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 5.5 Norwegian Report
Interview meeting about security technology and privacy

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

Author(s):
Åse Kari Haugeto, Norwegian 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

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
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

Table of Contents **page**

Annex 1 Participants' background 4

Annex 2 Agenda for the meeting (in Norwegian) 6

Annex 3 Material sent to the participants (in Norwegian) 7

Letter of Invitation *8*
Confirmation e-mail *10*
Letter of Confirmation *11*
Reminder *13*
Scenarios *14*

Annex 4 Questionnaire and interview guide (in Norwegian) 26

4.1 Spørreskjema om sikkerhetsteknologi og personvern *27*
4.2 Intervjuguide *56*

Annex 5 Transcripts of group interviews (in Norwegian) 59

Group 1 *60*
Group 2 *81*
Group 3 *95*
Group 5 *111*

Annex 6 Frequency tables 123

Annex 7 Comments from the questionnaire 201

Annex 1

Participants' Background

Selection Matrix

Below are the 26 participants that participated in the interview meeting distributed in a matrix. The matrix was made as a selection tool for the recruitment process. As only 31 persons applied to participate at the interview meeting, we did not use the matrix to select people. Anyway the matrix will give an idea of the people present at the meeting:

The matrix separates the individuals by age (17-34 years, 35-54 years and 55-80 years), sex and level of education (low, medium and high)

Age	17-34 years			35-54 years			55-80 years		
Females	1	1		3	2	4	1	1	2
Males	2		2	1	2	2		1	1
Level of Education	Low	Medium	High	Low	Medium	High	Low	Medium	High

As the matrix show there were a few more women (15) than men (11) present at the meeting. Most of the participants were between 35 and 54 years old (14). The distribution of participants below 35 years (6) and above 55 years (6) was even.

11 participants had higher education, 7 had medium level of education and 8 had lower education.
The level of education is generated from the responses of what is your highest level of education

- Elementary School (7 or 9 years of schooling) and secondary school (high school graduation) is regarded as lower education
- Vocational training (skilled level/craftsman's training) and short-term higher education (less than 3 years of study) is regarded as medium level of education
- Medium length higher education (3 - 4 years of study) and advanced higher education (more than 4 years of study) is regarded as higher education

These were the participants' occupations:

Accountant
Student/part time sales clerk
Economist
Aviation technician
Teacher
IT consultant
Technical Drafter
Head of department
Director
Building technician
Medical secretary
Operations assistant
Primary school teacher
Translator/teacher
Consultant/house wife
Illustrator/postal worker
Head of department
System consultant
Software developer
Self employed
Psychiatric nurse (ongoing pedagogic education)
Parental advisor
Student/sales clerk
Financial consultant
Financial advisor
Study consultant

18 participants indicated in the questionnaire that they live in the metropolitan area of Stavanger. 2 people were living in a provincial town, and 6 were living in a rural area.

There was an overweight of people in the middle age range, living in the city and with higher education. But still the group of 26 participants was quite well distributed in respect to the selection criteria, and can be said to represent quite a random selection of the population in that area.

Communication and Transport

The frequency of the use of different communication and transport possibilities was asked about in the questionnaire.

All the participants were familiar using mobile phone, e-mail and internet. Everyone except from one used mobile phone at least once a day. 22 out of 26 participants used e-mail daily, 3 at least once a week, and 1 at least once a month. 23 out of 26 participants used internet daily, 1 at least once a week, and 1 at least once a month.

Public transportation was not frequently used by the participants. 17 of the participants used public transport less than once a month. 3 at least once a month, 3 at least once a week, and only 1 reported to use it daily.

On the other hand the participants' use of car was quite frequent. 16 of the participants reported to use it every day, 7 at least once a week, 2 at least once a month and only 1 did never use a car.

Finally the frequency of going by plane was mapped. 24 out of 26 participants reported to go by plane every year, most of them more than 3 times (roundtrip) a year. 6 persons reported to go more than 5 times a year, 9 reported to go 3-5 times a year and 9 reported to go 1-2 times a year, and only 2 reported to go less than once a year.

Family and Children

The questionnaire also mapped the size of the participants' household, and if they had children at home.

11 of the 26 participants lived in households with 4 or more people, included themselves. 14 of the participants lived in households with 2 or 3 persons and only 1 was living alone.

21 participants reported to have children, 20 having them as part of their household. 10 of the participants had children below 14 years living at home.

Annex 2

Program of the meeting

Date: 4th of June 2007
Place: Kompetansesenteret to the Municipality of Sandnes, located in the town centre of Sandnes.

Program:

18:00	Welcome by Tore Tennøe (director) and Åse Kari Haugeto (project manager)
18:20	Introduction to security technologies by Christine Hafskjold (expert)
18:50	Fill in of the questionnaire, individually
19:40	Discussions in groups
20:50	Sum up with comments and questions
21:00	End of meeting

Annex 3

Material sent to the participants

This annex consists of the material the participants received prior to the meeting:

Letter of invitation	Page 8
Confirmation e-mail	Page 10
Letter of confirmation	Page 11
Reminder	Page 13
Scenarios	Page 14

Teknologirådet er et uavhengig, offentlig organ som skal følge med den teknologiske utviklingen, vurdere muligheter og konsekvenser ved ny teknologi, og stimulere til samfunnsdebatt. Viktige målgrupper er Stortinget, øvrige myndigheter og media. Les mer på: www.teknologiradet.no

Teknologirådet

Kjære innbygger

Oslo, 16. april 2007

Vi trenger dine synspunkter!
Teknologirådet inviterer deg herved til å være med på et intervjumøte om overvåkning, personvern og sikkerhetsteknologier i Sandnes 4. juni 2007. Formålet med møtet er å få frem vanlige innbyggeres tanker omkring fremtidens samfunn. Vi har fått tillatelse fra Folkeregisteret til å plukke ut 2000 tilfeldig valgte personer i Rogaland til å motta dette brevet. Du er en av dem.

Hvorfor personvern og sikkerhet?
Du er kanskje klar over at informasjon om dine aktiviteter i økende grad blir registrert og lagret ulike steder: Når du ringer med mobiltelefonen, eller mottar en e-post, når du blir filmet av kameraer på togstasjonen, eller når du betaler med kort i butikken.

Dette er mulig på grunn av stadig mer avanserte sikkerhetsteknologier. Slike teknologier er hovedsaklig utviklet for at vi skal kunne føle oss trygge. De kan bidra til å forhindre kriminalitet, oppklare forbrytelser eller hindre terroristanslag.

Utvikling og bruk av sikkerhetsteknologier kan også være problematisk. Når samfunnet i økende grad overvåker potensielle lovbrytere, medfører det også mer overvåkning av uskyldige mennesker. Hvordan kan vi finne en balanse mellom det å kunne leve trygt i hverdagen og en mulig undergraving av personvern og misbruk av personopplysninger? Det er dette vi gjerne vil høre dine synspunkter på.

Hvorfor deg?
Utviklingen innen sikkerhetsteknologier vil påvirke oss alle. Det er derfor viktig å ta hensyn til hva folk flest synes – og derfor spør vi nettopp deg! Vi forventer ikke at du skal ha spesiell forhåndskunnskap om temaet, men du bør ha et ønske om å dele dine synspunkter. Dine og de andre deltakernes uttalelser vil bli anonymisert før de offentliggjøres.

Hva er anledningen?
Møtet i Sandes og tilsvarende møter i Østerrike, Danmark, Tyskland, Ungarn og Spania er en del av EU-prosjektet PRISE. Resultatet av PRISE vil være retningslinjer for fremtidig utvikling av sikkerhetsteknologier i EU. Prosjektet gjennomføres av fire institusjoner i Norge, Østerrike, Danmark og Tyskland. Synspunktene til deltakerne fra intervjumøtene vil bli et sentralt element i prosjektet.

Mer informasjon om PRISE finner du på Teknologirådets nettsider www.teknologiradet.no (norsk), og på PRISE-prosjektets egne nettsider www.prise.oeaw.ac.at (engelsk).

Pb. 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no

Om møtet
Møtet er et såkalt intervjumøte. Det er et uformelt kveldsmøte som varer i omtrent 3 timer. Du vil møte rundt 30 andre deltakere med ulik bakgrunn, men ingen vil ha noen spesiell forhåndskunnskap om temaet. En ekspert vil introdusere ulike dilemmaer mellom personvern og sikkerhetsteknologier, og det vil bli satt av tid til spørsmål i etterkant. Alle får så utdelt hvert sitt spørreskjema, hvor de kan komme med sine personlige synspunkter om temaet. Til slutt blir det diskusjoner i mindre grupper om fremtidige teknologier tenkt i ulike situasjoner. Gruppediskusjonene blir ledet av intervjuere fra Teknologirådet. Diskusjonene blir oppsummert i en rapport fra hvert land, og i en felles rapport for hele PRISE-prosjektet.

Praktisk informasjon
Tid: 4.juni kl 18-21.00 Enkel servering fra kl 1730
Sted: Kompetansesenteret til Sandnes kommune, Langgata 54, Sandnes sentrum

Teknologirådet dekker reiseutgifter i forbindelse med møtedeltakelsen, og betaler et mindre honorar.

Hvordan kan jeg delta?
Hvis du synes dette høres spennende ut, ber vi om at du sender oss et brev eller en e-post med navn, adresse, telefonnummer, kjønn, alder, utdanning og hvorfor du ønsker å delta på møtet. På bakgrunn av brevene vi mottar vil vi plukke ut et bredest mulig utvalg av personer til å være med.

Du må sende svaret ditt **senest mandag 30.april** til:

Teknologirådet
v/Åse Kari Haugeto
Postboks 522 Sentrum
0105 Oslo

eller send en e-post til:
aase.haugeto@teknologiradet.no

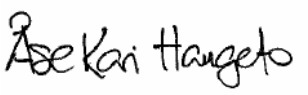
De som blir plukket ut vil få tilsendt en detaljert plan for møtet, samt en kort introduksjon om sikkerhetsteknologier. Alle som sender brev eller e-post til oss vil få svar senest i uke 20.

Hvis du ikke ønsker å være med, trenger du ikke svare på dette brevet. Navnet og adressen din vil ikke bli lagret av oss.

Har du noen spørsmål om arrangementet, kan du gjerne kontakte undertegnede.

Vi ser frem til å høre fra deg!

Med vennlig hilsen,



Åse Kari Haugeto
Prosjektleder, Teknologirådet

Fra: Åse Kari Haugeto
Sendt: 3. mai 2007 14:15
Til:
Emne: Intervjumøte i Sandnes

Takk for at du vil dele dine synspunkter om overvåking, personvern og sikkerhet!

Jeg vil med dette bekrefte at du er plukket ut til å være med på intervjumøtet i Sandnes 4. juni.

Ved å delta på møtet vil du være med på å gjøre en viktig jobb! Vanlige innbyggeres tanker omkring personvern og sikkerhetsteknologier er vesentlig når politikk og retningslinjer for teknologiutvikling skal utformes. Folk flest vil ofte se og oppleve ting på en annen måte enn eksperter som jobber med problemstillingene til daglig. Gruppen i Sandes vil bestå av ca. 30 personer med ulik bakgrunn, alder, bosted og motivasjon for å være med. Felles for deltakerne er at dere alle har uttrykt ønske om å få bidra i denne viktige diskusjonen. Fokus på møtet vil være å løfte debatten opp fra et rent faglig teknisk nivå og over til allmenne problemstillinger. Dermed håper vi å få større forståelse for hva slags fremtidig samfunn vi egentlig ønsker oss.

Tid for møtet: 4. juni klokken 1800-2100. Enkel servering fra kl 1730.
Sted for møtet: Kompetansesenteret til Sandnes kommune, Langgata 54 i Sandnes sentrum

Vi vil sende deg litt bakgrunnsstoff om temaet og praktiske detaljer om møtet i posten i slutten av mai.
Ta gjerne kontakt med undertegnede hvis du har små eller store spørsmål eller kommentarer.

Velkommen til møtet i Sandnes!

Med vennlig hilsen,

Åse Kari Haugeto

Prosjektleder
Teknologirådet
tlf: +47 23 31 83 14
mob: +47 93 64 67 24
e-post: aase.haugeto@teknologiradet.no

http://www.teknologiradet.no/

Teknologirådet er et uavhengig, offentlig organ som skal følge med den teknologiske utviklingen, vurdere muligheter og konsekvenser ved ny teknologi, og stimulere til samfunnsdebatt. Viktige målgrupper er Stortinget, øvrige myndigheter og media. Les mer på: www.teknologiradet.no

Teknologirådet

Oslo, 25. mai 2007

Kjære deltaker på intervjumøtet om personvern og samfunnssikkerhet

Nå nærmer dagen seg da du og rundt 30 andre skal møtes til intervjumøte i Sandes. Vi ser frem til å møte dere og høre deres synspunkter på håndtering av personvern og sikkerhet i fremtidens samfunn.

Tid: 4. juni klokken 1800-2100. Enkel servering fra kl 1730.

Sted: Kompetansesenteret til Sandnes kommune, Langgata 54 i Sandnes sentrum (se vedlagte kart).

Senteret ligger i gåavstand fra buss- og togstasjonen i Sandnes,i underkant av 5 minutter. Det er få parkeringsplasser i området, så vi anbefaler å parkere på parkeringshuset Ruten (rutebilstasjonen) hvis du kjører i egen bil.

Vi vil refundere dine reiseutgifter/ parkeringsutgifter i etterkant, så husk å ta vare på alle kvitteringer.

Om intervjumøtet
Målet for møtet er å få en bred forståelse av folks synspunkter på personvern og sikkerhetsteknologier. Temaet inneholder mange dilemmaer, og her finnes det ingen "rette" eller "gale" svar. Vi legger opp til et uformelt og engasjerende møte, der alle blir hørt.

Møtet er delt inn i tre deler. I den første delen vil deltakerne få en introduksjon til temaet. Målet er å gi alle en oversikt over de grunnleggende problemstillingene knyttet til sikkerhetsteknologi og personvern. Det blir anledning til å stille spørsmål.

I den andre delen vil du bli bedt om å fylle ut et spørreskjema om dine holdninger til ny sikkerhetsteknologi i forskjellige sammenhenger. Vi vil da være til stede for å svare på eventuelle spørsmål du måtte ha underveis.

I den siste delen vil deltakerne bli delt inn i grupper på 6-9 personer for å diskutere temaet grundigere. En intervjuleder fra Teknologirådet vil lede diskusjonen.

Til slutt vil alle samles og det blir tid til spørsmål og kommentarer.

Vi kommer til å ta opp gruppediskusjonene på bånd. Dette er for å sikre at vi får med oss alt som blir sagt til vår senere analyse. Alle dine ytringer under møtet (skriftlig og muntlig) vil i etterkant bli behandlet fortrolig og med full anonymitet.

Pb. 522 Sentrum
0105 Oslo

Prinsensgate 18
Norway

T: +47 23 31 83 00
F: +47 23 31 83 01

www.teknologiradet.no
post@teknologiradet.no

Tidsplan

18:00	Velkommen, introduksjon og spørsmål (felles)
18:50	Utfylling av spørreskjema (en og en)
19:40	Diskusjon i grupper
20:50	Oppsummering og kommentarer og spørsmål (felles)
21:00	Slutt

Det blir tilgang til drikke og snacks under møtet.

Forberedelse til møtet
Som vedlegg til dette brevet finner du litt bakgrunnsstoff om sikkerhetsteknologier og personvern – i form av scenarier (fortellinger). Scenariene presenterer hverdagslige situasjoner for to personer i en tenkt nær fremtid. De viser situasjoner der kjente sikkerhetsteknologier er i bruk, hvilke dilemmaer dette reiser og ulike syn på disse dilemmaene. I teksten vil du finne faktabokser med mer utfyllende informasjon om noen sentrale sikkerhetsteknologier.

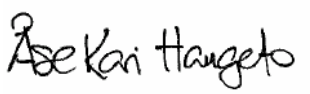
Vi ønsker at du leser disse scenariene i forkant av møtet og gjør deg noen tanker om situasjonene og dilemmaene som presenteres. Spørsmålene og diskusjonene på møtet vil være nært knyttet til scenariene.

Ved å delta på møtet vil du være med på å gjøre en viktig jobb!
Igjen vil vi takke for din interesse og ditt engasjement for temaet.

Ta gjerne kontakt hvis du har spørsmål eller kommentarer.

Vedlegg til dette brevet er:
- Informasjon om PRISE-prosjektet
- Scenarier
- Kart over Sandnes sentrum

Med vennlig hilsen,



Åse Kari Haugeto
Prosjektleder, Teknologirådet

tlf: +47 23 31 83 14
mob: +47 93 64 67 24
aase.haugeto@teknologiradet.no
www.teknologiradet.no

Fra: Åse Kari Haugeto
Sendt: 1. juni 2007 13:50
Til:
Emne: Intervjumøte mandag 4. juni: Personvern og sikkerhet

Hei

Jeg vil med dette sende en påminnelse om intervjumøtet om personvern og sikkerhet i Sandnes førstkommende mandag. Vi ser frem til å møte deg og høre dine synspunkter på temaet.

Tid: 4. juni klokken 1800-2100. Enkel servering fra kl 1730.

Sted: Kompetansesenteret til Sandnes kommune, Langgata 54 i Sandnes sentrum

(link til kart:
http://www.gulesider.no/kart/map.c?w=5.7322016469344&ps=4&tool=pan&n=58.8548540145909&s=58.8514466781286&e=5.74220165400651&imgt2=MAP&lne=&h=&scrollX=0&scrollY=0&imgt=MAP&lnw=&companies=&id=a_1010026)

Jeg håper at du har mottatt brev i posten med informasjon om møtet og bakgrunnsstoff vi ønsker du skal lese gjennom før du kommer.
I tilfelle du ikke har mottatt dette, legger jeg her ved scenariene i en egen fil. Disse vil være grunnlaget for diskusjonene på møtet.

Hvis du mot formodning ikke kan komme er det viktig at vi får beskjed om dette på forhånd.
Har du spørsmål, problemer med å finne frem eller lignende vil jeg være tilgjengelig på telefon nummer 93 64 67 24 på mandag.

Igjen vil jeg takke deg for at du har interesse og engasjement for dette tema. Dine synspunkter vil være viktige for å vite hvordan vi bør håndtere dilemmaer knyttet til sikkerhet og personvern i vårt fremtidige samfunn!

Med vennlig hilsen,

Åse Kari Haugeto

Prosjektleder
Teknologirådet
tlf: +47 23 31 83 14
mob: +47 93 64 67 24
e-post: aase.haugeto@teknologiradet.no

http://www.teknologiradet.no/

Sikkerhet og personvern

Scenarier

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

Innledning

Dette dokumentet vil presentere noen scenarier som viser hvordan sikkerhetsteknologier og overvåking kan brukes i hverdagslige situasjoner – i nær fremtid.

1.1 Hva er sikkerhetsteknologi?

Sikkerhet kan defineres som fravær av fare – det vil si en situasjon hvor den ønskede tilstanden ikke er truet eller forstyrret på noen måte. I PRISE-prosjektet forstås sikkerhet som samfunnssikkerhet – eller mer nøyaktig – som sikkerheten til borgerne som utgjør samfunnet.

Begrepet *sikkerhetsteknologi* kan dekke alt fra private alarmsystemer og virusbeskyttelse for PC-er, til grensekontrollsystemer og internasjonalt politisamarbeid via internett. I våre scenarier fokuserer vi hovedsakelig på teknologier eller tiltak (systemer, lovgivning, osv.) som er ment å øke sikkerhetsnivået i samfunnet ved å beskytte mot trusler fra individer, eller grupper av individer (ikke fra stater). Dette dekker kriminalitetsbekjempelse, antiterrortiltak, grensekontroll, osv.

I scenarieteksten presenterer vi enkelte fakta om de ulike teknologiene for å forklare hvordan teknologiene virker i dag og hvilke muligheter de har i fremtiden.

1.2 Hva er personvern?

Personvern forbindes generelt med beskyttelse av individets ukrenkelighet, selvstendighet og privatliv. I hovedsak dreier det seg om menneskers rett til å velge hvordan de ønsker å leve sine liv, og hva de ønsker skal være privat. Personvern anses som en grunnleggende menneskerettighet, og den første stadfestelsen av dette er artikkel 12 i Menneskerettighets-erklæringen.

Personvern er et vanskelig område å håndtere fordi personvernet nesten alltid konkurrerer med andre samfunnsgoder, som for eksempel mobilitet, effektivitet, sikkerhet eller bekvem-melighet. For eksempel: selv om vi vet at å gå med en påskrudd mobiltelefon gjør det mulig å spore hvor vi er, vil de fleste av oss ikke engang tenke på å la mobilen ligge hjemme! Og de fleste av oss vil heller ha en bompengebrikke i bilen fremfor å vente i kø med (anonyme) kontanter når vi kjører gjennom en bomstasjon.

Forskning antyder at mange mennesker ikke bekymrer seg for teknologier som krenker/griper inn i deres personvern, fordi de føler at de ikke har noe å skjule. Eksperter frykter at dette vil føre til en svekkelse av personvernet i samfunnet, som kan være vanskelig å vinne tilbake når det først er tapt. Og selv den mest lovlydige borger kan befinne seg i en situasjon hvor han ønsker verken å bli sett eller sporet.

Når det gjelder sikkerhetsteknologier og overvåking, hevder kritikere at mange av de iverksatte tiltakene ikke egner seg til å bekjempe terror, men bare til å berolige publikum med at “noe blir gjort”. Dette er fordi tiltakene kan omgås eller fordi trusselen de skal bekjempe er for usannsynlig til å legitimere det aktuelle tiltaket. Et eksempel er forbudet mange land har innført mot anonyme kontantkort til mobiltelefon. Kritikere hevder at dette forbudet bare rammer vanlige mennesker som ønsker å være anonyme. Forbrytere, derimot, har metoder for

å omgå forbudet ved å registrere seg med falsk identitet eller ved å bruke stjålne mobiltelefoner.

I USA er det de siste årene iverksatt antiterrortiltak som særlig krenker personvernet som griper inn i personvernet, slik som telefonavlytting, gjennomsøking av elektronisk kommunikasjon uten rettslig fullmakt, eller analyse av personer basert på informasjon samlet inn fra forskjellige kilder uten at vedkommende er informert.

Et viktig personvernprinsipp er at en person skal informeres når hans eller hennes personopplysninger lagres eller behandles, og at det er mulig å få tilgang til informasjonen og kontrollere at den er riktig. Personopplysninger skal bare samles inn og lagres dersom de virkelig er nødvendige, og de skal slettes når de ikke lenger trengs for det opprinnelige formålet.

Hva mener du om sikkerhetsteknologi? Scenarier som skal inspirere til debatt

Vi skal nå presentere historien til to mennesker: Carla og Peter. Vi vil følge dem i deres møte med ulike sikkerhetsteknologier og sikkerhetstiltak, og dele deres tanker og idéer om disse temaene. For å gjøre scenariene generelle har vi unngått å bruke spesifikke land, byer eller flyplasser som eksempler. Vi har i stedet forsøkt å vise hvordan forskjellige land – og myndigheter – har valgt ulike tilnærminger til innføring av sikkerhetsteknologi. Scenariene er lagt litt frem i tid, for å vise anvendelsen av enkelte sikkerhetsteknologier eller lovgivning som ikke er tatt i bruk ennå.

Vi håper at disse historiene vil inspirere deg til å tenke over sikkerhet og personvern og hva du mener om disse to verdiene.

Carla er 62. Hun har jobbet som lærer hele livet, men vurderer nå å førtidspensjonere seg. Alt er blitt så teknisk nå om dagen! Og barn virker mer bråkete enn før. Kanskje hun begynner å bli gammel? Denne uken vil hun imidlertid ikke bekymre seg over det. Sommerferien har begynt, og nå skal hun på besøk til sønnen sin som bor i et naboland.

Carla tar T-banen for å komme seg til jernbanestasjonen. Hun har "ladet" *universalbilletten* sin og bruker den til å betale for reisen ved å holde den opp foran leseren ved plattformsperringen. Billetten er et plastkort som inneholder en liten brikke. Brikken holder rede på hvor mange reiser hun har igjen på kortet. Carla har valgt en såkalt anonym billett. Hun vet at dette betyr at pengene går tapt dersom hun skulle miste billetten, og det er også litt ekstra bryderi siden hun må ha et separat kort. Den vanlige *universalbilletten* er selvfølgelig lagret i innehaverens *mobilenhet*. Alt du må gjøre er å bære enheten på deg eller i vesken din, og bekrefte med fingeravtrykket ditt når du passerer sperringen.

