

”Spørgsmål 27 & 28 er besvaret som PASSIV overvågning”

”Jeg mener, at udgangspunktet for stillingtagen altid må være: Hvilket samfund ønsker vi, og ikke: Hvad kan berolige mig? Man kan gøre folk hysteriske over for alt fra atomterror til husstøvmider. Derfor er det vigtigt at angribe sikkerhedsemnet fra sin basis: Hvordan skal det være at leve i DK? Hvilke risici bliver vi nød til at leve med?”

”Uigennemskuelig for almindelige borger. Med de konsekvenser det har og kan have.”

”Til side 6 – nr. 20: Jeg vil føle mig som en ærværdig person, hvis jeg bliver overvåget – altså som en VIP – Det er rart at man passer på mig!”

”Mange af spørgsmålene er ikke klare nok i deres formulering” Eksempelvis er det svært at vide om der i spørgsmålene 37-40 menes den ”tekniske mulighed”, eller om det er ”valget” at kunne gøre brug af denne tekniske mulighed. Jeg mener at der ikke skelnes nok imellem det at data er tilgængeligt / gemt i en database, og så det at ”filtrere” / søge i disse data. Dette kommer eksempelvis til udtryk i spørgsmålene 27-28 vedrørende video-overvågning, hvor der ikke nævnes hvorvidt der er tale om aktiv eller passiv video-overvågning. Også i spørgsmålene om aflytning og interadfærd fremgår denne differentiering ikke eksplicit.”

”Jeg opfatter ikke DNA som automatisk at indgå i biometri”

”Vil dette gøre nogen som helst forskel? Hvem blev hørt i forb. med AntiTerror lovgivningen? Hvorfor er det ok, at mine data bliver logget på nettet? Men ikke ok at, der er én som følger efter mig m. kamera på gaden? Internettet er et sted ligesom den fysiske virkelighed. Lad være med at ødelægge vores muligheder for at kommunikere og eksistere bare fordi ”I” er bange for at udefinerbart ”andet”. Terror har ALTID eksisteret. Nu er det bare flyttet til den vestlige verden. Der er alligevel ingen som lytter til borgerne i disse spgsm. Så hvorfor dette møde? Kommissionen læser ikke rapporterne. Dette vil bare være et projekt, der viser at ”I har spurgt borgerne”. Men lytter kommissionen? Jeg synes www.edri.org skulle have mere at skulle have sagt.”

”Teknologien vil aldrig kunne sikres mod misbrug og derfor bør man kun indføre det allermest påkrævede og ikke kun tænke på forbrydelser og terrorisme.”

”For mig at se knytter der sig to væsentlige problemer til øget brug af sikkerhedsteknologi i øget omfang:

- 1) Jeg er ikke overbevist, at det forhindrer terror eller kriminalitet i nævneværdigt omfang. Det gør det højst lettere at opklare forbrydelser efterfølgende.
- 2) Sikkerheden sættes ofte ind, hvor det er overskueligt fx i lufthavne, mens banegården er ”umulige” og derfor ikke bliver sikret i samme omfang. Men der kan være lige så stor effekt i at springe et tog i luften som et fly.”

”Off. dataregistre skal beskyttes 100% mod misbrug af uvedkommende personer, og ikke sælges til private købere / Eksempel TDC sælger kundeoplysninger er tidligere et off. teleselskab.”

”Sikkerhedsteknologier bør altid overvejes grundigt før man beslutter om de skal bruges. Der er stor forskel på i hvilken grad de forskellige teknologier krænker (og virker krænkende for) privatlivets fred.”

”Ved flere af spørgsmålene savnede jeg en skelnen ml. m/ dommerkendelse og u/ dommerkendelse. Fx spsm. 38 eller 40.”