Carla kan ikke noe for det, hun synes det er ubehagelig å bruke fingeravtrykk for å identifisere seg. Hun legger selvfølgelig merke til at dagens ungdom ikke synes å bry seg, men for henne vil fingeravtrykk alltid være forbundet med forbrytere og arrestasjoner. "Det er ille nok at du må avgi fingeravtrykket ditt og vise ID-kortet ditt når du ønsker å reise utenlands," tenker hun. Hun ønsker definitivt ikke å gjøre det oftere enn hun må!

Biometri

Biometrisk teknologi kan identifisere mennesker automatisk ved å bruke deres fysiologiske kjennetegn eller adferdsmønstre. Biometri kan brukes til å kontrollere tilgang til fysiske områder eller informasjon (datamaskiner, dokumenter). De mest brukte formene for biometri er fingeravtrykk og ansiktskjennetegn.

I de fleste tilfeller gjøres bildet av det biometriske mønsteret om til en *mal*, som er en digital avbildning av de avleste kjennetegnene. Av hensyn til personvernet anbefales det å lagre kun malen, og slette det opprinnelige bildet. Det opprinnelige bildet beholdes likevel ofte i systemer som brukes av politiet, for eksempel i biometriske pass, og i ansiktsgjenkjenningssystemer.

Vi kan skille mellom *identifisering*, som går ut på å finne ut hvem en person er ved å sammenligne hans eller hennes mønster med alle malene som er lagret i et system, og *autentisering*, hvor vedkommende sammen-

lignes med malen som er lagret om ham eller henne, for å bekrefte at personen er den han eller hun hevder å være.

Prosessen med å sammenligne et biometrisk mønster med en forhåndslagret mal kalles verifikasjon. Sammenligningen resulterer i en poengsum. Resultatet kan bli "godkjent" eller "avvist" avhengig av hvorvidt denne poengsummen overstiger en viss grenseverdi.

En utfordring med biometriske systemer er å finne den riktige balansen mellom hvor ofte man kan akseptere at systemet identifiserer feil person (*feilakseptrate* eller *falsk positiv*) og hvor ofte det mislykkes i å identifisere en registrert person (*feilavvisning* eller *falsk negativ*).

En viktig fordel med biometriske kjennetegn er at de er så sterkt knyttet til et individ. Biometrisk autentisering gir bedre tilgangskontroll, og identitetstyveri blir vanskeligere når personopplysninger kobles utelukkende til den riktige personen. Men dette er også den største risikoen ved biometriske systemer. Så snart et sett med biometrisk data har blitt kompromittert (for eksempel stjålet), er det kompromittert for alltid.

Peter er 32. Han jobber som selger hos en bilforhandler. Denne morgenen må han stå tidlig opp for å reise til en bilmesse i Mellom-Europa. Han står opp, tar en rask dusj, får med seg bagen sin, setter seg bak rattet og kjører mot flyplassen. Som vanlig er han sent ute, men siden han har registrert seg for *fast track*, burde det gå bra. Fast track lar deg hoppe over alt maset med innsjekking, hvor passasjerene skal sjekkes opp mot profilene til forbrytere og passene kontrolleres – og så er det selvfølgelig den omfattende sikkerhetskontrollen. Med fast track går du gjennom en særlig grundig registreringsprosess én gang – og lar flyplassen lagre dine personopplysninger. Til gjengjeld kan du unngå vanlig innsjekking og bare autentisere deg selv ved å bruke biometrisk teknologi ved inngangen.

Han sender en tanke til kollegaen sin som, slik Peter ser det, er fiksert på personvern. Han hevder det er for mye overvåking i samfunnet slik det er, og nå godtar han ikke engang informasjonskapsler på datamaskinen sin! Han har til og med avinstallert Googles verktøylinje – ingen gjør det! Dersom det er sant at amerikanske myndigheter bruker slike data til å kartlegge nettverk og søke etter mistenkelige profiler, ville det vel vært allment kjent? Akkurat nå har kollegaen hans sikkert vært oppe i noen timer og står allerede i kø for innsjekking og sikkerhetskontroll. Vel – han har selv bedt om det! Peter håper bare at kollegaen kommer seg gjennom sikkerhetskontrollen tidsnok til at de kan gå gjennom presentasjonen sin én siste gang før ombordstigning.

- o -

Carla ankommer jernbanestasjonen. Som på T-banen er det kameraer overalt. Skjermer og høyttalere på veggene gjentar sikkerhetsmeldinger som ingen legger merke til lenger. "– Ikke la bagasjen stå ubevoktet." "– Bildet ditt vil bli sjekket mot databasen over kjente terrorister." Den siste meldingen vakte debatt for noen år siden. Mange land annonserer ikke at de tar bilder av folk og sjekker dem mot ulike databaser, og det ble foreslått at de ikke måtte gjøre det her i landet heller. Men regjeringen var veldig klar på prinsippet om at mennesker skal få vite når og hvor de blir kontrollert. "Det er særlig viktig når du ikke har noen mulighet til å oppdage det selv. Du kan egentlig ikke vite når du blir tatt bilde av lenger," tenker Carla. Hun har hørt at enkelte land også sjekker folks e-post og telefonsamtaler automatisk for ord og uttrykk som er mistenkelige – men det må da bare være et rykte!

Carla føler seg litt ør på grunn av alt bråket og går mot den *stille sonen*. Hun må vise ID-kortet sitt for å komme inn, men straks hun er inne kan hun slappe av: "Ingen kameraer, ingen mobiltelefoner, ingen trådløs sone, ingen bråkete meldinger! Det

burde virkelig være flere slike teknologifrie soner," tenker hun.

Det er ikke det at hun ikke er vant med kameraene. Tross alt har slike kameraer vært å se mesteparten av hennes voksne liv. Men er de ikke blitt mer påtrengende i det siste? Etter at de begynte å bruke programvare for ansikts- og mønstergjenkjenning, har hun en følelse av å være mer iakttatt og gransket enn før: "Har jeg samme bevegelsesmønster som en terrorist akkurat nå?" Tenk så pinlig det ville være å gjøre noe som førte til at hun ble stoppet og sjekket av antiterrorpolitiet! Riktignok har hun aldri blitt stoppet, men hun kan ikke la være å tenke på det når det er kameraer i nærheten.

Og, i likhet med de fleste mennesker, kjenner hun noen som faktisk har vært feilaktig mistenkt for å være terrorist. Da teknologien var i sin tidlige fase, var det mange problemer med programvaren for ansiktsgjenkjenning. Politikerne ønsket ikke at noen som var på listen over ettersøkte ikke skulle bli gjenkjent av systemet, noe som resulterte i mange såkalte *falske positive*.

En kollega av henne med foreldre fra Iran ble forvekslet med en terrorist en gang. Han opplevde det som svært ydmykende, og det synes ikke Carla er det minste rart. Som han sa: "Når du har blitt arrestert av antiterrorpoliti med skuddsikre vester, og du ser ut som meg, så ser mennesker annerledes på deg etterpå – selv om politiet lar deg gå med en beklagelse". Hun vet at han holdt seg unna de mest videoovervåkede områdene en god stund etterpå. Særlig når han hadde barna sine med seg.

I det siste har stadig flere satt spørsmålstegn både ved legitimiteten og effektiviteten til kameraene. I enkelte områder av byen gjør de nå forsøk hvor de installerer bedre og sterkere gatelys istedenfor overvåkingskameraer. Visstnok med gode resultater!

Videoovervåking

Videoovervåking med *aktive kameraer* er når en operatør følger med på en tv-skjerm og kan kontrollere kameraet (dreie, zoome) til å følge et individ eller en situasjon som utvikler seg. Aktive kameraer kan brukes sammen med automatiserte overvåkingsprogrammer til å oppdage mistenkelige bevegelser eller identifisere mennesker ved å sammenligne bildet deres med en referansedatabase.

Passive kameraer: Slike kameraer tar opp det som skjer på et bestemt sted (for eksempel i en kiosk). Båndet blir kun sett på dersom en situasjon oppstår, for eksempel ran eller slåsskamp.

Mens de tidligste videoovervåkingssystemene var analoge, er digitale systemer nå blitt mer utbredt. Digitale bildesøk kan spare tid når man skal finne igjen bestemte situasjoner eller spore mistenkte i en database. Samtidig er mange bekymret over at slike bilder også er lettere å manipulere.

Automatisk ansiktsgjenkjenning

Automatiske ansiktsgjenkjenningssystemer er systemer hvor bildet av en person tas automatisk og sammenlignes med en database for identifisering eller autentisering. Identifisering av en tilfeldig person basert på denne teknikken ville ha krevd en meget stor database, og en behandlingskapasitet utover det som er praktisk mulig i dag. Slike systemer brukes derfor vanligvis til å bekrefte at en person ikke er på en begrenset liste over for eksempel kjente forbrytere eller terrorister.

Automatisk bilskiltgjenkjenning (ANPR)

ANPR-systemer leser bilskilt som er tatt opp med videoovervåking og sjekker dem opp mot en database. Systemer for bilskiltgjenkjenning brukes i en rekke land, som oftest i forbindelse med bomstasjoner eller fotobokser, men også for å identifisere stjålne kjøretøy.

Som ansatt hos en bilforhandler har Peter alltid den nyeste bilmodellen. Den han kjører akkurat nå er utstyrt med all den nyeste teknologien: Galileo-satellittforbindelse med navigeringssystem, automatisk nødanrop gjennom eCall og en rekke andre sikkerhetssystemer for kjøretøy. Peter er ikke engang sikker på hva alle systemene gjør. eCall-systemet er nå standard i alle nye biler, og det skal ringe

nødnummeret automatisk dersom bilen blir innblandet i en ulykke. Fordi det er knyttet til Galileo-systemet, kjenner eCall bilens nøyaktige posisjon.

I løpet av de siste årene har det kommet forslag om å bruke teknologien til andre formål også. Etter et mislykket terrorangrep i Berlin, stjal terroristene en bil og flyktet gjennom Tyskland. Det viste seg da at systemet også kunne brukes til å spore bilen, og til og med stoppe den! Bilen var nemlig en dyr modell med det siste innen tyverisikringsteknologi, slik at bilen faktisk kunne stoppes via en satellitt. Terroristene ble stanset og arrestert, og etter dette ble EU-landene enige om at systemene også skulle kunne brukes av politiet for å spore forbrytere og mistenkte terrorister.

I kjølvannet av en forskningsrapport om hvor mange liv som kunne ha vært reddet i trafikken dersom bilistene overholdt fartsgrensene, ble det foreslått at sikkerhetssystemer for kjøretøy også burde kunne kjenne fartsgrensen på en gitt veistrekning og sjekke denne opp mot fartsmåleren i bilen. Det opprinnelige forslaget var at en brikke i motoren burde hindre alle biler fra å kjøre over fartsgrensen. Men dette ble møtt med omfattende protester, både fra bilindustrien og fra bileierforbundene. For tiden fungerer systemet slik at hver gang en bil kjører over fartsgrensen, gjøres et anrop til det sentrale bøteregisteret, og boten trekkes automatisk fra bileierens bankkonto.

Peter tråkker på gasspedalen. Samtlige veistrekninger har ennå ikke blitt oppdatert i systemet, og han har lastet ned en oversikt over hvilke veier som ligger inne til navigeringssystemet sitt. Han blir varslet hver gang han passerer et skilt som er koblet til systemet – noe som betyr at han "må" holde seg innenfor fartsgrensen. "Det er bra at overvåking også kan fungere motsatt vei," tenker han.

Lokaliseringsteknologi

Det er mulig å beregne den omtrentlige posisjonen til en brukers mobilutstyr ved å bruke kjente koordinater fra for eksempel GSM-basestasjoner.

For en mer nøyaktig posisjonering brukes satellittbaserte systemer:

GPS er en forkortelse for *Global Positioning System*, et verdensomspennende satellittnavigeringssystem dannet av 24 satellitter som går i bane rundt jorden. Ved å bruke tre satellitter kan GPS beregne mottakerens lengde- og breddegrad. Ved å bruke fire satellitter, kan GPS også fastslå høyden over havet.

Galileo kommer til å bli et verdensomspennende nettverk bestående av 30 satellitter som gir nøyaktig tids- og lokasjonsinformasjon til brukere på bakken og i luften. Nettverket planlegges å være i full drift i 2010. Det vil være mer nøyaktig enn GPS-systemet, og det vil ha større utbredelse.

eCall

eCall-modulen i en bil inneholder sensorer som aktiveres ved en ulykke. eCall ringer nødnummeret og overfører informasjon om ulykken, inkludert tidspunktet, den nøyaktige posisjonen, kjøretøyets kjøreretning og kjøretøyets kjennemerke.

eCall vil ikke være koblet til et mobilnettverk hele tiden, men kun kobles til i en ulykkessituasjon - for eksempel ved aktivering av airbag. Det eksisterer imidlertid bekymring for at dette kan endre seg. Mange er også opptatt av hvordan myndighetene vil forholde seg til overføring av tilleggsdata (for eksempel til forsikringsselskaper), og til mulighetene for uautorisert tilgang til databaser hvor eCall-data er lagret. Fra september 2009 er det planlagt at alle nye biler i Norge og en del andre land i Europa skal være utstyrt med eCall.

Peter ankommer flyplassen. Bilskiltet hans ligger allerede inne i systemet, og bilen hans registreres automatisk idet han kjører inn på parkeringsområdet. Det er den samme teknologien som brukes i byene for å identifisere stjålne kjøretøy. Han trodde faktisk at et slikt system ville være overflødig etter at eCall ble koblet til Galileo, men visstnok vet noen av de organiserte bandene hvordan de skal sette

systemet ut av drift. Og han vet at enkelte land til og med krever at bilisten skal kunne koble eCall-systemet fra selv. Slike krav gjør det alltid vanskeligere for bilindustrien! Og hvorfor virker det som om forbryterne alltid ligger ett skritt foran teknologien?

Formålsutglidning (function creep)

Databasesystemer er sårbare for såkalt formålsutglidning, det vil si at dataene brukes til noe annet enn det opprinnelig formålet. Et eksempel på slik formålsutglidning er det norske utlendingsregistret – som også inneholder biometrisk informasjon som fingeravtrykk. Det opprinnelige formålet med databasen var å bidra til å fastslå identiteten til asylsøkere. Senere ble det åpnet for politiet til etterforskning av straffesaker.

Peter parkerer bilen og går mot terminalen og inngangen for *fast track*. Han legger fingeren sin på sensoren og ser rett inn i kameraet. Et grønt lys blinker og døren åpnes.

Selv om sensorene er blitt mye bedre enn de pleide å være, har noen mennesker fortsatt problemer med å bruke fingeravtrykk: bestefaren hans, for eksempel. Til tross for at han er en sprek 80-åring, blir han stadig mer isolert. Nå om dagen må du bruke fingeravtrykket ditt som ID overalt. Bestefaren er ukomfortabel med alt maset han opplever når sensoren ikke greier å lese avtrykkene hans. Så han pleier for det mest å holde seg hjemme.

Peter går av og til på biblioteket for å låne *ekte* bøker for ham. Det morer ham å tenke på hvordan biblioteksprofilen hans må se ut. Dersom den en gang blir analysert i jakten på mistenkelige personer, vil etterretningstjenesten kanskje stusse over at en mann i 30-årene låner bøker som "Dating for pensjonister" og "Våre venner småfuglene".

For noen år siden, like etter at et større terrorangrep ble avverget i USA, kom det faktisk et forslag om at sikkerhetsmyndigheter burde gis tilgang til å søke gjennom alle mulige databaser. Og det gjaldt ikke bare for mistenkte forbrytere eller terrorister. Myndighetene ønsket å analysere all informasjon i bibliotekenes databaser, mønstre for elektrisitets- og gassforbruk, trafikkdata for telefoni og internett, reisedata og handlevaner. Ved å søke etter mistenkelige mønstre, ønsket de å identifisere mulige terrorister.

Kollegaen hans, Alex, ble opprørt, og Peter hadde prøvd å argumentere med/mot ham: De ville da ikke ha bedt om dette hvis de ikke hadde hatt gode grunner? Myndighetene må da gjøre hva de kan for å fange terrorister? Alex var ikke overbevist, og argumenterte med at dataene i det minste burde analyseres i anonymisert form: "Hvis de finner noe som er mistenkelig, kan de få en fullmakt fra retten for å fastslå identiteten. Det finnes ingen god grunn til at de skal vite alt om alle!"

Peter hadde egentlig ikke vært særlig interessert i å diskutere saken videre, men kollegaen hans hadde snakket om det i det uendelige i lunsjpausene, og til slutt hadde Peter undertegnet et opprop mot forslaget. "Men jeg ser virkelig ikke poenget med det," sa han. "Dette kan da bare være et problem for dem som har noe å skjule?" På den annen side tok han seg i å lure på om det var blitt registrert et eller annet sted at han hadde skrevet under på det oppropet…

Total Information Awareness (TIA)

Total Information Awareness (TIA) var et program utviklet av det amerikanske forsvarsdepartementets forskningsenhet DARPA etter terrorangrepene i i New York 2001. TIA-programmet inneholdt tre dataverktøy – oversetting, datasøk og mønstergjenkjenning, samt avanserte samarbeids- og beslutningsstøttesystemer.

Målet med TIA var å kunne forutsi terrorangrep før de inntraff. Systemet var ment å skanne private og offentlige databaser, samt internett, for transaksjoner som kunne forbindes med et terrorangrep. Kongressen i USA stanset finansieringen av TIA i september 2003, men mange av programmene fra systemet er blitt videreført under ulike navn.

Carla sitter i den stille sonen og leser litt i boken sin, før hun setter kursen mot sikkerhetssperringen.

Sikkerhetssperringen på den internasjonale jernbaneterminalen er et resultat av økt krav om kontroll, ikke bare på flyplasser, men også på andre steder hvor mange mennesker samles. Hun vet at i noen land foretas det til og med sikkerhetssjekk ved inngangene til butikksentre og idrettsarenaer. For noen år siden ble en selvmordsbomber anholdt på et butikksenter i nærheten av der hvor sønnen hennes bor. Senteret hadde visstnok nettopp begynt med å bruke skanneutstyr ved inngangen, og terroristen visste ikke dette. Hun er likevel glad for at det ikke har kommet så langt i hennes eget land. Så langt er det bare flyplass- og jernbaneterminalene som bruker passasjerskanning.

Hun selv er ikke så bekymret for butikksentre. Tross alt har det ikke vært noen trusler mot hjemlandet hennes, så vidt hun vet. Men hun har sett statistikk som viser at stadig flere mennesker har gått over til å handle i de mindre butikkene i sentrum, og at butikksentrene hevder at de taper penger fordi de ikke får lov til å sette opp skanneutstyr som for eksempel *naken-maskiner*.

Carla tar ut passet sitt og går opp til irisskanneren. Hun vet at noen land fortsatt bruker fingeravtrykk i sine ID-kort og pass, men hun synes at det å bruke iris er tryggere. Leseren sammenligner irisen hennes med malen som er lagret i passet. Hun pleide å bekymre seg over det, men sønnen hennes, som jobber i IT-industrien, har forsikret henne om at det er fullstendig trygt nå. “Den opprinnelige krypteringen i det første passet var ganske dårlig,” sa han, “men med krypteringen som brukes nå, ville en superdatamaskin måtte bruke flere årtusener på å knekke den! I det tidlige passet lagret de dessuten selve bildet av ansiktet og enten fingeravtrykkene eller irisen. Nå lagrer de bare en *mal* – en digital

Radiofrekvensidentifisering (RFID)

RFID er et begrep for automatisk identifisering ved bruk av radiobølger. Ørsmå integrerte kretser (brikker) med lagret informasjon knyttes til dokumenter eller innlemmes i produkter. En *leser* kan deretter brukes til å lese informasjonen på brikkene som er innen rekkevidde.

Det finnes både aktive og passive RFID-brikker. Aktive brikker – som bompengebrikker – har eget batteri og er derfor større enn passive brikker, men de kan romme mer informasjon og kan virke på lenger avstand. Passive brikker har ikke batteri, men får den nødvendige energien fra radiosignalet fra leseren. En typisk anvendelse av passive brikker er det nye europeiske passet, som også er tatt i bruk i Norge.

De fleste brikker kan kommunisere med en hvilken som helst leser. Men det finnes også brikker som krever at leseren oppgir et passord eller en annen form for autentisering.

Biometriske pass

Et biometrisk pass består av selve dokumentet, (den lille røde boken), og en liten brikke.

Brikken inneholder obligatoriske og valgfrie data. I tillegg fungerer brukerens fotografi som et visuelt bånd mellom innehaveren og passet.

Den internasjonale organisasjonen for sivil luftfart (ICAO) har valgt å bruke en brikke som kan leses på avstand (RFID-brikke). ICAO har valgt *ansiktet* som det primære biometriske kjennetegnet som skal brukes i pass. *Finger* og *iris* anbefales som sekundære biometriske kjennetegn. EU har valgt å bruke bare fingeravtrykk som det sekundære biometriske kjennetegnet.

Det har vært mye debatt knyttet til biometriske pass, særlig i forhold til sikkerheten til den biometriske informasjonen. Det fryktes at informasjonen kan stjeles gjennom skimming (dvs. å lese informasjonen på avstand uten at eieren vet om det) eller avlytting (dvs. å fange opp informasjonen idet den overføres).

For å imøtegå i disse bekymringene er det utviklet et system for tilgangskontroll, *basic access control* (BAC). BAC bruker en krypteringsnøkkel som avledes fra tallene nederst i den maskinlesbare sonen (strekkoden) til å “låse opp” brikken slik at systemet kan lese den. BAC har blitt kritisert for ikke å være sikker nok, og sikkerhetseksperter har klart å knekke krypteringen i løpet av bare noen få timer.

avbildning – av de viktigste kjennetegnene ved irisen og ansiktet. Selv om noen skulle knekke krypteringen, ville de ikke greie å gjenskape ansiktet eller irisen for å etterligne passinnehaveren."

Hun føler seg også betrygget av at leseren bare lagrer irismalen hennes lenge nok til å sammenligne den med den som ligger i kortet hennes, og at malen ikke lagres i en sentral database. Men hun er ikke så sikker på hva som skjer når passet hennes kontrolleres ved en annen landegrense. Blir dataene slettet etterpå også der?

Hun husker det var en skandale for noen år siden med en sentral fingeravtrykksdatabase – var det i USA, mon tro? En av de ansatte stjal mange fingeravtrykk og solgte dem til internasjonale forbrytere. Tusenvis av mennesker fikk sin identitet stjålet og opplevde deretter alle slags problemer – fra å være "svartelistet" på grensene til å få bankkontoene tømt. Det var særlig vanskelig fordi det tok så lang tid før regjeringen faktisk ville innrømme at dataen var på avveie. Og i mellomtiden ville ingen tro at identitetene deres var blitt stjålet – eller at det engang var mulig å bruke noens fingeravtrykk til å stjele identiteten deres!

Carla vet imidlertid bedre. I fjor sommer fikk en venn av sønnen hennes ID-en sin stjålet, like før han og familien hans skulle på ferie. Han var redd de måtte avlyse alt fordi han ville være "svartelistet". Men det nye Schengen informasjonssystemet, som brukes i mange europeiske land, registrerer visstnok mennesker som har fått identiteten sin stjålet. På grunn av dette kunne han og familien reise som planlagt, og han ble aldri beskyldt for å være forbryter eller terrorist, selv om ID-en hans antakeligvis ble kontrollert grundigere enn andres.

Etter ID-kontrollen må Carla sende bagasjen sin gjennom skanneren, før hun går gjennom det som før ble omtalt som

Passasjerskanning (*nakenmaskiner*)

Teknologier som analyserer objekter ved *røntgen* eller *terahertzstråling* har bedre gjennomtrengning i materialer enn optikk. Dette betyr at de kan brukes til å avsløre og avbilde gjenstander som skjules av klær.

En *nakenmaskin* utnytter denne type teknologi til å avsløre om en person har våpen eller sprengstoff skjult på kroppen. Forskjellige systemer er i bruk. Noen systemer avslører alt under klærne – ikke bare skytevåpen og sprengstoff – derav navnet. Denne formen for sikkerhetsteknologi er prøvd ut på Heathrow i London (Terminal 4) siden 2004. Andre anvendelser avbilder de skjulte gjenstandene og kopierer bildene over på en nøytral figur.

nakenmaskinen. Hun er lettet over at selve nakenmaskinen aldri ble kjøpt inn til flyplassene og de internasjonale jernbaneterminalene i hennes hjemland. Sikkerhetsmyndighetene vurderte ulike maskiner, men bestemte at det var like sikkert å bruke den type maskin hvor gjenstander som er gjemt under klærne projiseres over på et nøytralt bilde av personen.

Selv om hun er 62, er Carla selvbevisst i forhold til kroppen sin, og hun er glad for at de unge mennene ved sikkerhetssperringen ikke får se henne naken. Hun må ta av seg skoene, men bortsett fra det har hun ingen problemer, og finner seg snart til rette på toget.

- o -

Peter går gjennom flyplasshallen og over til sikkerhetskontrollen. Fast track-kunder må selvsagt også gå gjennom en form for sikkerhetskontroll. Men de har sin egen inngang, og de er alle erfarne reisende. Ingen i *denne* køen har på seg beltespenne av metall, eller er amatørmessige nok til å ha småmynter liggende i lommen. Og det er år og dag siden de spesiallagde skoene for forretningsfolk inneholdt metall. Han trekker inn magen og går gjennom *nakenmaskinen*. "Hvorfor holder de alltid en så lav temperatur i dette rommet?" tenker han, og rødmer idet han legger merke til at en av sikkerhetsvaktene er en

Datalagring

En database defineres som en organisert samling med data. Når ulik informasjon om en person kobles sammen, avslører det mer om vedkommende enn når informasjonsbitene betraktes hver for seg. Et viktig personvernsprinsipp i forbindelse med databaser som inneholder personopplysninger, er derfor at bare den informasjon som er nødvendig for å oppfylle systemets formål skal samles inn, og at slik informasjon skal slettes når den ikke lenger brukes.

I det siste har vi sett en trend hvor regjeringer har ønsket å bruke databaser til formål, som for eksempel sikkerhetstiltak, som avviker fra det opprinnelige. Dette dreier seg gjerne om oppbevaring av IKT-data, slik som kommunikasjonsdata fra telefon-, mobiltelefon- og internettrafikk.

EU har vedtatt et direktiv om oppbevaring av slike data – det såkalte datalagringsdirektivet. Data som er forbundet med *hvem* som kommuniserer, samt *når* og *hvor*, skal lagres. Selve innholdet i kommunikasjonen lagres ikke. Dataene kan oppbevares i inntil 2 år.

Ulike amerikanske departementer meldte i 2005 at de hadde kjøpt personopplysninger fra såkalte *informasjonsselgere* for rundt $30 millioner. Slike selskaper samler inn og kobler sammen personopplysninger fra flere kilder og gjør dem tilgjengelige for kundene sine. Kildene kan være offentlige registre, informasjon som er allment tilgjengelig (for eksempel på internettet) og informasjon fra proprietære kilder som for eksempel private selskaper.

kvinne på hans egen alder. Han er likevel glad for at flyplassen bruker den *ordentlige* nakenmaskinen. Det føles liksom tryggere.

Peter legger merke til noe nytt ved sikkerhetskontrollen som han ikke har sett før. Etter nakenmaskinen er det en ny "sperring" som noen av passasjerene blir bedt om å gå gjennom. Han husker svakt noe om at et nytt sikkerhetstiltak skulle prøves ut på denne flyplassen. Det registrerer visstnok slikt som kroppsvarme, svette, hjerterytme… Slike ting kan være et tegn på sykdommer som SARS eller fugleinfluensa, eller vise at en person er nervøs. Noen av forsøkspersonene blir geleidet til intervjurommene like ved. Han er glad for at han ikke ble valgt ut til testen, selv om han har god helse og ren samvittighet. "Men å sette opp dette i *hurtigkøen*? Vet de ikke at folk som velger fast track har det travelt?"

Han går til den riktige utgangen og setter seg ned. Kanskje han burde ringe Yasmin og la henne vite at han er på vei? Hun jobber for bilprodusenten som firmaet hans representerer, og han møtte henne på den siste bilmessen han var på. De fant straks tonen, og han vil veldig gjerne treffe henne igjen. På den annen side vil han nødig ringe henne på mobilen sin. Han vet at broren til Yasmin er veldig aktiv i en ungdomsgruppe ved moskéen sin, og at Yasmin sannsynligvis står på en eller annen overvåkingsliste på grunn av "nettverket" til broren sin. Peter skulle ønske han hadde kjøpt noen anonyme kontantkort sist han var i Asia. Det er ikke lenger lov å selge slike kort i Europa.

Avlytting

Det finnes ulike måter å overvåke folk og deres kommunikasjon, enten den finner sted over internettet, telefonnettverk eller innenfor definerte områder. *Telefonavlytting* er en slik form for avlytting. Dette går i hovedsak ut på å installere avlyttingsutstyr i forbindelsen mellom to telefoner. Avlyttingsutstyret kan monteres på telefonen til den som skal overvåkes, men også på telefoner til personer han eller hun forventes å kontakte.

En mer omfattende form for avlytting er vilkårlig å avlytte samtlige kommunikasjonslinjer (telefon, mobil, internett) på jakt etter samtaler som kan være av interesse. Det er mulig å analysere kommunikasjonsmønstre og å søke etter gitte nøkkelord i innholdet Et eksempel på dette er Echelon-nettverket, som styres av en allianse mellom USA, Storbritannia, Canada, Australia og New Zealand. Systemet ble opprinnelig opprettet for å overvåke kommunikasjonen i eller til Sovjetunionen og Øst-Europa under den kalde krigen.

Han ønsker heller ikke å bruke internettet. Det er ikke godt å vite hva som blir loggført i flyplassens nettverk. Han er ikke

engang sikker på hvordan reglene er nå om dagen. Har politiet direkte tilgang til slike data, eller trenger de en rettskjennelse? Plutselig ønsker han at han hadde fulgt bedre med i personverndebatten. Han kommer definitivt til å spørre kollegaen sin når han kommer seg på flyet.

Sist han spiste middag med Yasmin, nevnte hun at hun var sikker på at e-posten hennes ble gjennomsøkt, og hun ba ham om å bruke et krypteringsprogram dersom han ønsket å skrive til henne. "En ukryptert e-post er som et postkort," forklarte hun. "Enhver som har tilgang til det kan lese den – visste du ikke det?"

Han *hadde* tenkt å skrive til henne, men han oppdaget at e-postprogrammet på jobben ikke har innebygd kryptering, og han fikk aldri somlet seg til å installere et nytt program. Han håper hun ikke er sint på ham fordi han ikke har holdt kontakten. "Jeg forklarer det senere," tenker han.

Det er tid for ombordstigning. Peter går til utgangen, legger fingeren sin på sensoren og går om bord som en av de første passasjerene. Det er fortsatt mye plass til håndbagasje. Han tenker på kollegaen som sikkert fortsatt står i sikkerhetskøen, før han lener seg bakover og lukker øynene.

- o -

"Mamma er på vei," sier Carlas sønn til sin kone etter at å ha fått en automatisk melding på mobilen sin. "Hun burde være her om tre timer." Moren hans vet det ikke, men den nye mobilenheten hun fikk til jul er koblet til en tjeneste som kalles *barnevakten*. Teknologien er en ny utgave av sporingsutstyret du kunne se i gamle spionfilmer, hvor spanerne kunne overvåke de mistenkte i form av små prikker på et kart. Hovedforskjellen er at ved å bruke Galileo-teknologien som er innebygd i mobilenheten, kan han følge morens bevegelser på et kart selv når han sitter i sin egen stue i et annet land.

Personvernfremmende teknologier

Teknologi som bidrar direkte til å beskytte personvernet kalles for personvernfremmende teknologi (PET).

Anonymisering er én slik PET. Det finnes tjenester som muliggjør anonym elektronisk kommunikasjon for vanlige brukere. Slik teknologi skjuler forbindelsen mellom brukeren og sporene han eller hun etterlater seg, og kan derfor hindre uønsket identifisering. Tradisjonell kontantbetaling og uregistrerte (anonyme) kontantkort er tiltak som gir anonymitet.

Identitetsforvaltning er også en form for PET: Noen ganger ønsker du ikke å identifisere deg selv, men heller bruke et pseudonym (for eksempel på internettfora). For å gjøre det vanskeligere å koble sammen ulik data, kan det være en god idé å ha forskjellige brukernavn (som ikke avslører identiteten din) og forskjellige passord til ulike formål. Identitetsforvaltningssystemer hjelper mennesker i å holde rede på sine ulike brukernavn. Noen ganger trenger bare den aktuelle tjenesten å bekrefte en bestemt egenskap – som for eksempel alder eller kredittgrense. I slike tilfeller kan en *identitetsutsteder* (f.eks. banken din, en teleleverandør eller arbeidsgiver) opptre som en pålitelig tredjepart og garantere for denne egenskapen, uten å avsløre identiteten din.

Kryptering går ut på å forvrenge meldingsinnholdet for å gjøre meldingen ulesbar for andre. Fordi all elektronisk kommunikasjon er utsatt for avlytting eller manipulering, er det i mange tilfeller avgjørende at kommunikasjonen finner sted på krypterte linjer, eller at innholdet krypteres før overføring.

Han forsøker imidlertid ikke å se for mye på det – det føles som å snoke i privatlivet hennes. Men han har satt opp noen regler som gjør at mobilen hans varsler dersom hun ikke er i bevegelse over lang tid hjemme hos seg selv, eller dersom hun ikke er hjemme om natten. Tross alt er hun i ferd med å bli eldre. Og når han bor i et annet land, kan han ikke passe på henne slik han føler at han burde.

Telefonen hans ringer: "Hei, det er mamma. Jeg er på vei nå – jeg burde være på stasjonen om tre timer eller så…"

Annex 4

Questionnaire and Interview Guide

Questionnaire page 27
Interview guide page 56

Spørreskjema om sikkerhetsteknologi og personvern

Velkommen til PRISE-prosjektets spørreundersøkelse om holdninger til sikkerhetsteknologier og personvern.

I dette spørreskjemaet vil du få en rekke spørsmål. *Vi ønsker at du setter en ring ved det svaret som er riktig for deg, dvs rundt tallet ved svaret.* Du skal bare gi ett svar på hvert spørsmål, unntatt når det er oppgitt spesifikt at du kan sette ring rundt mer enn ett svar. Dersom du setter ring rundt feil svar, kan du bare sette et kryss over det svaret, og så sette en ring rundt det riktige svaret. Spør oss gjerne underveis dersom du lurer på noe knyttet til spørsmålene.

Bakgrunn:

1. Kjønn

1. Mann
2. Kvinne

2. Alder *(skriv inn alder)*

- Alder: ____

3. Antall personer i husholdningen din, inkludert deg selv?

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

4. Har du barn?

1. Ja
2. Nei

5. Bor noen av barna hjemme? *(Du kan sette ring rundt mer enn ett svar på dette spørsmålet)*

1. Nei
2. Ja, jeg har barn under 14 år som bor hjemme
3. Ja, je har barn over 14 år som bor hjemme

6. Hva er din høyeste fullførte utdanning?

1. Grunnskole, 7 år

2. Grunnskole, 9 år
3. Yrkesutdanning/Fagbrev
4. Videregående skole/studiekompetanse
5. Universitet eller høyskole, inntil 3 år
6. Universitet eller høyskole, 3-4 år
7. Universitet eller høyskole, 4 år eller mer

7. Yrke (*fyll inn stillingsbetegnelse eller yrkestittel, evt. arbeidssøkende, ufør eller lignende))*

- Yrke: _____

8. Bor du i byområde eller landlig?

1. Storby
2. Småby
3. Landlig område

9. Hvor ofte bruker du mobiltelefon?

1. Minst en gang om dagen
2. Minst en gang i uka
3. Minst en gang i måneden
4. Sjeldnere enn en gang i måneden
5. Bruker ikke mobiltelefon

10. Hvor ofte bruker du e-post?

1. Minst en gang om dagen
2. Minst en gang i uka
3. Minst en gang i måneden
4. Sjeldnere enn en gang i måneden
5. Skriver ikke e-post

11. Hvor ofte bruker du internett?

1. Minst en gang om dagen
2. Minst en gang i uka
3. Minst en gang i måneden
4. Sjeldnere enn en gang i måneden
5. Bruker ikke internett

12. Hvor ofte reiser du med offentlig transport?

1. Minst en gang om dagen
2. Minst en gang i uka
3. Minst en gang i måneden
4. Sjeldnere enn en gang i måneden
5. Reiser aldri med offentlig transport

13. Hvor ofte reiser du med fly? (Tur/retur-reise teller som en gang)

1. Mer enn 5 ganger i året
2. 3-5 ganger i året
3. 1-2 ganger i året
4. Sjeldnere enn 1 gang i året
5. Aldri

14. Hvor ofte bruker du bil?

1. Minst en gang om dagen
2. Minst en gang i uka
3. Minst en gang i måneden
4. Sjeldnere enn en gang i måneden
5. Bruker ikke bil

Generelle spørsmål om sikkerhetsteknologi og personvern

Under vil du finne en rekke utsagn om sikkerhetsteknologi og personvern. I hvilken grad er du enig i disse utsagnene?

- Hvis du mener utsagnet er helt riktig, setter du ring rundt "Helt enig"
- Hvis du mener utsagnet er riktig, men du har enkelte motforestillinger, setter du ring rundt "Litt enig"
- Hvis du mener det er umulig å avgjøre om utsagnet er riktig eller galt, setter du ring rundt "Verken enig eller uenig"
- Dersom du i hovedsak er uenig i utsagnet, men ser at det kan være noe riktig i det, setter du ring rundt "Litt uenig"
- Hvis du mener utsagnet er helt galt, setter du ring rundt "Helt uenig"

15. "Samfunnets trygghet er absolutt avhengig av at nye sikkerhetsteknologier blir tatt i bruk."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

16. “Mange sikkerhetsteknologier øker ikke sikkerhetsnivået, men er bare tatt i bruk for å vise at noe blir gjort for å bekjempe terror.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

17. “Hvis du ikke har noe å skjule trenger du ikke bekymre deg over at sikkerhetsteknologier kan gå ut over personvernet ditt.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

18. “Når det først finnes sikkerhetsteknologier, kan vi like gjerne ta dem i bruk.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

19. “Ingen burde få personvernet krenket uten at det foreligger mistanke om en kriminell handling.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

20. “Det er ubehagelig å bli overvåket, selv om man ikke har gjort noe galt.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

21. “Det er sannsynlig at myndighetene vil misbruke nye sikkerhetsteknologer.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

22. “Det er sannsynlig at kriminelle vil misbruke nye sikkerhetsteknologier.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Sikkerhetsteknologier

I denne delen av undersøkelsen vil du få spørsmål om dine holdninger til spesifikke sikkerhetsteknologier og hvordan de brukes. De grå tekstboksene gir informasjon om den aktuelle teknologien det spørres om. Boksene inneholder en del av den samme informasjon som boksene i scenariene du fikk tilsendt i forkant av møtet.

De første spørsmålene fokuserer på hvordan du synes det er greit å bruke teknologien. For de fleste av spørsmålene her vil det være mulig å gi mer enn ett svar.

Deretter ber vi deg ta stilling til bestemte utsagn om teknologien. For hvert av disse ber vi om at du angir i hvilken grad du er enig i utsagnet.

Biometri

Biometrisk teknologi kan identifisere mennesker automatisk ved å bruke deres fysiologiske kjennetegn eller adferdsmønstre. Biometri kan brukes til å kontrollere tilgang til fysiske områder eller informasjon (datamaskiner, dokumenter). De mest brukte formene for biometri er fingeravtrykk og ansiktskjennetegn.

Et biometrisk bilde kan bli laget som det originale bildet eller i form av en *mal*, som er en digital avbildning av de avleste kjennetegnene. Av hensyn til personvernet anbefales det å lagre kun malen, og slette det opprinnelige bildet. Det opprinnelige bildet beholdes likevel ofte i systemer som brukes av politiet, for eksempel biometriske pass, og i ansiktsgjenkjenningssystemer.

En av hovedfordelene med biometriske kjennetegn er at de er så sterkt knyttet til en bestemt person. Biometrisk autentisering gir bedre tilgangskontroll, og identitetstyveri blir vanskeligere når personopplysninger kobles utelukkende til den riktige personen. Men dette er også den største risikoen ved biometriske systemer. Så snart et sett med biometrisk data har blitt kompromittert, er det kompromittert for alltid.

Biometriske pass

Et biometrisk pass består av selve passdokumentet, vanligvis i form av en liten bok, med en liten brikke i. Brikken kan bli lest av en leser fra en viss avstand

Det har vært mye debatt knyttet til biometriske pass, særlig i forhold til sikkerheten til den biometriske informasjonen. Det fryktes at informasjonen kan stjeles gjennom skimming (det å lese informasjonen på avstand uten at eieren vet om det) eller avlytting (det å fange opp informasjonen idet den overføres).

23. Hvilken type biometri ville du synes det var greit å bruke i tilgangskontroll? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Ansikt
2. Fingeravtrykk
3. Iris
4. Jeg synes ikke det er greit å bruke noen form for biometri til tilgangskontroll
5. Vet ikke

24. I hvilke situasjoner synes du det er greit å bruke biometri i tilgangskontroll? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Ved sikkerhetskontroll i banker
2. For flyplassikkerhet
3. Ved sikkerhetskontroll i butikker
4. Ved grensekontroll/passkontroll
5. Til sikkerhetskontroll ved sentralbanestasjoner og bussterminaler
6. Til sikkerhetskontroll ved store idrettsarrangement eller andre arrangementer som samler mange
7. Ved sikkerhetskontroll i andre kommersielle sammenhenger
8. Det er aldri greit
9. Vet ikke

Utsagn om biometri

25. "Det er akseptabelt at alle innbyggeres biometriske data (for eksempel fingeravtykk eller DNA) lagres i en sentral database som kan brukes til kriminalitetsbekjempelse."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

26. "Jeg føler at det er utrygt å bruke et biometrisk pass fordi det er en fare for at mine biometriske data kan bli stjålet."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Videoovervåking

Videoovervåking med *aktive kameraer* er når en operatør følger med på en tv-skjerm og kan kontrollere kameraet (dreie, zoome) til å følge et individ eller en situasjon som utvikler seg. Aktive kameraer kan brukes sammen med automatiserte overvåkingsprogrammer til å oppdage mistenkelige bevegelser eller identifisere mennesker ved å sammenligne bildet deres med en referansedatabase.

Passive kameraer: Slike kameraer tar opp det som skjer på et bestemt sted (for eksempel i en kiosk). Båndet blir kun sett på dersom en situasjon oppstår, for eksempel et ran, en slåsskamp, osv.

Automatisk ansiktsgjenkjenning

Automatiske ansiktsgjenkjenningssystemer er systemer hvor bildet av en person tas automatisk og sammenlignes med en database for identifisering eller autentisering. Slike systemer brukes derfor vanligvis til å bekrefte at en person ikke er på en liste over for eksempel kjente forbrytere eller terrorister.

Automatisk bilskiltgjenkjenning (ANPR)

ANPR-systemer leser bilskilt som er tatt opp med videoovervåking og sjekker dem opp mot en database. Systemer for bilskiltgjenkjenning brukes i en rekke land, som oftest i forbindelse med bomstasjoner eller fotobokser, men også for å identifisere stjålne kjøretøy.

Passasjerskanning (*nakenmaskiner*)

Teknologier som analyserer objekter ved *røntgen* eller *terahertzstråling* har bedre gjennomtrengning i materialer enn optikk. Dette betyr at det kan brukes til å avsløre og avbilde gjenstander som skjules av klær.

En "nakenmaskin" utnytter denne type teknologi til å avsløre om en person har våpen eller sprengstoff skjult på kroppen. Forskjellige systemer er i bruk. Noen systemer avslører alt under klærne og ikke bare skytevåpen og sprengstoff – derav navnet. Denne formen for flyplassikkerhet har blitt utprøvd på Heathrow (Terminal 4) siden 2004. Andre anvendelser avbilder de skjulte gjenstandene og kopierer disse bildene over på en nøytral figur.

27. Hvor ville du akseptere videoovervåkning? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. I butikker
2. I prøverom for å forhindre butikktyveri
3. På sentralbanestasjoner og bussterminaler
4. I banker
5. På flyplasser
6. På sportsarenaer og andre plasser/arrangementer hvor mange samles
7. På alle offentlige steder
8. Det er aldri akseptabelt
9. Vet ikke

28. Hva synes du om omfanget av videoovervåkning på offentlige steder generelt?

1. Det burde være mer videoovervåkning på offentlige steder

2. Antall videoovervåkningskameraer på offentlige steder er passe per i dag

3. Det burde være mindre videoovervåkning av offentlige steder

4. Det burde ikke være videoovervåkning på offentlige steder i det hele tatt

5. Vet ikke

29. Hvor er det nødvendig å skanne personer for å avsløre skjulte gjenstander, av sikkerhetsmessige årsaker? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. På skoler

2. På sentralbanestasjoner og bussterminaler

3. På flyplasser

4. På kjøpesentre

5. I offentlige bygninger (f.eks rettsaler)

6. Det er aldri nødvending

7. Vet ikke

30. Hva slags skanning ville du synes var greit?*(Du kan sette ring rundt mer enn et svar på dette spørsmålet)*

1. Skanning som viser alt som skjuler seg under klærne

2. Skanning hvor bilder og skjulte objekter projiseres på en nøytral figur

3. Skanning av kroppsvarme og hjerterytme

4. Skanning etter objekter av metall

5. Bagasjeskanning med røntgen

6. Skanning er ikke akseptabelt

7. Vet ikke

Utsagn om videoovervåkning og passasjerskanning

31. "Videoovervåkning gjør at jeg føler meg tryggere."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

32. “Videoovervåkning går ut over personvernet mitt.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

33. “Å skanne personer for å se etter skjulte objekter er et greit tiltak for å forebygge terror.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Lokaliseringsteknologi

Det er mulig å beregne den omtrentlige posisjonen til en brukers mobilutstyr ved å bruke kjente koordinater fra for eksempel GSM-basestasjoner.

For en mer nøyaktig posisjonering brukes satellittbaserte systemer:

GPS er en forkortelse for *Global Positioning System*, som er det eksisterende systemet. *Galileo* vil komme i fullstendig drift i 2010. Det vil bli mer nøyaktig enn GPS-systemet, og det vil få større utbredelse,

eCall

eCall-modulen i en bil inneholder sensorer som aktiveres etter en ulykke. eCall ringer nødnummeret og overfører informasjon om ulykken, inkludert tidspunktet, den nøyaktige posisjonen, kjøretøyets kjøreretning og kjøretøyets kjennemerke.

eCall vil ikke være koblet til et mobilnettverk hele tiden, og vil bare kobles til når det aktiveres. Det er imidlertid bekymring for at dette kan endre seg. Mange er også opptatt av hvordan man vil forholde seg til overføring av tilleggsdata (for eksempel til forsikringsselskaper), og til mulighetene for uautorisert tilgang til databaser hvor eCall-data er lagret. Fra september 2009 er det planlagt at alle nye biler i Norge og en del andre land i Europa skal være utstyrt med eCall.

34. Når er det greit at en lokaliserer hvor en mobiltelefon befinner seg? *(Du kan sette ring rundt mer enn ett svar på dette spørsmålet)*

1. Politiet kan lokalisere mobiltelefonene til mistenkte terrorister og kriminelle etter å ha fått en rettskjennelse
2. Politiet kan lokalisere en mobiltelefon når som helst uten en rettskjennelse
3. I en nødssituasjon, for eksempel ved en ulykke, et savnet barn eller når en person er ute av stand til å ta vare på seg selv
4. Det er aldri greit
5. Vet ikke

35. Når er det greit å lokalisere hvor en bil befinner seg? *(Du kan sette ring rundt mer enn ett svar på dette spørsmålet)*

1. Politiet kan lokalisere en bil med mistenkte terrorister eller kriminelle etter å ha fått en rettskjennelse
2. Politiet kan lokalisere en hvilken som helst bil uten en rettskjennelse
3. Politiet kan lokalisere en stjålet bil
4. Lokalisering kan brukes til fartskontroll og til å gi fartsbøter
5. Automatisk lokalisering og oppringning av nødnummeret dersom det skjer en ulykke
6. Det er aldri greit
7. Vet ikke

36. Bør eCall installeres i alle nye biler?

1. Ja
2. Ja, men det bør være mulig å koble fra hvis den som bruker bilen ønsker det
3. Nei, det burde være valgfritt
4. Nei, det burde aldri installeres
5. Vet ikke

Utsagn om lokaliseringsteknologi

37. "Muligheten til å lokalisere alle mobiltelefoner er en trussel mot personvernet."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

38. "Muligheten til å lokalisere mobiltelefonen til en mistenkt er et godt redskap når politiet skal etterforske og forebygge terror og kriminalitet."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

39. “Muligheten for å lokalisere alle biler er en trussel mot personvernet.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

40. “Muligheten til å lokalisere alle biler er et godt verktøy for politiet når de skal etterforske og forebygge terror og kriminalitet.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Datalagring

En database defineres som en organisert samling med data. Når ulik informasjon om en person kobles sammen, avslører det mer om vedkommende enn når informasjonsbitene ses på hver for seg. Et viktig personvernsprinsipp i forbindelse med databaser som inneholder personopplysninger er derfor at bare den informasjon som er nødvendig for å oppfylle systemets formål skal samles inn, og at slik informasjon skal slettes når den ikke lenger brukes.

I det siste har vi sett en trend hvor regjeringer har ønsket å bruke databaser til formål, som for eksempel sikkerhet, som avviker fra det opprinnelige. Dette dreier seg gjerne om oppbevaring av IKT-data, slik som kommunikasjonsdata fra telefon-, mobiltelefon- og internettrafikk.

Total Information Awareness (TIA)

Total Information Awareness (TIA) var et program som ble utviklet av det amerikanske forsvarsdepartementets forskningsenhet DARPA etter terrorangrepene i New York 2001. TIA-programmet inneholdt tre dataverktøy – oversetting, datasøk og mønstergjenkjenning, og avanserte samarbeids- og beslutningsstøttesystemer.

Målet med TIA var å forutsi terrorangrep før de inntraff. Systemet var ment å skanne private og offentlige databaser, samt internett, for transaksjoner som kunne forbindes med et terrorangrep. Kongressen i USA stanset finansieringen av TIA i september 2003, men mange av programmene fra systemet er blitt videreført under ulike navn.

Formålsutglidning (function creep)

Databasesystemer er sårbare for såkalt formålsutglidning, det vil si at dataene brukes til noe annet enn det opprinnelig formålet. Et eksempel på slik formålsutglidning er da det norske utlendingsregistret – som også inneholder biometrisk informasjon som fingeravtrykk – ble åpnet for politiet til etterforskning av straffesaker i 2003. Det opprinnelige formålet med databasen var å bidra til å fastslå identiteten til asylsøkere.

41. Hva synes du er akseptable grunner til å lagre data om kommunikasjon? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Å forebygge terrorangrep generelt
2. Å etterforske et bestemt terrorangrep som har funnet sted
3. Generell kriminalitetsbekjempelse
4. Å etterforske bestemte forbrytelser som har funnet sted
5. Kommersiell bruk
6. Det er aldri akseptabelt
7. Vet ikke

42. Hva synes du er akseptable grunner til å søke gjennom og sette sammen personlige data fra ulike databaser? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Å forebygge terrorangrep generelt
2. Å etterforske et bestemt terrorangrep som har funnet sted
3. Generell kriminalitetsbekjempelse
4. Å etterforske bestemte forbrytelser som har funnet sted
5. Kommersiell bruk
6. Det er aldri akseptabelt
7. Vet ikke

Utsagn om datalagring

43. "Myndighetene bør lagre alle de data de synes det er nødvendig å lagre av sikkerhetsgrunner så lenge de mener det er nødvendig."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

44. "Data fra fasttelefon, mobiltelefon og internettkommunikasjon bør ikke lagres lenger enn det som er nødvendig for å kunne sende faktura til kundene."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

45. "Det å søke gjennom og sette sammen personlige data fra ulike databaser er en trussel mot personvernet."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

46. “Det å søke gjennom og sette sammen data fra ulike databaser er et godt verktøy for politiet i forebyggingen av terror.”

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

47. “Databaser brukt til et annet formål enn det som opprinnelig var hensikten, kan være en alvorlig trussel mot personvernet”

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

Avlytting

Det finnes ulike måter å overvåke folk og deres kommunikasjon, enten den finner sted over internettet, telefonnettverk eller innenfor definerte områder. *Telefonavlytting* er en slik form for avlytting. Dette går i hovedsak ut på å installere avlyttingsutstyr i forbindelsen mellom to telefoner. Avlyttingsutstyret kan monteres på telefonen til den som skal overvåkes, men også på telefoner til personer han eller hun forventes å kontakte.

En mer omfattende form for avlytting er å vilkårlig avlytte samtlige kommunikasjonslinjer (telefon, mobil, internett) på jakt etter samtaler som kan være av interesse.

48. Når synes du det er greit med telefonavlytting? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. For forebygging og etterforskning av terrorangrep dersom man har en rettskjennelse
2. For forebygging og etterforskning av terrorangrep *uten* en rettskjennelse
3. For forebygging og etterforskning av kriminalitet dersom man har en rettskjennelse
4. For forebygging og etterforskning av kriminalitet *uten* en rettskjennelse
5. For kommersielle formål
6. Det er aldri greit
7. Vet ikke

49. Når er det greit å bruke telefonavlytting?

1. Politiet bør kunne avlytte all kommunikasjon og søke etter samtaler som kan være av interesse
2. Politiet bør kunne avlytte mistenkte og personer en mistenkt forventes å kontakte
3. Politiet bør kunne avlytte en mistenkt
4. Telefonavlytting er aldri greit
5. Vet ikke

Utsagn om avlytting

50. “Avlytting er et godt etterforskningsverktøy for politiet.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

51. “Avlytting er en alvorlig krenkelse av personvernet.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Personvernfremmende teknologier

Teknologi som bidrar direkte til å beskytte personvern kalles for personvernfremmende teknologi (PET- Privacy enhancing technologies).

Anonymisering er én slik PET. Det finnes tjenester som muliggjør anonym elektronisk kommunikasjon for vanlige brukere. Slik teknologi skjuler forbindelsen mellom brukeren og sporene han eller hun etterlater seg, og kan derfor hindre uønsket identifisering. Tradisjonell kontantbetaling og uregistrerte (anonyme) kontantkort er tiltak som gir anonymitet.

Identitetsforvaltning er også en form for PET: Noen ganger ønsker du ikke å identifisere deg selv, men heller bruke et pseudonym (for eksempel på internettfora). For å gjøre det vanskeligere å koble sammen ulike data, kan det være en god idé å ha forskjellige brukernavn (som ikke avslører identiteten din) og forskjellige passord til ulike formål. Identitetsforvaltningssystemer hjelper mennesker i å holde rede på sine ulike brukernavn.

Kryptering går ut på å forvrenge meldingsinnholdet for å gjøre meldingen ulesbar for andre. Fordi all elektronisk kommunikasjon er utsatt for avlytting eller manipulering, er det i mange tilfeller avgjørende at kommunikasjonen finner sted på krypterte linjer, eller at innholdet krypteres før overføring.

52. Hva slags personvernfremmende teknologier burde være lovlig tilgjengelig for alle? *(Du kan sette ring rundt mer enn ett svar på dette spørsmålet)*

1. Anonyme kontantkort
2. Krypteringsprogrammer
3. Identitetsforvaltning
4. Ingen personvernfremmende teknologier burde være lovlig tilgjengelige
5. Vet ikke

Utsagn om personvernfremmende teknologier

53. "Personvernfremmende teknologier er nødvendige for å opprettholde personvernet i dagens samfunn."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

54. "Personvernfremmende teknologier burde ikke være lovlige dersom de gjør det vanskeligere for politiet å forebygge og etterforske terror."

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Dilemmaer ved bruk av sikkerhetsteknologier

Vi vil nå presentere en del spesifikke dilemmaer mellom bruk av sikkerhetsteknologier og konsekvenser for personvernet. For hvert dilemma ønsker vi at du skal tenke gjennom fordeler og ulemper før du svarer på spørsmålet. Du kan gi mer enn ett svar til alle spørsmålene i denne delen av skjemaet.

55. Ved å bruke fingeravtrykk på kollektivtransport til å registrere når og hvor du reiser, kan det bli mulig å trekke betalingen for reisen direkte fra kontoen din. Dette vil gjøre betaling enklere, men vil medføre at alle dine reiser blir registrert og at du må bruke fingeravtrykk for autentisering.

Hva ville du synes om en slik løsning? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Jeg kan akseptere at reisene mine registreres og å bruke fingeravtrykk fordi det gjør betalingen enklere
2. Jeg kan bare akseptere en slik løsning dersom fingeravtrykket mitt lagres som en mal og ikke kan gjenskapes
3. Jeg kan bare akseptere en slik løsning dersom de registrerte reisene slettes etter at betalingen er gjort
4. Det å bruke fingeravtrykk burde være en mulighet, men ikke det eneste alternativet for betaling
5. Jeg ville aldri brukt fingeravtrykk for autentisering på kollektivtransport
6. Vet ikke

56. Gjennom å registrere detaljerte opplysninger i en database tilknyttet flyplassen, og ved å akseptere visse sikkerhetsteknologier som kan bli sett på som krenkelse av personvernet, kan det bli mulig å sjekke inn raskere på flyplassen.

Hvilke sikkerhetsteknologier og avkall på personvernet ville du være villig til å akseptere for å kunne sjekke inn raskere på flyplassen? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Jeg ville akseptert en grundig første sjekk for så at mine data ble registrert i en permanent database tilknyttet flyplassen, for å kunne bruke biometriske kjennetegn for autentisering ved alle senere anledninger

2. Jeg ville akseptere å passere gjennom "nakenmaskinen"

3. Jeg ville akseptere skanning som sjekket svette, kroppsvarme og hjerterytme

4. Jeg ville ikke være villig til å gi opp noe av mitt personvern for rask innsjekking på flyplassen

5. Vet ikke

57. Aktive overvåkningskameraer og automatisk ansiktsgjenkjenning hvor menneskers ansikter sjekkes mot en database over kjente terrorister kan brukes for å forhindre terrorangrep, for eksempel på flyplasser og togstasjoner. Effekten av slike teknologier er imidlertid ikke bevist. Tiltakene kan også føre til at uskyldige feilaktig blir mistenkt for å være terrorister og innbrakt til avhør.

Hvilken kostnad er du villig til å akseptere for at samfunnet skal ta slik teknologi i bruk? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Aktive kameraer og automatisk ansiktsgjenkjenning burde tas i bruk uavhengig av hvor mange uskyldig som feilaktig mistenkes for å være terrorister

2. Aktive kameraer og automatisk ansiktsgjenkjenning burde tas i bruk dersom kun et lite antall uskyldige feilaktig mistenkes for å være terrorister

3. Aktive kameraer og automatisk ansiktsgjenkjenning burde bare tas i bruk dersom ingen uskyldige feilaktig mistenkes for å være terrorister

4. Aktive kameraer og automatisk ansiktsgjenkjenning burde kun tas i bruk på steder hvor det har vært mye kriminalitet eller som er spesielt sårbare for terrorangrep

5. Aktive kameraer og automatisk ansiktsgjenkjenning burde ikke tas i bruk noen steder

6. Vet ikke

58. Ny teknologi gjør det mulig å søke gjennom og sette sammen personlige data fra ulike databaser for å avsløre mistenkelige kommunikasjonsmønstre eller mistenkelig internettbruk. Hensikten er å forutse og forebygge terrorangrep, men dette medfører at man må gjennomsøke data fra uskyldige mennesker.

Hva slags praksis for å søke gjennom og sette sammen personlige data fra ulike kilder synes du er akseptabel? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Politiet burde ha adgang til å søke gjennom og sette sammen data fra alle mulig databaser, slik at de kan identifisere mønstre som kan avsløre mulige terrorister

2. Politiet burde bare ha adgang til å søke gjennom og sette sammen data fra ulike databaser dersom dataene anonymiseres, og kun kan kobles til en identifisert person etter en rettskjennelse

3. Politiet burde aldri ha mulighet til å søke gjennom og sette sammen data fra ulike databaser for å søke etter mistenkelige mønstre

4. Vet ikke

59. Teknologien eCall kan installeres i alle nye bilder for å kunne ringe opp nødnummeret ved en ulykke. Man kan tenke seg at teknologien også kan benyttes til å lokalisere biler for andre formål, for eksempel dersom de blir stjålet eller brukt til kriminalitet eller terror. Dette forutsetter imidlertid at alle bilers bevegelser registreres til enhver tid.

Hvilken bruk av eCall synes du er greit? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Jeg synes det er greit at eCall kan aktiveres av politiet for å lokalisere en bil dersom det er nødvendig for å forhindre kriminalitet eller terror

2. Jeg synes det er greit at eCall alltid er aktiv, og kan brukes til å utstede fartsbøter

3. Jeg synes det er greit at min bils bevegelser blir registrert til enhver tid

4. eCall bør ikke brukes til noe annet enn å rapportere ulykker

5. Det burde være frivillig å installere eCall

6. Vet ikke

60. Personvernfremmende teknologier (PET) kan bidra til å bevare personvernet ved kommunikasjon over telefon eller internett. Men PET kan også brukes av kriminelle og terrorister for å skjule sin identitet i planleggingen og utførelsen av kriminelle handlinger.

Dersom hensikten er å bevare personvernet til vanlige personer, hvor stor risiko er du villig til å akseptere for å kunne få lovlig tilgang til personvernfremmende teknologier? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Jeg kan godta at det er tillatt med anonyme kontantkort, selv om dette kan gjøre det vanskeligere for politiet å etterforske og forebygge kriminalitet og terror

2. Jeg kan godta at det er tillatt å bruke kryptering, selv om dette kan gjøre det vanskeligere for politiet å etterforske og forebygge kriminalitet og terror

3. Jeg kan godta anonymitet på internett, selv om dette kan gjøre det vanskeligere for politiet å etterforske og forebygge kriminalitet og terror

4. Jeg kan godta at anonymitet på internett gjør at personer som søker etter barnepornografi ikke kan spores av politiet

5. Jeg kan ikke akseptere at personvernfremmende teknologier gjøre det vanskeligere for politiet å etterforske og forebygge kriminalitet og terror

6. Vet ikke

61. Dersom en teknologi kan gi god samfunnssikkerhet, hvilke konsekvenser kan du akseptere for dem som ikke kan bruke teknologien eller nekter å bruke teknologien av hensyn til sitt personvern? *(Du kan sette ring ved mer enn ett svar på dette spørsmålet)*

1. Jeg kan akseptere at mennesker som ikke ønsker å ta teknologien i bruk av personvernshensyn blir ekskludert fra å benytte enkelte offentlige tjenester

2. Jeg kan akseptere at mennesker som ikke har mulighet til å ta teknologien i bruk blir ekskludert fra å benytte enkelte offentlige tjenester

3. Jeg kan akseptere at mennesker som ikke ønsker å ta teknologien i bruk av personvernshensyn opplever noen ulemper for eksempel når de benytter offentlig transport

4. Jeg kan akseptere at mennesker som ikke har mulighet til å ta teknologien i bruk opplever noen ulemper for eksempel når de benytter offentlig transport

5. Jeg kan ikke akseptere noen konsekvenser for mennesker som ikke ønsker å ta teknologien i bruk av personvernshensyn

6. Jeg kan ikke akseptere noen konsekvenser for mennesker som ikke har mulighet til å ta teknologien i bruk

7. Vet ikke

Demokratispørsmål

I denne delen av undersøkelsen vil du få presentert en rekke utsagn om demokratispørsmål knyttet til sikkerhetsteknologier og –tiltak. Hvem skal ha mulighet til å påvirke beslutninger knyttet til sikkerhet og personvern, og hvordan?

I hvilken grad er du enig i de følgende synspunktene? Gi kun ett svar for hvert utsagn.

62. "Politikere må alltid gjøre viktige spørsmål til gjenstand for offentlig debatt og høringer før de tar avgjørelser om innføring av ny sikkerhetsteknologi."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

63. "Temaet sikkerhet og personvern er så komplisert at det ikke gir mening å trekke allmennheten inn i diskusjonen."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

64. "Menneskerettighetsorganisasjoner har en rett til å bli hørt når man skal ta viktige beslutninger knyttet til sikkerhet og personvern."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

65. "Det er viktig at kommersielle selskaper som medvirker i produksjon av sikkerhetsteknologier også har en rett til å bli hørt når man skal ta viktige beslutninger knyttet til sikkerhet og personvern."

1. Helt enig

2. Litt enig

3. Verken enig eller uenig

4. Litt uenig

5. Helt uenig

66. “I forbindelse med at det skal tas viktige beslutninger omkring sikkerhetsteknologier, er det viktig at alternative løsninger er belyst og inkludert i debatten.”

1. Helt enig
2. Litt enig
3. Verken enig eller uenig
4. Litt uenig
5. Helt uenig

Forslag knyttet til personvernfremmende teknologier

I denne delen av undersøkelsen vil vi at du skal vurdere noen forslag knyttet til hvordan man kan utvikle, ta i bruk og forske på sikkerhetsteknologier uten å krenke personvernet. For hvert forslag ber vi om at du oppgir hvor viktig du synes det er å gjennomføre forslaget.

Dersom du synes det er veldig viktig å gjennomføre forslaget, setter du ring rundt “Viktig”
Dersom du synes det er viktig, men ikke bør prioriteres høyest, setter du ring rundt ”Litt viktig”
Dersom du ikke synes det er så viktig, setter du ring rundt “Ikke så viktig”
Dersom du ikke synes forslaget skal gjennomføres, setter du ring rundt “Ikke viktig i det hele tatt”
Dersom du er usikker på hva du skal svare, setter du ring rundt “Vet ikke”

Forslag

67. ”Når det samles inn personlige data fra intetanende individer må dataene anonymiseres fram til det foreligger en rettskjennelse for å avsløre en persons identitet som følge av funn i dataene.”

1. Viktig
2. Litt viktig
3. Ikke så viktig
4. Ikke viktig i det hele tatt
5. Vet ikke

68. ”Kun autorisert personale skal ha adgang til å samle inn personlige data.”

1. Viktig
2. Litt viktig
3. Ikke så viktig
4. Ikke viktig i det hele tatt
5. Vet ikke

69. ”Før man innfører en sikkerhetsteknologi eller et sikkerhetstiltak, må man vurdere konsekvensene for personvernet.”

1. Viktig
2. Litt viktig
3. Ikke så viktig
4. Ikke viktig i det hele tatt
5. Vet ikke

70. ”Finansiering av forskningsprosjekter på sikkerhetsteknologi bør avhenge av hvor grundige analyser man har gjort av konsekvensene for personvernet.”

1. Viktig
2. Litt viktig
3. Ikke så viktig
4. Ikke viktig i det hele tatt
5. Vet ikke

Avslutningsspørsmål

Du har nå svart på mange ulike og detaljerte spørsmål knyttet til sikkerhet og personvern. Til slutt vil vi be deg svare på to spørsmål:

70. Har holdningen din til sikkerhetsteknologier og personvern endret seg gjennom utfyllingen av dette spørreskjemaet?

1. Ja, holdningen er blitt mer positiv til sikkerhetsteknologier generelt
2. Ja, jeg er blitt mer skeptisk til sikkerhetsteknologier generelt
3. Nei, jeg har ikke endret holdning
4. Vet ikke

71. Dersom du har noen kommentarer knyttet til sikkerhetsteknologier du ønsker å gi uttrykk for, og som du ikke har hatt mulighet til å uttrykke tidligere i spørreskjemaet, kan du gjøre det her:

1. Jeg har ikke noe å tilføye
2. Mine kommentarer (tilføy under):

Intervjuguide

Spørsmålene i uthevet skrift skal diskuteres av deltakerne. Etter hvert spørsmål følger en liten forklaring med formålet på spørsmålet. Ved de fleste spørsmålene følger noen underspørsmål. Disse er til inspirasjon og kan brukes som støtte i diskusjonen hvis nødvendig. Underspørsmålene er ikke obligatoriske, og men kan nyttes hvis bordstyrer mener det er behov for det.

Spørsmål

1. Hva er dine umiddelbare tanker om sikkerhetsteknologier og personvern?
Formålet med spørsmålet: Et åpent spørsmål for å starte diskusjonen og å gi deltakerne mulighet til å fremlegge sine umiddelbare holdninger.

2. Hva synes du om scenariene?
Formålet med spørsmålet: Få deltakerne til å snakke om det de har lest i scenariene for å få inntrykk av hva de synes om den fremtiden som er skissert der.

Underordnede spørsmål:
- Hvordan er balansen mellom sikkerhet og personvern i scenariene?
- Synes du det er viktig å kunne få den type fordeler som er skissert i scenariene?
- Skissere scenariene en forlokkende fremtid?

3. Hva synes du er viktige positive potensialer for sikkerhetsteknologier?
Formålet med spørsmålet: Få deltakerne til å fokusere på de positive potensialer og få et inntrykk av hva de synes er fordelene man kan oppnå ved bruk av sikkerhetsteknologier.

Underordnede spørsmål:
- Hva kan du oppnå ved sikkerhetsteknologier? -Gi eksempler!
- Hva er den viktigste positive muligheten?
- Hvorfor er dette viktig?

4. Hvilke negative effekter av sikkerhetsteknologier er du bekymret for?
Formålet med spørsmålet: Få deltakerne til å fokusere på de negative potensialer og trusler ved sikkerhetsteknologier, og få et inntrykk av hva deltakerne ser som den største trusselen.

Underordnede spørsmål:
- Hva er de mest negative effekter av sikkerhetsteknologier? - Gi eksempler!
- Hva er den største trusselen?
- Hvorfor er dette en stor trussel?

5. Når mener du sikkerhet er viktigere enn personvern - og omvendt?
Formålet med spørsmålet: Få deltakerne til å debattere dilemmaet mellom sikkerhet og personvern for å få et inntrykk av når (i hvilke situasjoner) og evt. hvor mye av personvernet de er ville til å gi opp av sikkerhetsgrunner.

Underordnede spørsmål:
- På hvilke steder eller i hvilke situasjoner synes du det er greit at bruk av sikkerhetsteknologier går ut over personvernet
- På hvilke steder eller i hvilke situasjoner synes du personvernet er viktigere enn sikkerhet?

6. Hvem bør være med å bestemme hvordan nye sikkerhetsteknologier kan brukes?
Formålet med spørsmålet: Få deltakernes synspunkter på demokratiske hensyn og viktigheten av å involvere ulike interessegrupper når beslutninger om tema tas.

Underordnede spørsmål:
- Hvilke interessegrupper bør bli hørt? (innbyggere generelt, menneskerettighetsorganisasjoner, teknologiutviklere, politikere etc.)

7. Har du formeninger om reguleringer av nyutvikling og bruk av nye sikkerhetsteknologier?
Formålet med spørsmålet: Få deltakernes synspunkter på hvordan man bør håndtere utvikling og implementering av nye sikkerhetsteknologier.

Underordnede spørsmål:
Bør det være begrensninger på utvikling av sikkerhetsteknologier, eller bør industrien kunne utvikle det de selv ønsker?
Bør myndighetene kunne bruke den sikkerhetsteknologien de mener er viktig, eller bør det være reguleringer i så fall hvilke reguleringer?

8. Har din deltakelse i dagens arrangement endret din holdning til sikkerhetsteknologier og personvern?
Formålet med spørsmålet: Finne ut om informasjon og debatt om temaet har endret deltakernes holdninger.

9. Har du noen sluttkommentarer du ønsker å legge til?
Formålet med spørsmålet: Gi deltakerne mulighet til å komme med et siste ord i saken før møtet er over

Underordnede spørsmål:
- Har noe gjort spesielt inntrykk gjennom samtalen?

Rules of thumb
"Rules of thumb" and tips on how to carry out the group interview in a good way.

Introduction
Start by presenting yourself, "My name is ... I'm from ..., and I'm going to be the moderator at this group conversation. But you just talk and I will make a list of speakers if necessary.
After that you do a presentation round where people say their name and why they have come to the interview meeting

After that the TAPE RECORDER IS STARTED !! This is done in a free-and-easy way and by a easy comment. It is important to create a light atmosphere and play down the seriousness to make sure that the participants are not oppressed by the situation.

The first question is raised and the group interview is on its way.
The first question is always a "brainstorm" question, and a can affect a lot of immediate attitudes. It is important to give space, be open and listen in the beginning.

On the way
It is not important that all participants answer all questions, but the interviewer should have an impression of what they all think.
If anyone is hiding, the interviewer can always ask "Do you agree, John, or what do you think?"

There will be overlap in questions and answers. Skip questions if they have already been debated and answered
Tick of on the way, when you think that a question have been debated

It is important that all questions are debated. But questions that are more important to the participants than the ones in the interview guide can appear in the discussion and there should always be time to discuss these questions (as long as they are related to the security and privacy debate).

If someone becomes too dominating, it is the interviewers job to bring on the other participants. Ask e.g. "What do the rest of you think?" Interrupt if necessary, it is important that everybody is heard.

If the participants don't say much at the group interview, the interviewer can "take a round" saying that "at the next question I would like to take a round where everybody gives an answer".

Ask for reasons and arguments, "How come you think that... / What is the reason for...

Be aware of the participants reactions; Do they feel comfortable, do they seem under pressure or uneasy etc.

If you are through all the questions before time, you can go back to some of the questions that have not been debated that much on the way.

Closing
When there is 7-8 minutes left, it is a good idea to take a round where everybody gets to make a final remark. The final remark can be things that they have not have the time to state already or points or messages they would like to underline.

You can also ask if something has made a special impression during the conversation.

Annex 5

Transcripts of group interviews

Group 1	page 60
Group 2	page 81
Group 3	page 95
Group 4	page 111

Underlined sentences are used as quotas in the report.

Gruppe 1

Og så er det bare for dere å forskyne dere med brus og kaffe. Underveis kan dere også gå ut og hente litt, så det. For å komme i gang med diskusjonen så kan vi bare ta en liten runde. Hvem vi er og litt hvorfor vi er her. Vi kan begynne med deg

Jeg heter Kirsten. Jeg er daglig leder og frisør. Hvorfor jeg er her, det kunne vært litt spennende å høre litt forskjellig om forskjellige typer teknologi der er og sikkerhetsteknologi.

Pål Karr. It-konsulten, jobber for Cap Gemini, jeg jobber endel blant annet med datasikkerhet, og kommer jo borti personvern og sikkerhet i den sammenheng.

Mitt navn er Jan Inge Hjelmås. Hyggelig å bli invitert. Hvorfor jeg er her, det er fordi jeg har fått lov til å være her. Jeg synest temaet er interessant og som min nabo, som jobber innen it – IBM. Synes dette har vært veldig interessant.

Jeg heter Svein Bjur. Jeg er tegner og illustratør, jobber også i Posten. Det er noe jeg tenker på, når man jobber i Posten, det er personvern der også. Det var litt gøy å få en invitasjon, så jeg synes det var interessant å være med.

Og du har vært ute å snakket skjønner jeg?

Jeg har snakket med Aftenposten. Jeg heter Unni Evenes, jeg har jobba med regnskap og lønn i godt over 30 år. Nå har jeg unnet meg for en gangs skyld et friår. I løpet av det året har jeg sittet veldig mye på internett, og har satt meg inn i det på en annen måte en på jobben.

Jeg heter Arnhild Heim. Jeg jobber som tekniker innen bygg, har gjort det siste fem året. Fagområde som Einar. Og ble litt interessert i dette i og med at du setter endel elektroniske spor i løpet av en arbeidsdag og at du har kommunikasjon med store flatesoner (?) Synes det er litt spennende.

Jeg er da altså Kari og skal snakke med dere. Deres umiddelbare om tanker om sikkerhetsteknologi og personvern, jeg vet ikke om vi skal ta en runde med dette og hva dere er spesielt opptatt av?

Sånn umiddelbart tenker jeg sånn positivt. Men det er helt til jeg setter meg inn i hva teknologi der er, og hvilke spor man setter igjen. Så, når jeg leser disse scenariene, så blir jeg litt sånn «åh – hjelp». Da så jeg at du ikke var anonym lenger, hvis alt dette kommer på bane. Da ble jeg litt mer betenkt egentlig over det. På mange måter, både positivt og negativt.

Det som var en ny tanke for meg, det var at – ehm – jeg vet jo hvor lett det er å finne disse sporene. Jeg har jobbet endel med det, og vet at du setter spor overalt. Jeg tror nok selv om vi har de beste tanker om hvordan du skal bruke dataene, så vet du ikke hva du skal bruke det til i fremtiden. Så kommer det en eller annen gang til å bli misbrukt, helt garantert. Dette misbruket som vi ikke vet om, det er det eneste jeg er redd for.

For å begynne der han slapp, så er det det jeg er mest opptatt av. Hvordan disse dataene blir forvalta og hvem som får tilgang til dem, det er det viktigste. Jeg har ikke noe imot at det blir gjort innsamling av data. Jeg har ikke noe mot hvis det samles enda mer, hvis målet er å forhindre kriminalitet og terrrorisme. Og den type ting. Med det at det kun autoriserte

personell som må få tilgang til dette, ikke at hvem som helst kan ha det morro og se hvem som var på byen forrige helg. Det skal kun brukes for politiet og hvis det er mistanker. (5:10)

I utgangspunktet så tenker jeg som så at jeg ikke har tenkt å gjøre noe gærent. Det er slik vi alle tenker. Det er samme søren hvor mange overvåkningskamera det er og spor vi legger igjen. Men likevel er det noe som streiker i meg. Fordi at det du sier med hensyn til politiet og at de skal få tilgang – jeg er ikke så glad i politiet og stoler ikke helt på dem. Det er et eller annet som skjærer seg i meg når det gjelder sånn teknologi. Når Gud og hvermann sitter å ser i kamera og sitter og ser i Kirkegata at der er det noen som går han, og så videre. Hvem er han? Og hvem er i politiet? Det er endel folk i politiet, jeg får det ikke til å stemme, det streiker i meg. Så, det var foreløpig det ihvertfall.

Ja, jeg synes dette er veldig interessant og det er derfor jeg hadde lyst å være med. Jeg er i utgangspunktet, som jeg sa til Aftenposte og, veldig positiv, ut i fra den tankegang at vi alle (bråk i mikrofon) vi har ingenting å skjule. Jeg har ikke følt meg tråkket på tærne, for jeg tror ikke det blir misbrukt, i utgangspunktet. (bakgrunnsbråk) Vi må se saken i forhold til de vi vil ha tatt, og det er terrorister og folk som driver på med narkotika, ikke minst hvis vi kunne fått bedre kontroll på det, som ødelegger enormt mye for samfunnet, og endel andre kriminelle ting som vi kunne gjort noe med. Når vi vet at vi bor i Norge i dag føler jeg meg såpass trygg på at det ikke kan bli misbrukt. Jeg diskuterte med han andre i stad. Jeg synes faktisk det er mye mer plagsomt for privatlivet å bli nedring av telefonselgere. Får jeg mange eposter så sletter jeg dem bare. Men en telefon som ringer irriterer meg vanvittig. Vi har satt oss på liste for at vi ikke vil ha telefonsalg. Men de ringer hele veien.

Anonyme telefoner. Ja, «hehe». Beste vennina mi er fra østlandet, «haha», (uforståelig)

Har du noe du mener?

Nei, jeg ble satt ut. (uforståelig) hovedsakelig sånn som det blir nevnt her. Du samler endel informasjon og det skal brukes, i kontrollerte former. Og så er det da med denne autoriseringen og klareringen av disse personene som skal bruke denne og lagrings-ting og sånt noe som du kommer inn på i jobbsammenheng. Med lagring av forskjellige data. Det er litt sånn at ting kan brukes og misbrukes, men altså vi er mennesker. Det er litt spesielt å sette opp et scenario som dette.

Hvor lenge blir forskjellige data lagret? Da tenker jeg på mobiltelefon, kort, sånn brikke, når du kjøper.

Til disken er full (latter).

Noe er det restriksjoner på vet jeg, for eksempel data om passeringer i bomringer lagres i to år. Men det klager Datatilsynet på, for de mener at det bør slettes med en gang regningen er betalt.

Helt enig.

Men andre ting. Siden du nevnte det, gis det begrunnelse for at det lagres i to år?

Her er en fotograf fra oss. (bråk) Gis det begrunnelsen? Det er vel mer en sedvane enn et velbegrunnet tall.

Jeg synes det er veldig greit de spørsmålene med hensyn til om du er villig til at politiet kan med rettsbekjennelse – og så videre. Fordi at da har ikke den politienheten i et oppheta miljø – som det sikkert kan være innenfor politiet, og de må gjøre sånn og sånn for å få tatt han fyren der. Da må det gå litt tid før de får det på bane og det med sikkerheten blir sett litt utenfra. (samtykke fra andre) Så det synes jeg er en grei måte å vinkle den greia på.

Men det er jo litt avhengig av hvor lang tid det tar å få den rettskjennelsen. Hvis det kan ta en uke er det gjerne litt for sent. Da er vedkommende ute av landet. Så er jeg ikke (uklart) Hvis politiet mener, når jeg sier politiet er det som regel en med juridisk kompetanse som kommer med det utsagnet.

(flere prater i munnen)

Da bør det være mulig å få rettskjennelsen «nesten sånn».

Hva menes med rettskjennelse? Da er saken på tinghuset? Eller er det, sant?

Du vet ikke hva. Hvis du ser, bare for å dra det til noe vi alle kjenner til, dette med politi i sivil. Når du tar veldig kjappe avgjørelser, og du brekker etter folk som må gjøre – ja, du har jo dødsfall på grunn av dette der. Så hvor, hvem er det som tar avgjørelsen der? En sånn en patrulje kunne stoppa det mennesket foran, og ikke at man kjører etter han. Altså, sånn ting mener jeg er hastegreier. (?)

Dette med sikkerhet, du vil jo finne folk som misbruker sitt verv og sin tillit, i misbruk eller tillit til autoritet. Du finner det overalt, og du finner det i rettssystemet og. Jeg går ut fra at du skal ha rettskjennelse for å etterforske videre på noe så er det ikke en person som bestemmer det. Det er snakk om å sette ned en gruppe eller en kommisjon, slik at flere personer bestemmer at «okey», her er det klare beviser. «da kan vi kjøre saken videre»

Jo, men da går det over lenger tid.

Unnskyld, hvis jeg kan få arrangere litt. Hvis vi kan sette oss litt nærmere hverandre. (bråk)

Før vi går over til scenariene dere har lest, vi formidlet positive og negative konsekvenser ved ny teknologi. Har dere noen kommentarer på balansen i scenariene? Synes dere det er balansert i den ene eller andre retningen i forhold til hva dere ser for dere fremtiden?

Jeg føler den er litt (uforståelig)

Ja, i hvilken retning da?

Ja, for å fremme teknologien, altså fremme større sikkerhet og mer aksept for ny teknologi. Føler jeg denne er lagt opp til.

Så du synes det er greit?

Nei, jeg føler at den er lagt opp til at man skal gli inn i et ståsted hvor det er større aksept. Jeg synes den er litt forledende rett og slett.

Jeg synes det motsatte. «javel?»

Jeg føler at det ble satt veldig opp mot hverandre, de to. At hun var veldig for, og at han var veldig skeptisk.

Men du synes allikvel at det var for .... ?

Jeg synes det var «pro-personvern» sånn som jeg leste det. Men dette er måten jeg leser det på. Det var ikke noe sterkt ene veien, det var det ikke.

Det var en ting som var litt skremmende synes jeg. Det var han som var ute og skulle på bilmesse, som hadde kjøpt seg det som heter «Fast-track». Da begynte jeg med en gang og tenkte at hvis du kan kjøpe deg ut av dette, så mister det jo litt av hensikten. Da kan man altså kjøpe seg ut av køen og da er det den menige mann som blir taperen. Det var en farlig tankegang i det scenariet der.

Jo, men, det var ikke sånn at med Fast-track så hadde man ganske mye informasjon, og at dette var en av forutsetningene for å få Fast-track.

Jo, men jeg synes, hva pris setter du på det? Hvis du sier at det blir aktuelt, da sier du at det blir «sånn skikkelig» ...

Da sier du jo samtidig at de som har mye penger ikke er terrorister da? (prater i munnen på hverandre)

Alle med gullkort skal foran. (latter)

Men altså, dette kan jo også bli sett på som en fordel, at du slipper å stå i kø og det er jo andre fordeler her som blir beskrevet. Er det noen av de fordelen som dere ikke har i dag, som synes virkelig greier?

Fordeler med?

Med sikkerhetsteknolog? Altså Fast-track er jo en fordel, du vil jo kunne slippe å stå i kø. Men så har du jo en ulempe også, det er ikke det. Et annet eksempel som på en måte er en fordel, er jo det med (bråk) «i-call i» (bråk og latter). Greie fotobilder.

Ja, det går jo på dette med personvern dette. Altså, du kan jo bli sporet per i dag. Spiller det så mye rolle om du får enda mer?

Altså, hvis jeg setter det på spissen, sånn som jeg tenker. Så kunne jeg godt funnet meg i både det ene og det andre. Hvis vi må ta tak i ting vi er virkelig ute etter.

Men så har du jo de som vi virkelig er ute etter, de ligger jo ofte et skritt foran oss uansett. Sant? Det jeg har inntrykk av er at det blir den meninge mann som ikke gjør noe galt som trekker det korteste strået. For de ligger hele veien litt foran. Og jeg er ikke så veldig begeistret for det at jeg skal gå gjennom alt mulig for at jeg skal komme meg ombord på et fly. Jeg synes det er kjempegreit å ha sikkerhetskontroll, og jeg vet jeg føler meg trygg. Men jeg har ikke vært villig til å gi fra meg fingeravtrykk og alt mulig altså. Da vet du jo ikke hvordan det blir brukt, hvor lenge det blir lagret, om det blir misbrukt, sant? (16:45)

Det hadde man konfiskert for lenge siden. Jeg tror ikke noe mer, altså, før, det første du gjorde når du reiste til syden var å klaske passet ditt på disken, og da hadde de det der også. (samtykke fra andre) Ja, der er jo fødselsnummer og personnummer. Og du har din identitet. Om du verifiserer med tommelen eller passet eller ... ?

Men holder ikke det da?

Men passet ditt melder du stjålet. Men hva gjør du med fingeren? Så da kan du jo, altså, jeg mener det ikke så grovt. Men fingeravtrykkene dine. (blir avbrutt)

De kan lage falske pass? De gamle passene ble forfalsket ja? Det er det du risikerer.

Ja – men, på film så klipper de av fingrene! (latter)

Jeg mener det ikke så bokstavelig, men altså, hvis de får tak i fingeravtrykket ditt – du kan jo ikke melde fingeren din stjålet. Altså, jeg synes det er verre med slike ting. For meg er det det.

Altså, sånn som du nevner, hvis du er en forbryter, så vil du jo virkelig gjøre noe galt.

Altså, du sier det, så betyr det at ikke at sikkerhetskontrollen på flyplassen vil forhindre at fly faller ned?

«nei» (samtykke fra flere)

Den kunne altså ikke vært der i det hele tatt?

Det gjør det jo vanskeligere, det gjør det jo.

Jeg forstår ikke hvorfor du skal identifisere deg når du skal ombord i et fly i det hele tatt. Du gjør ikke det når du tar buss eller trikk.

Du trenger ikke identifisere deg, det viktigste er jo at du ikke har med deg noen farlige gjenstander eller noe som...

Du kan gjøre et på et tog. Jeg forstår ikke helt. Det er jo psykologisk, fordi det har skjedd et eller annet.

Det er litt farligere med fly da. (prater i munner på hverandre)

Kjører du et TGV-tog i 300 km/t inn i en stasjon, så får du jo.

Det kunne jo vært litt sikkerhetskontroll der og.

Ja, men, det er det også.

Å, herregud, da må det jo være på busser og trikker og overalt. (latter fra de andre) Da stopper jo hele verden! Da må vi bare være hjemme. (latter)

Vi blir så paranoide hele gjengen altså!

Uansett så er det viktig som hun sier at disse terroristene og hackerene, de kommer til, det kommer de alltid til å gjøre. Og det som er viktig er det at vi følger med. Og så gjør det vanskeligere for de. Sånn at det ikke blir for lett for de å gjøre ...

Men kanskje måten å gjøre det vanskelig for dem – er ikke overvåking. Sånn elektronisk overvåkning, kanskje andre metoder? Sånn at man kan gå tilbake til den gamle gode måten med infiltrering og sånne ting, av mennesker?

Jeg er litt enig, det kan jo gjøres andre veien og. Gjennom informasjon og tilrettelegging, sånn for eksempel, «et skudd i helt annen retning» - på skoler har de jo slike anti-mobbe kampanjer. For å bedre hverdagen til ungene, så kanskje man må tenke i den retningen, at man må forebygge litt på et tidligere tidspunkt slik at folk ikke blir så stygge med hverandre.

Det er så mye enklere med overvåking, for da kan man automatisere alt sammen. Da gjør de det i stedet.

Jeg ser på denne nye teknologien som («herleich» ?? uforståelig dialekt), det er jo ikke dermed sagt at det bare er ny teknologi. Folk må jo jobbe på gamle måter, det er jo en kombinasjon. Det er jo ikke sånn science-fiction at det bare er roboter og datamskiner som sitter.

Men, tror du det blir sånn at det sitter folk som finner opp alle disse greiene her? Det kommer stadig vekk nye ting. Det blir mer og mer avansert. Tror du det bare blir sånn at myndighetene nikker og sier «jaha» hver gang det er noe nytt og godtar etterhvert som det kommer? Er det det som blir greia, tro?

Folkene som sitter på toppen, de skal jo ha kontroll. Klart at de sier ja til ting som kan hjelpe dem å kontrollere andre. Det var jo litt sterkt sagt...

Så er det det at personvern også går på at du ikke skal *føle* at du blir kontrollert. Synes jeg i alle fall. Jeg vil ikke føle meg kontrollert hele veien. Jeg har lyst å ha litt frihet.

Ja, men, du vil ikke føle deg kontrollert, for det er så skjult at du ikke merker det engang. (snakking i munnen på hverandre) Ja – jeg synes det er ganske skummelt også.

Hvor langt skal det gå?

Ja, hvor langt skal det gå uten at vi snart ikke kan få lov til å gå på do engang?

(flere stemmer, uklart)

Du har jo ingen kontroll at dette vil fungere. Det er jo det som er skremmende synes jeg da. Med disse sikkerhetstiltakene og sånn. At det misbrukes, altså misbruket som kommer inn i dette.

Ja, det er jo det vi har snakket om, det er det jeg og mener, at jeg vil føle meg så kontrollert at jeg vil aldri egentlig vite om jeg har noen bak som vil misbruke dette.

(flere stemmer uklart)

... at de kan gå inn og ta din identitet og forandre dine spor slik at du plutselig blir en kriminell uten å ha gjort noe.

Jeg tenker på – hvis vi prøver, for nå er det ... men – altså, ser dere at det er noen positive sider ved sikkerhetsteknologi i det hele tatt?

Å ja, haugevis. (latter) Det er det som er problemet! Det er jo masse fordeler ved det, det er det som er problemet, at du kan lett automatisere alt. Og du kan jo bekjempe kriminalitet veldig bra med det. Men det er ikke nødvendigvis den mest fornuftige måten å gjøre det på, fordi at det går ut over uskylde også.

Men er det noen ting som du ser kan være positivt for *deg*, ut fra det verdisettet du har i dag?

Altså, positivt, hvis du har komplett overvåkning så er det ikke noen kriminalitet lenger. Det er jo veldig positivt for meg det. Så det – men – jeg ville ikke hatt det.

Det er jo greit å vite at det er ingen som ser på deg når du legger deg i senga di og ser på mens du sover

– eller gjør andre ting (latter)

Det som også er viktig er at vi vet jo at mange av disse kriminelle sakene som blir oppklart på mye kortere tid enn det vil ellers ha tatt, saker som kanskje ikke har blitt oppklart i det hele tatt hvis vi ikke har hatt teknologi som vi har i dag. Det er jo positivt for oss. For det er klart at når kriminelle ting blir oppklart fortere, så er det litt mer skremmende for andre som har planer om å gjøre tilsvarende ting. Så det blir en preventiv effekt.

Men så hender det da ofte at det blir dratt inn uskyldige. Det er jo også dumt.

Det er jo ikke så ofte...

- jo, det skjer. Titt og ofte er det overskrifter i avisen om akkurat det, at nå har det «tatt den» og så sitter den så og så lenge, og så, plutselig, nei, det var ikke den likevel. Så sier de beklager, og så er det en fot ut til han.

Det skjedde jo før de hadde teknologi også, for å si det sånn. Det burde forhindres. Hvis du blir dømt og alt dette her, så er det ikke så mye å stå innefor heller, men det er en helt annen ting enn å bli dømt og komme ut igjen og gjøre nye kriminelle handlinger. Så sånn sett, så skulle det gjerne vært sånn at vi har fått lov til å *merket de* rett og slett. At «hallo, han skal vi få lov til å følge hele veien» , for han har fått en dom. Og da blir det enda verre hvis han ikke har gjort det.

Jeg pleide å tenke det at DNA er jo ideelt. La oss ha et register over alle mennesker her på kloden med deres DNA. Skjer det en forbrytelse og du mister en dråpe blod eller hva det skulle være, så vet du hvem det er. For du har registeret.

Men, kan vi gå så langt som vi gjorde med bikkja mi? At vi sprøyta inn en chip «inni her», ikke sant? Hun blir scanna hele tia.

Det hadde vært flott. Hvis du er uheldig og ikke finner frem i verden, «er det bare å ringe». Så hvis noen finner din passkode eller din kode, så vet du nøyaktig om du er på jobb eller på (uklart). Ser på flystevne eller går på pub.

Jeg synes det er viktig at det er en form for overvåkning, noe må det være. Men det må være for et bestemt formål, som er et bra formål, som er et fornuftig formål. Og så må du overvåke de som overvåker.

Ja, det er viktig (flere samtykker) Hvis du ikke overvåker de, blir det misbrukt. Makt korrumperer, og det skjer uansett.

Men altså, det som helt klart er realiteten er at, som du sier, at man har overvåkning og det har man alltid hatt. Så det vil man alltid ha. Og den nye teknologien er jo kommet. Så den blir jo til en viss grad tatt i bruk. Spørsmålet er jo mere hvilke typer teknologi og løsninger som er akseptable. Og er det noen av de som vi har snakket om i dag, når dere leser scenariene, når dere ser - «okey, dette er greit». Kan dere komme på noen eksempler på det?

Jeg kan komme på ett som ikke som ikke var greit, da fikk ihvertfall jeg frysninger på ryggen. Det var det eCall hvor det utvikles slik at de kan sitte å trekke fartsbøter av deg hele veien.

Det synes du ikke var greit?

Nei, det synes jeg ikke var greit (latter).

Jeg er enig, med faktisk, eCall i rette sammenheng er veldig bra synes jeg. (flere snakker samtidig)
Jeg følte det nesten var skrevet litt på spøk, men det verste var at det kunne brukes til at du blir via GPS fulgt hele veien med om du overskrider fartsgrensen. Og da var de kommet så langt at de bare trakk fartsbøtene av kontoen.

Men, hva er forskjellen med det og ferdskriverene da? Der har du jo akkurat samme dilemmaet.

Nei, men du kan jo bli tatt uansett. Altså, kjører du i 90 i 80-sonen, så vet dem det. (flere snakker samtidig, raskt, på uforståelig dialekt)

Hvis de mistenker en som kjører langtransport for at han ikke har overholdt hviletidene sine og fartsgrensa, så kan de gå inn på ferdskriveren og fakke han for det.

Ja, men nå sitter en politimann og overvåker. Så ser han «oi, han kjører litt for fort, oi, det var den boten!» (latter)

Jeg tror ikke det er realiteten i det hele tatt. (uklart) så stod de jo nå i pinsen og skuflet folk for å få de til å kjøre fortere bare for å holde flyt i trafikken. Så du har begge sider av akkurat det der.

Altså, en viktig ting med eCall er at hvis det har skjedd en ulykke vil du få oppgitt at det har skjedd og nøyaktig posisjon.

Jeg synes det er veldig positivt faktisk. Faktisk den mest positive overvåkningsbiten jeg kjenner.

Så kommer neste da, så skal forsikringsselskapet vite hvem som var uaktsom. Ikke sant, «kjørte du i 90?», «prøvde du bremsa?», «ga du gass?», «prøvde du å svinge unna?» Sant, det er jo spørsmål om *hvor mye* informasjon du skal få legge inn i den da.

Det burde du kunne få bestemme selv synes jeg.

Det som er dumt er at du så må betale premie der etter da. Og det kommer forsikringsselskapene til å gjøre.

Ja, forsikringsselskapene skal jo ikke ha tilgang til sånt noe *i det hele tatt!* Da er du ute på ville veier da! (flere snakker samtidig)

Hva var det hun het så fint. Det registeret på innvandrerene. På asylmotakene, så var det jo et register som tidligere ble brukt på (uklart), som nå plutselig ble åpent for politiet, slik at de kunne få lov til å lete i de arkivene for å finne.

Det er jo det som skjer hele veien (avbrytes)

Og det er jo det man har med lagringstid og sånt noe. Hvem skal bestemme og hvorfor det skal være, for eksempel som du sier, med passeringene. Hvorfor skal det lagres i to år? Har det noen unnskyldning for å lagres i to år? Det er det jeg mener, det er akkurat som at de ikke kan komme med noen god argumentasjon for at de skal lagre ting som ikke skulle fått lov til å bli lagra.

Nå ser jeg at Kristine sitter her, og jeg lurer på om du skal akkurat si litt om dette og hva som skjer?

Vet du om det? Jeg har et spørsmål. Jeg barer lurer på dette med status med dette med lagring av data.

Altså, datalagringsdirektiver?
Ja, hvordan det praktiseres i Norge i dag? Jeg har fortalt dem, du må bare si hvis det er feil, at bomringpasseringer lagres i to år.

Det aner jeg ingenting om, nei, det tror jeg ikke er riktig. Det som er regelen i Norge i dag, er at du har ikke har lov til å lagre data lenger enn det du trenger for å gjøre noe praktisk, altså, foreksempel å sende en faktura. Sånn at, Telenor, teleselskapene har lov til å lagre i forhold til de abbonementene de tilbyr, så det er mellom tre og fem måneder tror jeg. Bomselskapene er jo tilsvarende, det kommer an på hvilken type abbonement du har. Hvis de har en klagesak gående så kan de lagre det til den saken er avsluttet. Men det du har sagt om to år er jo det datalagringsdirektivet som EU har foreslått. Det dreier seg om bare om teledata. Fasttelefoni. Mobiltelefoni. Nettbruk. Der er det foreslått at man skal lagre nummeret som ringer og hvem de ringer til, hvis det er mobiltelefoni, hvor de befinner seg og hvilken basestasjon de henger på, hvor lenge de snakker, og en del sånne ting. Hvis det er internett, så er det hvor de, hvilken IP-adresse de har når pcen logger seg på, og litt sånne ting.

Hvorfor det?

Det er fordi at politiet skal i etteforskning ha litt mere data og søke i. Det har litt bakgrunn i disse Madrid-bombene, der var jo endel av, en ganske viktig grunn til at de oppklarte det var bruk av mobiltelefoner, sånn nummer. Vi fikk opp litt sånn som at når noen har lagt ei bombe i skoen på flyplassen.

Det var jo ramaskrik om dette her. Fordi det skulle være påbudt for teleoperatøren å skulle lagre dataen så lenge, og det kosta jo en formue.

Det har vært mye diskusjon om det. Som EU har foreslått, er at det skal være minimum 6 måneders, som bare er *litt* lengre enn hva mange operatører lagrer i dag. Men de lagrer nok ikke så mye data på internett som det som blir pålagt i direktivet, fordi det er jo veldig få som ringer til internett på nytt hver gang de skal logge på. Når de betalte så betalte de for å ringe et spesielt nummer og de betalte for den tia de satt på internett. I dag er det veldig få som har den typen abbonement. I og med at de må lagre det de trenger for å fakturere, så trenger de ikke så mye informasjon lenger. Men politiet bruker jo denne typen data i forhold til etterforskning, både for å finne ut hvem som har vært hvor på internett, for eksempel i Baneheia-saken, så var det jo dette med om han kunne ha vært der, selv om han hadde vært i kontakt med en annen basestasjon og dette var en viktig del av bevisførselen. Så det brukes til sånne ting. Og EU har satt minimum 6 måneder, maksimum 2 år. Det er jo interessant, for da har du noen land som protesterer fordi teleopratørene protesterer for det er dyrt hvis de må betale kostnadene selv. De (uklart) Og så har du andre land som hadde innført mye lenger, Italia for eksempel, hadde innført fem år, så de protesterer fordi de ikke får lov til å lagre så lenge som de vil. Og hvis de da tar det inn, så må de følge det.

Men – mobiltelefoner i dag brukes nesten ikke til å ringe lenger. (uklart) Hva blir lagret av det du bruker telefonen til? Er det bare ringing, sms eller, altså?

Altså, hvis du bruker kalenderen din for eksempel? (snakker i munnen på hverandre)

Neinei, det er jo mange som bruker telefonen som en data.

Nei, det er bare når man er i kontakt med nettverket, når du ringer opp ett eller annet nummer, eller kobler opp deg på ett eller annet hvis, altså en tjeneste som krever at du bruker teleoperatør.

Ja, altså sånn som SMS og MMS og sånt noe også? Blir det og lagret? På lik linje med en ... (uklart)

Etterhvert kommer alt på nettet til å bli lagret uansett (latter)

Alle ganger du på en måte bruker nettverket, kobler deg opp, ringer opp noen, sender noen noe, så blir det lagret da fra hvilken mobil som gjorde det, hvem det gikk til.

(uklart – spørsmål til Kristine)

Direktivet er - Det er noen EU-land som har protestert på det. Irland, og – nå husker jeg ikke alt de andre. Men jeg tror det skal behandles i Stortinget til høsten, så det er ikke så langt unna i Norge altså. Ja, og vi pleier å være veldig kjappe med å innføre nye direktiver, og vi pleier aldri å ikke innføre et direktiv (latter)

«annerledes-landet» (latter)

Det har allerede vært litt diskusjon på Stortinget i tilknytning til behandling av Stortingsmelding av IKT. Der var det litt om personvern og da var det noen partier som ønsket at Stortinget skulle anbefale at regjeringen gikk inn for at Norge skulle lagre i seks måneder, som er den minste mulige tiden. Det ble ikke flertall for at de skulle anbefale noe annet, men det ble ikke flertall for at de skulle anbefale det.

Så det er fremdeles ganske åpent i Norge da. Men Datatilsynet for eksempel, har jo vært ganske klare i sin anbefaling om at vi ikke bør gå lengre enn seks måneder. Jeg tror ikke politiet har fremsatt noe krav om at de ønsker lenger lagringstid. Sånn som politiet vi hadde i vår gruppe sa, så er det ganske ferskt, veldig ofte når de trenger ting så er det det nylig ting har skjedd, eller så er det veldig gammelt og da vil det uansett være vekk. Det er ikke ofte politikere (uklart – latter)

Det er i grunn det som bør styre lagringstiden, det er ikke det vi sier, gamle data har politiet hatt behov for. Hvis de har hatt behov for data som var ett år gammelt, så kanskje...

Så er det, hvor ofte har de behov for det (uklart)

Det er det som bør trekke, for vi har jo ingen grunnlag (uklart)

En av de tingene som datatilsynet har vært opptatt av er jo og, altså, hva det tiltaket er viktig for at forbrytelse blir oppklart eller var det bare et bidrag. Det er jo mange ting som kan spille inn.

Datatilsynet har faktisk bedt om å få tall på det. For det fins ikke noe data på det. Hvor gamle data har politiet bedt om gjennom. De har bedt Telenor om å oppgi hvor mange henvendelser de har fått. Det sliter de visst med å få fram.

Bør kanskje spore politiet litt mer så kan vi finne det ut.

Ja, de bør kanskje gjøre litt oppgjør for seg selv (latter)

(opphold)

Ja, har dere tiltro nå til at politikerene vedtar datalagring, en fornuftig datalagring?

Nei, absolutt ikke.

Jeg har jo *blå øyer* jeg, de kunne lagret hva de ville for min del, hvis det kunne vunnet fram i kampen mot terrorisme og narkotika. Jeg kan ikke skjønne per i dag, hvordan data kan misbrukes på noen som helst måte. Og hvis da, på en eller annen måte, det kom fram noe som viste at noe kunne misbrukes, så mener jeg at vi er så demokratisk, ihvertfall per i dag, at Norge, at det måtte kunne gått an å korrigert seg, justert seg inn på noen måte. Vi bor jo ikke i noen politistat.

Altså, terrorisme er ikke noe problem i Norge i dag. Det største problemet i Norge i dag er vel trafikkulykker og hjerteinnfarkt. Vi kan overvåke for å hjelpe til på trafikkulykker, og vi kan også hjelpe hjerteinfarkt, å tracke hvor folk er. Så, sånne ting er det vi kunne fokusert på.

Ja, så mener jeg, hvis nye teknologier kan hjelpe politiet mot kriminalitet, ikke minst narkotika, som tross alt ødelegger så mange ungdommer.

Så det du sier, er at du vil ha et fullstendig overvåka samfunn altså. Nei, i prinsippet, det som jeg ser for meg i dag, i mine øyner, så kan ikke jeg skjønnet at de sporene jeg legger igjen etter meg, de er uinteressante, og for de fleste så er det jo helt uinteressante spor, hvem du har ringt og hva du har gjort. Det er derfor jeg sa, jeg blir litt forspøka(?), for den jeg likte minst er den hvor du heile veien, si, du kjører på hytta, det er ikke en bil og du vurderer situasjonen frem, altså, det verste scenarioet var jo det at dette vil gjøre at det kommer en melding fra GPS til et bøteregister når du kjører i 90 når det er bare 80 der. Det synes jeg er å trå inn i mitt privatliv

Det synes jeg er ubehagelig (uklart) hvis du har vært inn i en butikk og kjøpt en vare. Så tar du den magneten. Så er det «du, der, bli med her, så skal vi fikse det». Du er jo ikke særlig. Der er det også denne overvåkningen da hvor det rammer en uskyldig og så har du betalt for varen, så kan du likevel liksom føle at du (uklart)

Har du sett når folk stjeler klær?

Nei, altså, men du føler jo uansett, hvis du da går forbi og du enda har en alarm i posen med klærne dine at «oi». Eller hvis du mot formodning kommer hjem, uten at du har utløst en alarm og skal tilbake i butikken si at «du glemte å ta alarmen».

Eneste som ikke tar ikke blir tatt er den enkelt-tyven, for han har enten fjerna alarmen eller tatt et plagg uten alarm på. Det er det jeg sier, om overvåkning

Men altså, lagring av data i seks måneder. Vi er jo et demokrati og vi vil jo sannsynligvis ikke i løpet av seks måneder bli noen politistat. Er det noe problem da? Er det noen data som ikke bør lagres? Du sa du ikke hadde tiltro til politikere?

Jeg har ikke tiltro til noen som får for mye makt. Og det har jo vist seg gang på gang i historien at får de for mye makt, så går det galt. Så selv om ikke datadirektivet sier mer enn seks måneder, så mener du at det er for mye eller for lenge?

Altså, jeg tror nok 6 måneder er fornuftig for formålet, så vil jeg akseptere det.

Jo, men kunne ikke det vært noe sånn at vi når vi tenker på terrorisme og kriminalitet generelt, kunne det ikke da vært mer hensyn til en rettsinstans som vurderte dette her, skal disse spesifikke data lagres lenger enn seks måneder? Det måtte jo være endel mennesker som hadde noe med akkurat det å gjøre.

(uklart)

I demokratiets ånd, ikke sant? Ellers så mener jeg det at det skulle vært lagra minst mulig altså.

Det har ingen hensikt, når jeg har fått telefonregninga mi og betalt den, hvorfor i huleste skal telefonselskapet ha mine samtaler liggende lagra da?

Ikke samtalene.

Nei, men informasjon, telefonnummer og alt det der. (uklart) det *gjør* ingenting, men det gjør noe med den frihet (uklart, mye snakking)

Politiet? Interessert? De er er ikke interessert i å se hvem du har ringt til. Det er ingen som har tid til det engang. Det er ingen som vil gå inn og si ... det hjelper jo ikke.

Det vil alltid være mennesker som misbruker sånne ting.

Hvis du har muligheten til overvåkning og sånn. Du hadde jo et tilfelle nå nettopp hvor det var en som hadde overvåka ekskjæresten sin i flere måneder med video og lyd og alt. Hva klarer ikke denne mannen? Altså, her ser du et tydelig overtramp på folks personvern og likevel så klarer man ikke å dømme denne personen. Det synes jeg er skremmende. Har vi lover som kan ivareta denne type overvåking?

Det klarer du ikke å forhindre, for den type utstyr er for salg. (uklart)

Men altså, du kan godt dømme folk som driver overtramp om de heter Nilsen eller Jensen eller hva de heter.

Du har bevis på det, kanskje? Jeg vet ikke.

Det burde du hatt. Alt som går ut over andre mennesker.

Men, når er sikkerhet viktigere enn personvern? Altså, på hvilke situasjoner og på hvilke steder, altså, i scenariene er det veldig fokusert på reising ikke sant, togstasjon, flyplass og så videre. Når er sikkerheten viktigere, når kan du være med på å oppgi noe av personvernet ditt for sikkerhetshensyn?

Spesifikke situasjoner tenker du på?

Ja, spesifikke situasjoner.

Jeg føler ihvertfall på fly, synes jeg det er helt greit med sikkerhet. Jeg føler meg tryggere når jeg vet at alle har gått gjennom.

Jeg føler meg ikke mer sikker på flyet, selv om jeg blir overvåket.

Du føler deg mindre sikker på grunn av? ...

Nei, jeg ser ikke noen effekt.

Det er gjerne ikke overvåking, men å gå gjennom en sikkerhetskontroll og sånne ting.

Men, de gjør det jo veldig mye vanskeligere for de som vil kapre flyet, at der er en sikkerhetskontroll. Det er jo en eller annen skrulling som er lei livet sitt og som gir blaffen og som tar seg en tur.

Du leser jo stadig vekk om folk som kommer med økser og våpen og alt mulig rart på flyet.

Har det ikke blitt mindre etter, jeg holdt på å si, de satte i gang så strenge sikkerhetstiltak?

Men ihvertfall så er jo sannsynligheten for å bli tatt er jo større hvis det er sikkerhetskontroller om det ikke er det.

Det går jo, det har jo allerede gått for lang. Når de tar og kontrollerer piloten og styrmann på flyet altså, da har det gått alt for langt. Som en venn sier til meg, han er pilot, «hvorfor skal dem kontrollere oss? Vi kunne kjørt flyet i bakken akkurat når vi vil? Vi skal ikke sitte å kutte oss i halsen med kniv, hva er vitsen?»

Det har gått alt for langt (flere samtykker)

Hvorfor nevne fly hele tiden? Jeg satt plutselig å tenke på teater og på kino. Du kontrolleres ikke når du går på kino. Du kan jo ha en bombe i lomma! Du kan være selvmordsbomber og «bang sier det» og så går det 150 stykker med en gang!

Egentlig så burde vi følt oss veldig usikre hver gang vi går på kino. (latter)

Butikken også! Det kan komme en med bombe i lomma i butikken og altså!

Altså, sikkerhet. Jeg kan gi mye av min person til sikkerhet, hvis jeg *vet* at det fungerer. Altså, at det beskytter meg mot kriminelle så kan jeg gi opp veldig mye. Men, hvis det skal være sånn at det beskytter de kriminelle, så er jeg ikke interessert i det.

Men hva skal til for at du vet at det fungerer?

Nei, det er jo det som er cluet da. Har vi noen garanti for at denne egentlig virker? Kanskje vi skal ha en innføringsperiode, slik som vi hadde med veiavgift, som ble innført over en periode?

Jeg vil tilbake til det jeg sa litt tidligere, med at, «hva er det vi skal beskytte oss mot?» Hva er den største, det er jo for å dø vi er mest redd for, ikke sant? Hva er størst sjanse for at vi dør av? Det er trafikkulykker eller hjerteinnfarkt eller den typen ting. Hvorfor i all verden sitter vi å sjekker mot terrorisme og sånt i Norge? Fordi at vi er redd for det. Det vi skal sjekke mot, er jo det som det er størst sjanse for.

Det var visst det i løpet av 2006, ihvertfall to store terroristaksjoner i Europa som ble forhindret.

Ja, sikkert.

Vi kan ikke sitte på haugen og si at det aldri skjer her. Det kan jo like godt skje her som alle andre plasser.

Risken er (uklart) sammenlignet med de andre tingene.

Hvis terroristene får vi at i Norge, «der er det ingen kontroll» som helst, så ville jeg følt meg mer utrygg altså. Norge må jo følge med på tilsvarende

Det er jo fremdeles bare å fly (flere bryter ut på en gang, uklart) Det er ikke (?) sikkerhetskontroller nedover Europa.

Hvis jeg var en terrorist og skulle ta Norge, så ville jeg tatt et cruiseskip og kjørt det inn i Ekkofisk. Det hører man ingen kontroller mot. Det har sikkert vært (uklart)

Nå har jeg ikke vært på noe cruiseskip, men det kan jo for alt jeg vet (uklart)

Jeg har vært mye på cruise og jeg synes det er utrolig topp, for den saks skyld. Men det er jo og betryggende, for det er jo utrolig sikkerhetskontroll. Du har jo bilde på kortet, og de sjekker mer bilde i boka, at du er registrert, sjekker hva (uklart – latter)

Vi var i Frankrike for noen år siden, og der hadde de kontroller inne på togstasjonen. Da må du gjennom kontroll. Jeg synes det var glimrende, det gjør meg ingenting å gå gjennom der. Alle, om du skulle inn og ut, så var det like mange kontroller alle veier. Synes det er helt greit jeg.

Det er jo passe mellom Norge og England med kontroller, på fly.

Det er greit hvis det øker sikkerheten.

Jo, det er jo det jeg mener, altså, hvis vi hadde fått det på togstasjonene her også, at man må gjennom en sånn piper for å komme inn på toget - «helt greit». Det trenger ikke nødvendigvis bare være et fly eller, det kan godt være på båt også.

Du kan jo ha det sånn at du kan ta en sånn nakenscanning når du skal på pub, sånn at puppene står ut.(latter) Nei, det trenger vi ikke.

Hva slags overvåkning skal vi ha da? Altså på flyplasser så kontroller de alt. Vi ser damer driver å kontrolleres (uklart – latter)

Hva slags kontroll skal vi ha når vi går på et tog. Skal vi blinke inn i et kamera?

Neineinei, ikke sånn. Når vi var i Frankrike, så var det sånn at du går gjennom en sånn scanner for at du ikke har våpen med deg eller sånne metalldupeditter. Altså, ikke personen, nei, det bryr jeg meg ikke om på sånne plasser. Men at du ikke kommer inn med en pistol eller en skarp kniv eller altså sånne ting. Slik at det piper når det er metall. Sånne ting tenker jeg på.

Men hvis du har dynamitt med så er det greit.

Da vet ikke jeg hvordan de skal scanne det. Har ikke peiling på hvordan det går gjennom. De har vel noe metall på det også?

Jeg tror ikke det. Er bare plastikk.

Problemet er at du kan aldri overvåke alt. Og så lenge du vet hva som blir overvåket, så tar ikke terroristen det med seg, han tar jo andre ting med seg. Så vi er like usikker.

Men, hva med kamera på gata, kamera i byen. De kan jo forhindre kriminalitet eller begrense.

Ja, men da forhindrer du akkurat der hvor kameraene er. Hvis folk vet hvor de er, så går de jo ikke der å begår forbrytelsen sin.

Nei, men da kan vi som regel føle en full trygghet, akkurat der som kameraene er.

Da må du stå der hele dagen da?

(uklart – mye prat på uforståelig dialekt) du har ihvertfall større sjanse for å ta gjerningsmannen. Du har jo ingen garanti for at du...

Du har jo ikke garanti for noen ting.

Men de som får, si, tatt et innbrudd et sted hvor det ikke er noe kamera, så må de jo som regel ihvertfall passere et kamera. Så sånn sett så, vil det forhindre ihvertfall.

Hvis vi beveger oss vekk fra – vi snakker så mye om flyplasser. Altså, store ansamlingssteder, sånn som på Vegårdshei (?), og jeg har tenkt på det når jeg har vært på nye Stavanger stadion på store konserter, og det har vært veldig mye folk. Litt sånn ubehagelig følelse av hva folk som er inne. Og, jeg vet ikke egentlig hvor mye de sjekker. Men når du ser til utlandet, på disse store fotballarenaene, så er det jo ikke tvil om at overvåkning har tatt disse hooliganene og. Og det er jo en ting som jeg tror de fleste vil ha vekk fra fotballen, det er jo rene rampen.

De er jo folk som har vært bedritne før. Som har vært filmet, tatt inn til avhør og fotograferte. Og da blir jo de gjenkjent når de kommer på nytt igjen.

De har jo overvåkningskamera på (uklart)

Alle må sjekkes når du går rundt på store stadion i utlandet. ... de har bevismateriale på folk som starter skikkelig bråk.

De tar dem faktisk på flyplassen på vei inn til der hvor de skal...

Da vi for eksempel var i Barcelona, så var vi en stor gjeng som skulle på hjemmekamp. Men vi fikk ikke kjøpe billetter sammen, vi måtte sitte hver for oss. Vi fikk maks sitte fire stykk samlet. Og det var jo veldig lukka. Du fikk ikke komme fra den ene cella til den andre uten at du gikk gjennom en kontrollpost, så akkurat sånne plasser så føler jeg at du er nokså sikker på større arenaer.

Og det er en fordel at sikkerhetsteknologi blir brukt til for eksempel ansiktsgjenkjenning? (samtykke)

Der har du en stor fordel. Men så har du jo sånn som (uklart, dialekt, kanskje lokalt stedsnavn). Men der føler jeg at jeg er utrygg. For der er store massesamlinger, så hvis noen

vil oss noe her, så er det bare (uklart ord igjen). Ikke sant? Altså, det er for stort. Det er for usikkert.

Altså, du går ikke dit fordi du føler deg usikker? Vil bruk av sikkerhetsteknologi der gjort at du?

(latter) Nei, jeg tror ikke. Men, altså, bare sånn i prinsippet.

Du vet at, det er for mye fokus på terrorisme om dagen. Siden 2001 så er det bare det som man er redd for. Det har jo ikke skjedd noe terrorisme i Norge enda. Hvorfor akkurat det? Overvåkning kan jo brukes til så mye annet.

Jeg huska før 11/9, hva var greia da? Og hvis du ser på nå, nå har jo da miljøet, du veit de C02-greiene blitt hausa opp slik at du hører ikke noe annet. Nå har vi (uklart)

Men, igjen, tilbake til realiteten, så må vi finne en balanse mellom sikkerhet og personvern. Hvem bør være med å bestemme når nye sikkerhetsteknologier skal tas i bruk?

De som blir rammet av det.

Jeg synes alle interesseorganisasjoner. Både de som er, til og med de som utvikler teknologien, som vet mulighetene og umulighetene. De som blir påvirket av det. De som skal bruke informasjonen. Som nevnt i skjemaet, menneskerettighetsorganisasjoner.

Jeg er ikke enig i at de som utvikler og lager disse overvåkningssystemene skal være med for mye å bestemme.

Nei, det er sant, de har en interesse i det, man skal være forsiktig med det.

Nei, for det er jo de som. Det må jo være andre instanser som mener at vi trenger noe sånn eller sånn. Kan dere lage noe sånt? Ikke sant? Og ikke det at de «hallo, *vi kan lage ting vi*».

De kan komme inn etterpå når de andre har bestemt at vi trenger overvåkning sånn og sånn.

De skal bare svare et behov.

Det er jo viktig å vite hva som er. Hva er det de holder på å utvikle, de store selskapene.

Det må jo være helt åpent. Mener jeg. Det er ikke godt å vite hva de utvikler, hva de jobber med.

Men, dere snakker om de som blir berørt. Det er folk da, sånn som oss? Hvordan kan vi?

Og hva de forventer vi skal bruke all den informasjonen til? Hva matnyttighet har denne informasjonen? Er det preventivt? Er det forebyggende? Er det noe nytte i den?

Men hvordan skal vi vite hva vi .. Er politikerene gode representanter?

Nei, det vil jeg ikke tro. Det er noen kanskje. Det går vel mer på tillit til kompetanse til de som sitter der. Jeg mener det må være behovsprøvd rett og slett, all overvåking.

Helt enig.

Yes (latter)

Det blir tatt opp (latter)

Men, så er det jo snakk om reguleringer som man på en eller annen måte må regulere. Eller er det kanskje noen som mener at det ikke trenger å være det? Bør det være begrensninger? Altså, type offentlige organer, type politi, bør de ha begrensninger, eller bør de kunne bruke det de mener de har bruk for å gjøre jobben sin?

I det offentlige rom så mener jeg det skal være skilting for overvåking.

Men, lov å overvåke så mye man vil, så lenge det er skiltet?

Ja, for du blir mer bevisstgjort.

Hva mener du med skiltet?

Sånn at man får beskjed når det kommer en fotoboks, eller at man får beskjed om at man blir fotografert. Men selvfølgelig, skjult overvåking i de tilfellene det er mistanke om kriminell handlinger. Da tenker jeg ikke nødvendigvis terror, men andre og. Det er masse rart kriminelt.

Jeg mener at du igjen så skaper, kan disse grupper, skape et behov.

Hva mener du med disse grupper?

Nei, jeg tenker på hvis politiet sier at de skal bruke den teknologien de ønsker i hvor stort omfang de bare vil? Jeg mener, politikerene, de dirigerer forsvaret, ikke sant? De militære, de får ikke lov til å gjøre akkurat som de vil. Men da mener jeg at politiet, av alle disse som driver med sikkerhet, skal få lov til å gjøre hva de vil heller. Det må være en begrensning, det må være noen som kan styre dette her.

De er underlagt jurister. Justisdepartementet.

Og de bør sette klare regler altså. Det var det du spurte om? (samtykke)

Men, så lenge den teknologien da oppklarer innbrudd, kriminalitet, terror tidligere, så synes jeg det er helt greit.

Nei, jeg synes ikke *uansett* altså, det gjør jeg ikke.

Som jeg sa i stad, hvis man har total overvåking kan du oppklare alle forbrytelser. Men du skal ikke ha *total*.

Hadde ikke det vært herlig?

Nei, det synes jeg ikke. Det hadde gått ut over så mye annet.

Det hadde blitt misbruk igjen. Du ser jo, da kan de jo arrangere. Du ser jo de Jackass-tilfellene hvor folk på nettet ser på dette på film og tror det er reelt og så blir det bank og så blir det bare tull og tøys. Sant, du har litt dette her med at dette noen ganger skjer, og så blir det en glipp, og så blir du kriminalisert, fordi at du var på feil sted på feil tidspunkt. Altså, det er faren med den totale overvåkingen. Og at folk kan stjele din identitet.

Total overvåking kan du ikke få noen gang.

Da er vi ikke mennesker engang.

Det ville vært umulig. Vi må bare finne de mest kritiske stedene for å si det sånn.

Det er det jeg og mener. At per i dag er Norge såpass gjennomsiktig at hvis vi er på ville veier må vi kunne klare å stoppe det i tide. Hvis den vanlige mann føler at dette blir ...

Hva skal vi gjøre med dette, du ser på disse mafia-tendensene. Hvordan skal vi overvåke (uklart). Det er noe som er veldig skjult. Det er jo veldig kriminelt. Hvordan skal vi få bukt med det? Det er der de store pengene ligger. Det er der det fosser ut på (uklart) og sånt noe.

Det er vel der man snakker om å overvåke for eksempel datatrafikk, mobiltelefontrafikk, data, bank, for å kunne fange opp nettopp.

Hvor lenge tror du bankene tror du bankene har oversikt over dine transaksjoner?
Forver...

Det er lenge det. De kan jo risikere at de må bevise noe.

Det vil jeg ikke at de skal ta. For jeg vil se det selv. Jeg vil gå i nettbanken min og se hva jeg gjorde for tre år siden. (samtykke) Jeg synes rent generelt at det er greit med overvåking av offentlige rom. Med det å ha kamera på torget synes jeg er greit. Men overvåking av privatsamtaler er ikke greit med mindre du har rettskjennelse eller en annen instans først.

Men da må du få bekrefta og at de er kriminell for at de i det hele tatt skal komme i søkelyse. Du må ha mistanke. Og det betyr at hvis du går på feil plass til feil tid så kan du bli overvåka.

Men betyr det at det er greit å gi fra seg biometrisk informasjon på en flyplass, fordi det er et offentlig rom?

Det er ikke overvåking, det er noe annet. (samtykke)

Det er greit at du kan gå igjennom og vise at du har betalt ting. Men hvorfor skal du identifiseres med irisen din eller biometriske ting og tang?

Du må jo det for å komme inn i USA for eksempel.

Det synes jeg er høl i hue.

Jeg liker ikke sånne ting, jeg kunne ikke tenkt meg å gi fra meg sånne.

Jeg kommer aldri til å reise til USA lenger jeg, nettopp på grunn av måten de håndterer dette. Jeg reiste mye til USA før.

Hvor langt har vi kommet i å mistenkeliggjøre folk da? Altså, hvorfor blir man mistenkeliggjort da? Da må du jo tenke hvilke årsaker og og kjenne på dette hvorfor folk ødelegger for andre da.

Risikoen ved at jeg, tenk hvis jeg reiser til USA. Hvis de scanner meg og finner ut at jeg har likhet med en eller annen terrorist, jeg kan risikere å ende opp på Guantanamo for resten av livet mitt. Det er jo helt vilt. Det er andre tilstander i Norge ihvertfall.

Da kan du jo bevise sannsynligvis at du har vært på andre steder til gitte tidspunkt. Da har du jo en fordel at det er lettere å bevise. At du var på torget i forrige uke. At du har brukt bankkortet ditt.

Hvis du kan stole på de du skal bevise det til da..

Det er det jeg synes er litt skummelt med fingeravtrykk og ansikt og alle sånne ting. Hvis du er uheldig, så (uklart) Men herre fred, du kan jo aldri vite hva de gjør, de kan jo kappe av deg fingeren (latter).

Fingeravtrykk overlater du deg overalt, så det kan hvem som helst stjele egentlig.

Men jeg synes det blir litt mer konsentrert når du legger det fra deg og det skal legges inn på.

Jeg synes du er inne på noe med det når du snakker om å kappe av fingeren, så råe kan de være. At, hvis du hadde hatt milliarder på bok, og folk visste det, kriminelle folk. De hadde ikke tatt fem øre for å klippe av deg fingeren og satt den på plass altså.
Fingeren må være levende for å lese av (mye prating, uklart)

Det skal visst være en varm finger.

Legg den i mikroen.

Det er absolutt et poeng dette med identitetstyveri i forhold til biometri er mye mer.

Det er vanskeligere å melde en finger stjålen (latter)

Bare ta en siste spørsmål. Tiden begynner å renne ut. Har deres holdninger til disse temaene endret seg gjennom deres deltagelse i dette prosjektet?

Nei (fra flere)

Vet du hva, jeg svarte nei jeg og, men sannsynligvis så har det det.

Jeg var i utgangspunktet som jeg sa, at jeg ikke brydde meg fordi jeg ikke har tenkt å gjøre noe gærent, men nå så har jeg steila litt altså. Har fått en aversjon mot utviklinga i teknologien.

Du sa dine også, i hvilken retning da?

Observerer du noen, så endrer du personen.

Tar du kontakt om en uke, så har vi gjerne sagt noe annet. Du har normalt sett ikke tre timer fokusering på dette emnet. Sammenhengen er vanligvis sånn, fem minutter. Så det er jo klart dette, vi har jo mye mer fokus på dette akkurat nå.

Det er jo i grunn uvanlig å fokusere så mye på ting vi ikke kan gjøre så mye med.

Teknologien går sin gang, så vi er nødt til å følge opp. Det som er viktig er at de blir godt kontrollert. Beste måten å sikre at de ikke blir misbrukt, har jeg ikke forusetninger for å si noe om. Det er jo det som er det mest kritiske da. Misbruk av data.

Ja, vi må sette klare regler for hva man har lov til å bruke ting til.

Men det må ikke være til hinder i en etterforskning da.

Jo – hvis reglen sier at det ikke skal brukes i en etterforskning, så skal den ikke det.

Det har jo, da er vi igjen tilbake til at du beskytter den kriminelle da.

Men da begynner du jo å tøye grensen igjen (latter, uklart, opptak slutt)

Gruppe 2

Da vi kanskje du begynne?

Jeg heter Tomas Rettvik, jeg går på Sandnes Allmenfaglig skole. Ligger rett oppi bakken her. Jeg er med fordi jeg er interessert i teknologi. Så da tenkte jeg at dette var jo en mulighet.

Mitt navn er Mette (uklart). Jeg jobber på Ressurshelsetjenesten på Sandnes som foreldreveileder. Og så har jeg barn selv i slutten av tenårene. Så jeg tenker at, og jeg er selv mye på nettet, så jeg tenker at jeg ønsker å få et mer bevisst forhold til det.

Jeg heter Kristin Sandal og jeg ble med fordi jeg synes det er veldig interessant. Jeg diskuterer den type ting både i jobbsammenheng og i privat sammenheng og synes det var kjekt å kunne være med å diskutere.

Ja, jeg heter Bjørn Børresen, jobber med programmering til daglig. Jeg har veldig interesse for teknologi generelt og dette området spesifikt. Og derfor synes jeg det er kult å kunne være med.

Jeg heter Nina (uklart). Jeg jobber med voksenopplæring. Når dette brevet kom i posten, så tenkte jeg at dette var så interessant at dette vil jeg være med på. Ikke noe mer komplisert grunn enn det.

Jeg heter Randi Joa. Jeg er mor til en funksjonshemmet gutt, og han har det med å stikke av. Jeg kunne godt tenkt meg å, i stedet for å ringe til politiet, å kunne sport han opp selv. Dermed så er jeg interessert i dette temaet.

Jeg heter Ole Gunnar Rosnes. Jeg jobber i Storebrand. Jeg er opptatt av samfunnssikkerhet og at vanlige folk skal være beskyttet, litt mer enn kjeltringene. Jeg har ofte mer inntrykk av at kjeltringer er mer beskytta en vanlige, ærlige folk. Så det var min årsak til at jeg vil være med på denne gruppa.

Flott. Da ser det ut som at vi har diverse av bakgrunn, interesse og det hele tatt. Da trur jeg bare vi begynner med de første spørsmålene. Det er et litt åpent spørsmål, et idemyldringsspørsmål, så da er det bare å komme med mye forskjellig. Det er ingenting man sier som er dumt, det er ingenting som er rette og gale svar. Her diskuterer vi hva vi mener og tror, og det er lov å stille spørsmål og undre seg litt. Det første spørsmålet er «hva er deres umiddelbare tanker knyttet til sikkerhetsteknologier og personvern?»

En umiddelbar tanke kan være at det kan være en konflikt. Altså, at den ene går ut over den andre, at det blir gjerne sånn interessekonflikt. Litt vanskelig å av og til ta stilling til. Man vil jo ikke at noen skal utføre terror, men vi vil heller ikke at noen skal vite alt vi gjør på hele tiden.

Jeg tenker, når jeg søker trygghet i forhold til det, så kan det fort bli utrygt også. Det er liksom, sånn sammensatt.

«det er mange som har lest 1984?» (latter)

Det koster litt personvern å få litt trygghet rett og slett.

Det er jo jeg villig til å gjøre.

Ja, altså, jeg og, det er greit. Det er derfor jeg sa det jeg gjorde i innledningen, fordi kjeltringer er ofte mer beskytta enn vanlige folk.

Jeg synes, av og til, så undrer jeg meg over sikkerhetstiltak må jeg si. I forhold til hvor effektive sikkerhetstiltakene kan være. Vi har masse sikkerhetstiltak som skal få deg til å føle deg tryggere, men egentlig så gjør de deg mer paranoid. Du kommer på flyplassen, så har de alle mulige scanninger og de tar av deg belter og sko og alt skal igjennom, i det hele tatt. Hvorfor gjør de det? Hva kan folk komme seg igjennom med egentlig? Vi hører jo forskjellige historier, og vi blir mer fokusert på hva som kan gå galt. Så vi får også utvikla et slags paranoid folk som tror at (uklart)

Ja, det tror jeg og er viktig, sånn som det siste sikkerhetstiltaket på flyplassen. Det at du ikke kan ta med deg så og så mye veske og at det må opp i en sånn liten pose. Det virker jo som at det er noe tull de har funnet på for at de skal vise at de gjør faktisk noe. De har jo vist at det er mulig å lage bomber av flytende materiale, det er ikke noe problem å lage det med de materialene du har oppi den posen. Så da spør man seg hvorfor det i det hele tatt er innført tiltak nesten.

Det er ofte en falsk trygget, rett og slett.

De har et gedigent gjerde langs hele vågen nede i byen, så du kan ikke gå og se på båtene. Du kan jo komme i en lettbåt på utsiden fylt med bomber og sprenge (latter) og så skal du liksom føle at nå er det trygt, for det er et stort gjerde. (flere snakker på samme tid)

Det som skjer at det er cruisebåter og så sperrer de den blå promenaden. Så du kan ikke bruke den om sommeren, for det er cruisebåter som ligger der. Så du kan jo ta buss (uklart)

Det er jo litt sånn at, jeg vet ikke om det er sannhetsgehalt i det hele tatt, men liksom, jo flere sikkerhetstiltak et sted har, jo usikrere er befolkningen. Jeg vet ikke om befolkningen er usikre, eller , jeg vet ikke om det er usikker i landet, om det er derfor de har sikkerhetstiltak, eller om sikkerhetstiltakene gjør folk usikre, men jeg var i Latin-Amerika, og der stod de med avsagsd hagle utenfor alle butikkene, jeg følte meg ikke veldig trygg altså. Selv om det sikkert var derfor de var der. Så det har jo noe med ...

Jeg tenker det er sånne operasjoner i forhold til å sikre oss. Men det at vi selv etterlater oss spor hele tiden, hvor vi enn går, med kort, bankkort, vi kjører bil gjennom bomringen, jeg synes det tenker vi ikke over i det daglige og hvor skummelt det kan være. Enten om jeg tenker på en sjalu ektefelle, hva med en arbeidsgiver, hva med en privatetterforsker, hvem kan spore mine greier? Er det åpent for hvem som helst? Kan de kjøpe det? I så fall, finnes det noen korrupsjon? Da blir man paranoid hvis jeg skal virkelig tenke tanken fult ut. Kan det skje? Det er skummelt.

Det synes jo jeg er faktisk hakket verre enn den som foregår på flyplassene. Og det som foregår på flyplassene bruker du jo bare ekstra tid på. Mens den du skisserer der synes jeg er mye verre. Det er jo veldig praktisk. (latter) Det er jo det som er problemet. Forbaske denne bruken av kort og plastikk altså, du kan jo ikke kjøpe lodd av ungene i gata lenger.

De kommer med sånn kortautomat (latter)

Men, de har det jo i kirka nå! (latter)

Tomas, hva sier du?

Jeg vil si at jeg synes den utviklinga i USA som foregår er skummel, den som blir tatt for The Patroit Act, som gjør at de har lov til å telefonavlytte hvem som helst, uten å ha begrunnelse i det hele tatt. Og de kan bruke det til liksom, du får ikke beskjed om at du har blitt avlytta etterpå, du får jo ikke gi din egen versjon av saken hvis det skulle skje noe. (uklart) Det gjelder jo også når du ringer til USA, at du gjør samtaler rutet gjennom sentraler i USA. Om du ikke ringer til USA, men til Afrika, så kan det likevel bli avlyttet hvis det rutes gjennom USA.
Jeg bare tenker på i forbindelse med det du sa om at folk gjør ting frivillig. Jeg synes det er ganske skummelt Vi snakket om (Facebook? -> uklart). Dette her med kommersielle selskaper og hva de har lov til å legge inn i kontrakter som du skal godta. Sånn som Facebook, så vidt jeg har skjønt, det er ingen som leser de forutsetningene før de aksepterer, ikke sant? Så har de da, så vidt jeg har sjønt, hvis du aksepterer vilkårene til Facebook, så får da kompaniet rettigheten til all informasjon du legger ut og alle bildene du legger ut, på Facebook, selv etter at du har sluttet å bruke det. Ikke sant, så har de den informasjonen om deg, og den har de rett til å bruke og til å koble sammen med annen informasjon på nettet. Og dette trykker folk på «jadda, jadda». Så er det jo sånn at flere og flere arbeidsgivere Googler folk. Når samtidig det første du gjør når du skal ansette noen, er at du Googler de. Ikke sant, hva slags informasjon ligger ute på nettet, i forhold til om du er den rette person til en stilling, eller, jeg vet ikke med forsikringsselskaper, men det kunne vært et poeng det og. At du trykker akseptere i veldig mange sammenhenger, så har du ikke lest og satt deg inn i hva du faktisk gir tillatelse til. Det er litt sånn, det synes jeg er ting som jeg savnet litt i papirene, dette med, skal ikke det finnes en grense for hva kommersielle selskaper har lov til å skrive med liten skrift på sånn? Jeg har prøvd å lese gjennom det, men jeg kommer ikke gjennom.

Jeg er på Facebook selv jeg, så jeg skal ikke (latter). På en annen side, så er et det med nettet som jeg synes er så fantastisk er det at vi kan Google, så får vi den informasjonen vi vil ha – fort. De automatiske sikringssytemene på noen nettsider og noen chattesider, og det er klart, jeg tenker på dette med sikringssytemer, det er nok ikke fult så oppe som det tilbudet er. Noe har jo klart å tilby sikringssytemene, det er jo, kanskje det kan være en måte? Men – det kan jo brukes og, det kan brukes av kriminelle, og andre igjen. Jeg tenkte dette med at en har behov for å spore, og det er fint. Men at det må være en slags sikring av hvem som får spore hvem. Vi sier jo ja til at Politiet kan spore hvis du har fått rettskjennelse, men at det på en måte er en bestemt hensikt, ikke slik at det kan bare åpnes opp for politiet eller hvem som helst. Sånn at staten kan bare scanne deg og finne hva som helst av nyttige ting. Det skal være en bevissthet rundt det, sånn at det må være en rettslig kjennelse. Det er sikkert en falsk trygghet det også, men at det skal være *noe* sikring. Jeg synes vi bare aksepterer alt, «jøss». (flere snakker samtidig) Nei, sånn spesifikt tenker jeg, men det går jo an å være bevisst på dette der. Jeg tenker på barn og unge: «ja, jeg aksepterer – boink!» Så blir de liggende for alltid.

Det som skjedde med Facebook og sånne tjenester i den dot.com kræsjen som skjedde i 2000 og noe, da de selskapene gikk konken. Disse nyoppstartede selskapene, det kan jo ikke facebook være, det er jo et ekstremt stort marked akkurat nå. Når de gikk konken, det eneste de hadde av verdi var brukerdatabasene og de solgte de til hvem som helst. Fordi det var det

de hadde som var vært noen ting. Så det var noen selskaper som kjøpte brukerdatabaser, og kjøpte informasjon fra forskjellige steder som var gått konken og solgte det videre. Så da oppstår det sånne situasjoner som den, som ikke er..

Der mener jeg det burde være mye større kontroll med videreføring av informasjoner. Rett og slett i forhold til lagring. Hvor lenge kan det ligge lagra?

Hvordan kan vi kontrollere det? Hvordan skal vi kunne klare å kontrollere alt det som ligger på verdenswebben.

De kan ikke kontrollere den, men det kan ihvertfall være ulovelig. (flere snakker samtidig) hvis du bryter lover, så kan ikke du, da kan det ofte ta litt tid.

Men i forbindelse med dette, at man kan ikke selge vekk personopplysninger som du har liggende. Kundelister og sånne ting.

Jeg tenker at kjeltringer får tak i den informasjonen uansett. Uansett hvor lovlig/ulovligt det er. Kjeltringene får tak i det.

(uklart) – ikke bare kjeltringer, med i USA, så stod det i det heftet vi fikk, at myndighetene hadde brukt 30 milliarder dollar fra de private selskapene om informasjon. Og det er jo for eksempel, hvis du er inne på en nettside som du ikke vil – hvis du havner i en rettssak så finner forsikringsselskapet ut at du har kjøpt alt fra pornografi til alkohol, som kan gå ut over at du er et dårlig menneske. Det er jo ikke informasjon som.

Det misbrukes jo, ikke sant?

Problemet er jo at for det første så finnes det jo kriminelle, det er jo en ting, som kan, hvis ting havner i feil hender, så er det. Og det finnes utro tjenere overalt, som kan selge informasjon. Selv om vi kan tenke at det ikke har noe med meg å gjøre, så kan vi komme i en situasjon hvor vi tenker at det ikke har noe med meg å gjøre. Så er det mennesker som, det kan være alt fra industrispionasje, til som du sier, hvis man er oppe i en rettssak, der interesser står mot hverandre og sånne ting. Så lenge ting er lagret, selv om det finnes klare regler for hvordan det kan brukes, så er et jo en fare med det. Med ting som er – jeg jobber jo i NAV. I trygdeetaten og Aetat slått sammen. Og nå er det jo mye mer som (hosting, uklart) – kan jo koble informasjon fra arbeidsledighetstrygt mot mottatt lønn og sosiale tjenester for å unngå trygdemisbruk. Det er jo kjempefint. Det er kjempebra at man kan det der. Men det er veldig mange personer nå, som har veldig mye tilgang til veldig mye informasjon. Og det er jo sånn at det er utrolig mange som kan være utro tjenere i det. Og det er utrolig mye informasjon som kan brukes av personer som kanskje ikke skulle hatt tilgang til det.

Kjempebra. Mange viktige og bra poeng. Vi kommer sikkert tilbake til noen av dem etterhvert. Det neste spørsmålet er «hva synes dere om scenariene?»

Jeg fikk ihvertfall et nytt syn på ting. Jeg hadde ikke tenkt over akkurat de scenariene. De ga et litt bredere perspektiv. Det ble bare så privat. Det ble satt inn i en verden. Det kunne jo tenkes at «javisst – sann!» jeg tror det var det som gjorde at ... ja ...

Det er først og fremst han som puttet den greia på moren sin (latter) – det var jo sikker bra det! Eller, det var ikke så bra? Altså... (prating i munnen på hverandre)

Det er jo noen ektefeller som vil følge etter hverandre, og da tenkte jeg - «det var skummelt». Noen vil jo rømme fra en person, men så blir man fulgt. Det visste jeg ikke. Jeg trodde jeg visste mye sånt, men det gjorde jeg altså ikke. Så det ble «alt jeg ikke vet!», tenkte jeg da.

Det er både på godt å vondt. (samtykke og samtidig prating) Vet du for mye, blir det gale det også, vet du for lite så har du lite å hvile deg på. (uklart)

Det som jeg tenkte om disse scenariene var at «jøss», hvor langt fram i tid er dette? Er dette noe de kan få til akkurat nå, eller er det noe de tenker at de kan få til frem i tid? Jeg hadde litt problemer enkelte plasser å skille helt. Er jeg litt naiv, eller hva er det? Følger jeg ikke med?

Jeg tror dette er veldig nært frem i tid, så noen av tingene er ikke i bruk *nå*, men de er under utvikling. Ingenting av det som står der er out of the blue. Det er ting som kan skje innen de neste 5 årene.

De biometriske spor? Det med fingeravtrykk, iris og ansiktsavtrykk og sånn. Kanskje de lagret alt og sånn? Kjempeskummelt tenker jeg det blir. De kan da bare snappe min identitet rett foran nesa på meg, slik tenker jeg at det blir. Det er ihvertfall viktig å ha et bevisst forhold til bruken av så personlige ting. I den forbindelse så må (uklart) De har jo like stor – hvordan skal det bli med de? (uklart)

Ansiktsscanning og sånn, det er jo et problem hvis du er ute for en ulykke. At det skjer ett eller annet som gjør at ansiktstrekkene dine forandrer seg.

Du oppdaterer jo ansiktet ditt hos kirurgen(latter) – sånn «Face Off»

Men vi vet at nå er det slik at det kan være en gammel mann som har problemer med fingeravtrykk. Så det er ganske sårbart.

Det jeg likte med scenariene er at de kom opp med ting som jeg ikke har tenkt på, som for eksempel at det tilfelle hvor han, personen, Petra, som skulle til. Som hadde kjent igjen en iraner og hadde tenkt å ta kontakt, men han ville ikke ta kontakt for da kunne det kanskje bli problemer. Da tenker jeg sånn at det blir jo et kaldere samfunn hvis du for slike bekymringer at du må holde deg unna visse typer.

Nå går vi jo tilbake til å sende brev i posten, for de kan ikke bli sporet. Så det er jo, det blir jo ikke kaldere, det går gjerne seinere, går et skritt tilbake.

Det blir jo vanskeligere, og da gidder du ikke. Da blir det til at du ikke gjør det.

«da var det ikke noe til forhold, hvis du ikke gadd å ta kontakt igjen» (ironisk stemme og latter)

Vi var kollegaer, så jeg vet ikke.

Den nakenmaskinen som har vært prøvd ut i London, den har vi aldri hørt om. (snakking i munnen på hverandre) Jeg så bilder på nettet.

– bilder på nettet? (ironisk stemme og latter)

Nakenmaskinen ble jo testet ut på Heathrow. Tore har jo gått igjennom den og det ble veldig sånn. Du følte det ikke så veldig sterkt når du gikk igjennom, for du ser jo ikke bildet. Du vet du går gjennom, men det blir litt sånn fjernt likveld fordi du ikke selv ser bildet. Men det har vært blitt gjort forsøk hvor folk har fått se bildet etterpå og da har de syntes det har vært helt forferdelig. Men du tenker ikke gjennom det når du går sånn gjennom.

Men det var vel skilter og sånn når du skulle gå gjennom?

Sånn som på Heathrow så tror jeg det er fremdeles på forsøksstadiet. Jeg tror det stod et sånn stort skilt «you may be randomly selected for a test search, if you refuse, you will be hand searched.» Så det var jo veldig (latter) Det er jo litt ubehagelig hvis det er menn som står og plukker ut.

Kanskje de kunne gjøre slik at det er menn den ene dagen som plukker ut andre menn og kvinner den andre dagen som plukker ut kvinner.

Eller omvendt? (mye latter)

Ja, de bare plukker ut pene kvinner hele tiden. Jeg har og hørt at det er noen som har sagt at hvis det er, en tysk kollega har sagt at hvis det skulle være gjort, så måtte de som skulle søke på den skjerme være et sted hvor de ikke kunne se den personen, for det hadde blitt veldig nært hvis man vet hvem som ser en, og det hadde blitt enda mer ubehagelig hvis man vet at noen ser på en, men ikke at man selv kan se den personen... Men – den maskinen fins.

Takk til deg. Et underspørsmål til dette. Skisserer scenariene et forlokkende samfunn?

Nei, jeg synes ikke det. Det er vanskelig å svare på. For det høres jo veldig enkelt ut. Men du er jo ikke beskytta på noen som helst måte. Så det er jo veldig tosidigt.

Og samtidig for tredve år siden, hvis du hadde spurt noen om de hadde skissert en forlokkende fremtid om at alle dine kjøp er registrert, så ville han sikkert svart «nei». Men det er jo avhengig av kortet.

Randi?

Jeg er ikke så veldig bekymret for denne overvåkninga jeg. Hvis jeg kunne sluppet og stå i kø når jeg skulle ut å fly og blitt sjekka ut på forhånd og fått en sånn snarvei, så ville jeg jo sagt ja til det. Den mobiltelefonen til hun moren, den ville jeg gjerne hatt. Men jeg ser jo problemet, og tenker på konflikter som kan oppstå. Det er veldig *der*. Hva jeg synes, og hva som kanskje er realiteten. Den er litt annerledes enn hva jeg kanskje kunne tenkt. Det er det altså.

Når vi snakker om det med sikkerhet på flyplass, så er det veldig mange, spesielt når man flyr til utlandet. Det er ingen plasser det er så strengt som her i Norge.

Hva med deg Tomas, synes du det er en forlokkende fremtid?

Vinklingen var jo litt negativ da, i skisseringen av scenariene. Men, det stilig med den bilen som ble stoppet av en satelitt, og at de visste den var stjålet. Og at man kan stoppe eventuelle

terrorister som er på vei til å utføre noe. Samtidig synes jeg hele det der begrepet med terrorisme. Vi sier «vi må bekjempe terrorisme», så da kan vi gi slipp på de og de rettighetene liksom.

Terrorisme er en joker som du kan slenge ned i hvilken som helst setting. «Synes du det er greit at politiet gjennomsøker tilfeldige hus?» og da svarer jeg «nei, selvfølgelig ikke!» - «men det er jo for å bekjempe terrorisme» - «åå, men okey». Altså, (latter)

De skal jo ha en mistanke. Men det er grenser der og. Hvorfor har de mistanke?

Så er det jo, altså, hvis du har en rettslig kjennelse, og det er jo liksom sånn det der, tilatelsen, for da har du en kjennelse og har tillatelse til å gjøre en god del ting. Så skal ting være anonymisert frem til du har en rettslig kjennelse. Men, så lenge, jeg er litt der, teknologien eksisterer og den er slik at det er lett å få tak i den type informasjon, så vil det alltid være noen som henter den informasjonen uten rettslig kjennelse og jeg er ikke veldig paranoid. Jeg kjenner folk som er mye mer paranoid enn meg. I forhold til hvordan du skal... (uklart)

Altså, jeg tror ikke at myndighetene er ute etter folk. Vi har jo, ettertiden viser jo alltid, at det har vært noe i fortiden som ikke har vært bra. Så skal vi komme om 20 år, så skal vi si at dette har ikke vært bra. Det har jo vært sikkerhets, amerikansk etteretning har jo fått komme til Norge og fått muligheten til å prøve å arrestere folk i Norge. Denne informasjonen blir jo gitt ut av Norge, i det hele tatt, så det er jo en masse ting der som ikke er bra. Som på en måte du ikke styrer over. Så lenge det finnes informasjon som er lett tilgjengelig, så vil det alltid være muligheter til snarveier. Det tror jeg sånn vil det bli. Så er spørsmålet i hvilken grad og hvor mye du kan ofre. Jeg tror ikke at vi har ordnet opp «det på 70-tallet, det har vi ordnet opp i» - nei, jeg tror ikke det er slik.

Det er jo både positive og negative potensialer i sikkerhetsteknologiene. Neste spørsmål er hva dere synes er de positive potensialene til sikkerhetsteknologien? Vi har jo vært inne på noen, men kanskje vi kan snakke litt om hva som er de viktigste positive potensialene?

Det må jo være å kunne være i forkant av kriminalitet tenker jeg. Da tenker jeg på trygghet igjen, i forhold til at alltid skal kriminelle være mer i forkant i politi av samfunnet. Alltid skal de være mye lenger, og det gidder jeg ikke. Det er grådig irriterende! Jeg er enig med deg, jeg tenker, «shitt au» Slipp det løs! Det ville jeg jo ikke heller... (latter) Så det blir sånn todelingen, sånn med NOKAS-saken, tenker jeg, pokker ta – her er jeg og! Men det blir sånn følelsesmessig for vi tar noen slike diskusjoner, folk vet jo hva det handler om.

Andre positive potensial? Det er jo og det at de gjør ting, ting blir lettere, sånn som i de scenariene du beskriver at du slipper kø, slipper betale, at du liksom bare får fingeravtrykket, så blir det så lett.

Så kan du putte penger inn i ryggen (latter) Det er jo det som er fremtiden. Få laget en liten chip under en negl sånn, så har du hele kontoen med deg. Trenger ikke noe sikkerhetskort eller noe.

Så går du rundt i et kriminelt område, så er det eneste de er interessert i å få av deg, er fingeren! Ja, så går det masse folk med amputerte fingre (flere prater samtidig)

Kriminalitet og det at ting går raskere. Har dere andre ting?

Jeg tenker på dette med sporing jeg, så tenker jeg på hun stakkars Madeleine, så tenker jeg på hvor hun har blitt av og alle de andre savna ungene. En tid tilbake i tid, så var det en i min egen vennekrets som ikke ville leve lenger, som satte seg i bilen og kjørte og som tok sitt eget liv, og han fant vi ikke. Til slutt klarte vi å spore han via mobiltelefonen, og det var vi veldig glad for, for vi brukte veldig mye energi på å finne han. Altså, det var veldig godt å finne han, vi skjønte jo hva som hadde skjedd, men akkurat den typen med å spore. Der er tross alt ting der som er – både positive og negative sider.

Aldri så godt at det ikke er gale for noe.

Er det noen andre positive ting dere kan tenke på? Vi kan komme tilbake til dette. Så kan vi gå til de negative effektene.

(uklart) de kriminelle får lettere tak i informasjon enn politifolk.

De kan selge den informasjonen de har fått til andre kriminelle. De har alle rettigheter til det du ligger ut.

Det er galskap at man skal kunne ha sånn på datamaskinen. Det jeg tenker med denne Facebooken, jeg har ikke gjort, jeg har vært inne og sett på. Og så har jeg tenkt at dette skal jeg ikke bruke tid på. Jeg tenker bare på hvordan alle tenker at «alle andre gjør det også». Til og med statsråder og jeg vet ikke hvem som gjør det. Det må jo være lovlig, det er jo i Norge. Du skjuler deg litt rundt den der «alle andre»

Det er jo et amerikansk selskap, så jeg tror ikke de har noen verken lov eller intensjon om å følge norske lover.

Det blir jo litt sånn, i det her scenariet, i det at ungdommen ser ikke ut til å bry seg om sånne ting som er der. Det *er* jo sånne ting som, jeg tror det er slik at jo eldre du er, jo kanskje, det er jo slik, folk går jo frivillig på Big Brother. Det er jo en tendens i samfunnet som virker som om at folk ikke synes det er så viktig å ha den privatsfæren lenger og jeg tror kanskje det har, nå husker ikke jeg krigen. Jeg tenker, jo lengre det er siden man har en erfaring med at noe har blitt misbrukt, jo mindre skeptisk er du til nye ting. Så, du har på en måte ingen en erfaring av at dette kan bli misbrukt. Du har ingen venner som har fått dette misbrukt. Så blir det ikke noe viktig, og så, jeg synes det er litt skummelt jeg. At så lenge du aksepterer sjøl, så skal alt være lov.

Det som er mest skummelt synes jeg, er at folk er så vanvittig naive. Dette har jo også med, ungdom som vokser opp i dag, de sier «alle andre gjør det jo». Altså, kokain, det er ikke farlig det, «alle andre gjør det».

I det siste har de lansert mobbekampanjer på nett. I forhold til å mobbe hverandre på nettet. Og det er det vanskelig å komme til livs. Dette er en mulighet vi har, det er vanskelig å kunne styre med lover og regler akkurat nå, så det må kanskje kunne være en fordel å kunne la folk være å mobbe. Og dette var det ene, også det med kommersielle krefter i forhold til at de kan spore opp hva jeg er interessert i gjør at det dumper ting i postkassen min. Det dumper ting ned i postkassen min. Altså, de kartlegger mine behov uten at jeg har sagt at det er greit. Og kanskje jeg kan melde meg av en del ting, men likevel så dumper det ned en del ting.

Hvis du abbonerer på endel blader, så selger de det videre, for da blir de interesserte i slike ting.

Det er ikke tilfeldig at krybbedødforening ringer om barsel en uke etter at du har kommet hjem fra sykehus! Men de sier selv at det er tilfeldig. Det er vanskelig å vite, men det er jo sånn. Jeg vil jo egentlig ikke at forsikringsselskaper (uklart, latter). Dette med, hva har du lov å skrive, hva har du lov å godta i forbindelse med kommersielle selskap. Dette med forsikringsselskap, om de skal få lov til å få en godkjenning av en person til å få legejournalen. Fordi, okay, jeg kan si nei, du kan ikke se legejournalen. Men så sier de – du får ikke forskring. Ikke sant? Da *må* jeg gi fra meg legejournalen min. Dette er en tenkt situasjon, så sier jeg *nei*, du skal ikke få lov til å be meg om det. Det skal faktisk være lov til å være noen ting hvor du kan si «nei, dette aksepterer jeg ikke!»

Det er det samme som det på nettet, enten så aksepterer du det, eller så gjør du det ikke. Det er ikke alle som helt forstår hvorfor det er så strenge regler. Det er klart at de trenger å gå i legejournalene, men det er jo der det skjer noe, så kan vi vite hva som (uklart) når vi skal få utbetaling. Og synes du det *da* hadde vært greit å betalt ei forsikring og funnet ut at du får ingenting likevel.

Jeg har det sånn at jeg har en tante som har epilipsi, så hun får ikke livsforskring, fordi hun blir sett på som en for stor risiko liksom. Det er synd at mennesker med ulike medisinske lidelser ikke skal få dette fordi at de har.

Jeg vil bare si en kommentar. Jeg mener jo at grunnen til at jeg mener det jeg mener, er at jeg skjønner hvorfor forsikringsselskap ikke vil gi forsikringer til personer som har større sjans for å komme ut for ulykke. Det skjønner jeg, for de er jo kommersielle selskaper. Hvis vi hadde gått inn og sagt at nei, det får faktisk ingen forsikringsselskap lov til å gjøre, så hadde det jo vært litt (uklart – farlig?)

(flere snakker i munnen på hverandre)

En liten kommentar. I forfjor fikk jeg en uføreforsikring gjennom jobben, og da var det to ting som jeg la merke til i den saken var at jeg måtte gi fullmakt til at forsikringsselskapet kunne ta kontakt med legen min og at de kunne avbryte forsikringen hvis de følte at jeg kom i en risikogruppe. De lurte også på om jeg hadde hatt problemer, tatt medisiner, eller hatt psykiske problemer. Og så, etterpå, når jeg skulle skrive under ,så fikk jeg beskjed om at dette var en bedriftsavtale, og da fikk jeg beskjed om at jeg ikke hadde noe valg. Jeg kunne slått meg vrang, men jeg gidder ikke det. Så det jeg ender opp med, er at jeg føler ikke jeg kan gå til legen min lenger og si at jeg er deprimert, for da kan det jo hende at forsikringsselskapet ringer opp legen og spør «hvordan går det med Børresen?» (latter) «Han var deprimert» «da blir det kansellert»

Det er jo derfor de ber om disse tingene i forbindelse med (uklart) (latter)

Da har vi fått sett på noen av de negative aspektene, blant annet når det gjelder utlevering av data og når det gjelder overvåking og sånne ting. Er det noen andre negative effekter knyttet til sikkerhetsteknologier?

Jeg tenker på det med, det hadde noe med etikk å gjøre, med menneskeverd. Det handlet om det å være menneske, og at det er en grense for hvor mye vi kanskje skal bli – var det negativt

det? «åå, jeg tenkte en så fin tanke om det...» Det *skal* være risikofylt å leve, det skal aldri være helt trygt. Og det er da jeg tenker at hvis vi skal gå rundt å tro at det er så trygt, at det ikke er noen risiko lenger, så mister vi noe viktig. Det var det jeg tenkte. Da har vi gjort en feil. Så den der paranoiaen hvor vi søker trygghet og trygghet – da mister vi *oss selv.* Vi mister etterhvert, hva skal vi si, etthvert menneske har ansvar for å sjekke ut hva som er trygt og hvor vi går hen. Vi har et ansvar for å søke informasjon om den verden vi begir oss inn i. Enten det er Facebook, enten det er bøker vi låner på biblioteket, eller om det er hva som helst. Altså, vi tilegner oss informasjon, og vi kan *aldri,* de skal ikke ta ifra oss den plikten tenker jeg, at «åånei, nå skal jeg saksøke noen!», eller hva som helst. Det å bruke hodet, er jeg litt redd for, at vi skal la oss bevisstløs la oss lede inn i all slags personvern. Det var det jeg tenkte

Hvis det blir 100% trygt, så mister du hele forsvarsmekanismen.

Det er akkurat som om at du blir dødssyk av en forkjølelse.

Bra, da tror jeg vi går videre på neste spørsmål, og det er hvilke situasjoner er sikkerhet viktigere enn personvern? Og omvendt? Og når kan man si at personvern er viktigere enn sikkerhet, og omvendt?

Det kan være vanskelig, kjempevanskelig. Jeg har en sånn greie på at noen steder velger du å gå. Og du har et alternativ, det er ikke alltid. Hvis du går på flyplassen for å ta et fly, kunne du ha tatt toget i steden for. Du går på en flyplass, og flyplassen sier at den trenger sikkerhet, og det vet du om på forhånd, at de gjør sånn og sånn. Eller hvis du kommer på en eller annen svær landskamp i fotball. Og du velger å gå inn der, og de sier at «vi kan ikke gi sikkerhet», og de sier «take it or leave it». Her gjør du sånn. Og det er litt sånn, nei, for jeg har mitt personvern, så jeg skal gå inn på denne landskampen og ingen får lov til å sjekke om jeg har våpen. Det blir litt sånn, okey, hvis du er så opptatt av personvernet ditt så ser du den kampen hjemme på tv. Mens steder hvor du ikke har et valg, så synes jeg personvernet er viktig. Hvis det er ting du *må*, så synes jeg det er viktig at du skal få lov til å si, å slippe å bli overvåket på et eller annet vis. Hvis du *må* gå og registrere deg som arbeidsledig på et eller annet vis, så skal du få lov til å gjøre det litt anonymt. At ikke alle får nummeret ditt, «pling pling». (latter)

Randi, har du noen tanker?

I forhold til det du nevnte om sønnen din, så er det en stor sikkerhetsrisiko, men der er jo også personvern inne i bildet.

Ja, og jeg setter jo sikkerheten foran personvernet i den saken. Det gjør jeg jo, det er veldig viktig.

Er det et vanskelig valg å ta?

Nei, ikke for meg. Det er jo veldig individuelle behov. Det er mange som har individuelle behov. Du kan ikke si at alle skal kunne spores overalt, men du kan ikke vente at du får en rettslig kjennelse for at du kan spore. Det må jo kunne kategoriseres. Slik at noen faller i den ene og den andre kategorien. Det er jo umulig i dag, vi får ikke det i dag. Du kan jo spore hunden din!

Det er ikke lov til å gjøre det..

Hvilke andre situasjoner er det sikkerhet er viktigere enn personvern?

Jeg synes det er greit at de sjekker om folk er tidligere dømt før de ansetter i barnehagen for eksempel. (flere prater i munnen på hverandre) Det er jo litt rart hvis man som søker ville ha jobben og sa at «nei, mitt personvern er viktigere».

Ja, det er jo du som oppsøker jobben, folk som søker arbeid må bli sjekket. Er det det som blir straffen da, at hvis du begår ulovlige handlinger så mister du litt av retten til personvern? Samtidig så strider det mot demokratiske prinsipper som sier at når du har sonet straffen din så er du fri og du har gjort din plikt, ikke at det er noe som forfølger deg hele livet.

Men det spørs jo, mener jeg, jeg er helt enige, at hvis man har sonet straffen, så bør man være fri, men hvis man har gjort noe alvorlig, så bør man være beheftet med det. Jeg sier, man har jo gjort det likevel. I forhold til dette med barnehager spesielt.

Når er personvern viktigere enn sikkerheten?

Security first. (uklart) skulle ringe en telefon, så er personvern viktigere enn sikkhert, i forhold til at de skal kjøre sånn web-overvåkning av hele befolkningen. (uklart) hvis du gjør noen ting, så trigger det plutselig at du er mistenkt. Sånn som Echelon-systemet i USA, der de innhenter sånne spesielle nøkkelord og hvis det inneholdt visse ord, så ble det lagret og trigget.

Du sa ikke noe om sikkerhet før det? Hva slags sikkerhet, sammfunssikkerhet? Altså, personvern, når går enkelte mennesker hensyn foran sammfunssikkerheten?

Jeg tenker, hvis du er en person hvor du har en sikkerhetsteknologi, for eksempel hvis du scanner epost, telefonsamtaler, søk over nettet, scanner etter et spesielt ord. Hva er forholdet mellom personvern og sikkerhte? (tenkepause) Vi kan tenke litt på det. Så kommer neste spørsmål, og det er «hvem bør være med å bestemme hvordan mulige sikkerhetsteknologier kan brukes?»

Jeg synes det, sånn som det gjøres nå med teknologirådet, at de både bruker eksperter og at de bruker og vanlige *borgere,* at de sjekker det litt opp mot hva den vanlige mannen i gaten, hvordan han vil ha det. Det synes jeg er bra, for de ekspertene kan gjerne bli litt «for eksperter». De kan miste litt bakkekontakten. Det skal bli så veldig, jeg synes det var veldig tiltalende slik som det ble sagt i begynnelsen, at man sjekker referanser i alle.

Jeg synes ikke ekspertene skal tillegges mer vekt enn det bør være (uklart, høy prating i bakgrunnen)

Så har du politikere som ofte har mye å si.

Sender dere inn innspillene etter at dere har henta inn opplysninger fra eksperter og vanlige folk, sender dere da innstilling til storting, regjering og departementet?

Og så har de sine egne meninger, og så (uklart – latter)
Det er først og fremst til stortinget, men det kan være at hvis det er en spesiell sak så kan det sendes til en komite som jobber med det. Vi gir ut sånne råd til tinget, som vi gir til spesielle

grupper og til folk som kan være itneressert i det. Om de tar det med i sine avgjørelser på grunnlag av det, det er jo...

Det ser dere jo i ettertid dag.

Men ihvertfall så ser vi direkte resultat i de meldingene de kommer med.

Jeg vil jo tro at de meldingene som kommer fra teknologirådet at det vil gi et godt grunnlag, et grunnarbeid som er gjort i de utallelsene, de vil veie tungt for at departementet skal ta en beslutning. Såpass tro har jeg på politikerene. Jeg tror faktisk de lytter til slike råd.

Så vi kan stole på politikerene i saker som har med sikkerhetsspørsmål å gjøre?

Ja, altså,det spørs jo litt på hvilket politisk nivå, ikke sånn politisk høyre og venstresiden, men er mer enige i denne typen ting.(uklart – finansdepartementet – latter)

Jeg har tro på lobbyister også. Alle slags tema og emner i politikken, og akkurat dette, hvis de får det fra teknologirådet, så velger jeg å tro at de vektlegger det.

En ting jeg tenker på, er dette med at dette blir tatt opp med lekfolk, og at dette blir tatt opp som et tema og kommer i avisene. Jeg er opptatt av en slags utdanning i det. Vi lærer ikke om det i min generasjon. Vi vet ikke så mye, vi er ikke så opptatt av. Og så holder ungene på vettu. (latter) Det er sånn allmen informasjon og utdanning, og slik kan denne type informasjon hjelpe til med.

Så det er viktig at folk også er med i denne diskusjonen?

Vi lever jo i et demokrati, vi blir jo som regel hørt når vi hever stemmen.

Jeg tror altså, det er jo mange kommersielle interesser når det gjelder denne teknologien også. Det er jo sånn det er, og det er mange. Både stor økonomi og makt å ha tilgang til sånne ting som dette her. Så jeg tror nok det er mange som ønsker å påvirke et sånt arbeid som dette her. Og jeg synes vel egentlig at det er viktig at man på en måte lar alle sider, at folk bør delta, det er kjempekjekt. Jeg synes det er viktig at folk som jobber med person, datatilsynet, menneskerettighetsorganisasjoner, men også kommersielle interesser, fordi at det er enormt viktig å se den siden, for hvis ikke blir det sånn at de kommersielle interessene har sin egen agenda på sidelinjen. Kommersielle interesser har også en plass i dette systemet her. Vi er ikke kommunistisk.Vi må på en måte finne alle, og at alle skal få litt å si.

Neste spørsmålet er litt relater. Og det er om dere har noen formeninger om regulering av nyutvikling av sikkerhetsteknologier. Burde man regulere hvordan type teknologi som vi utvikler? Burde det være noen begrensninger?

Jeg synes ikke det høres ut som en smart ide å begrense utviklingen. Det vi må tenke på er hvordan vi tar ting i bruk. Og har regler på hvilke systemer folk har. Det er ingen som gidder å bruke millioner av kroner på å utvikle noe de ikke kan bruke.

Jeg vet heller hva som vil bli godkjent. Det er jo litt viktig.

I forbindelse med at jeg skulle hit, så søkte jeg på forskjellige ting. Så sjekket jeg på sånne «spy-sider». Og sjekket ut hva man kan få hjem av eget utstyr og ha på egen PC. Det er ganske spooky, og det var i grunnen ganske billige ting og sånn. Men jeg har absolutt ingen tro på at hvis du sier «nei, det får du ikke forske mer på». Så vil de si «nei, det er forbudt, det vil vi ikke forske mer på». Det er jo ikke sånn, man forsker jo på ting som man kan få en fordel av. Ingen aner jo hva som er i den kjempesvære senderen som står i (uklart, lokalt stedsnavn?) Du vet jo ikke hva som er der.

Og du har helt sikkert kriminelle forskere også. De kan vi ikke bestemme over.

Trenger vi ikke begrense og regulere hva industrien utvikler av teknologi?

Jeg tror det er umulig, det går ikke an. Det vi risikerer er at de kriminelle utvikler det i stedet, at vi heller bør ta konsekvensutredninger og se på bruken av det. (uklart)

Jeg tenker på software for å overvåke nettet. Det må jo være lov til å utvikle det på egen maskin, men det er når du tar det i bruk det blir ulovelig.

Jeg har vel en viss tro på at jo bedre teknologi som finnes, jo midnre sjanse er det for feil, det er jo litt sånn som det stod i scenariet, i begynnelsen så hadde de mange feil, feil-score, feil utvalg av personen, så forbedret de systemet, så fikk de færre og færre. Det vil jo si at, jaa, de kan få lov til å ha dette systemet, og det har blitt bedre og bedre, og sikrere og sikrere. *Men* dere kan kun få lov til å bruke det hvis sånn og sånn, og i de og de situasjonene, ikke sant? Tror ikke du kan si at det er forskjell på forskning (uklart?)

Da er vi enige? (latter og samtykke) Da er vi på nest siste spørsmål. Har deltagelsen deres i dette arrangementet endret deres holdninger til dette temaet? Er det noe dere har tenkt og snakket om og sånne ting?

Jeg vil si nei.

Jeg vil ikke si om temaet, men jeg vil si at jeg har blitt mer bevisst. Det har jo åpnet mye større rom, har lært mye.

Jeg er helt enig. Jeg blir vel egentlig der som jeg har alltid vært sånn sett, men jeg blir mer bevisst. Spesielt de scenariene, hvor det er sånn «oi, er det mulig??» Du går litt i tankene, men jeg mener at jeg tror i grunn det samme, selv om det har åpna seg en større forståelse.

Jeg tror ikke jeg har endra så mye mening underveis. Jeg svarte på spørreskjemaet, og merket at jeg ikke har forandret så mye.

Jeg er litt enig, men å bli mer bevisst er jo også å bli litt mer nøyansert kanskje? Så i en sånn hovedretning så kan jeg si at de har jo ett poeng – kanskje? (latter)

Altså, jeg har alltid vært åpen for nye ting. Så når jeg leste de casene, så tenkte jeg «nei Gud så skeptisk jeg ble», så tenkte jeg, nå var jeg i balanse igjen. Det er klart, jeg tenker, det er noe med hva som skapes når man får kunnskap av nye ting, men om en måned så er jeg ikke oppdatert igjen. Men man er aldri oppdatert *nok*, men det er veldig spennende altså.

Jeg er litt skeptisk kanskje. Jeg er veldig glad i teknologi og jeg er veldig glad i å leke med nye ting, men det er klart, selv om jeg har en tendens til å veldig lett, så sier jeg at jeg har (uklart) Det er noe med den utviklingen jeg har sett i USA som jeg er skeptisk til.

Så det er noe du har utviklet gjennom denne samtalen, at du kanskje har blitt litt mer skeptisk?

Ja (uklart, latter)

Hvordan skal du klare deg å trekke deg ut av Facebook, uten å legge igjen noen spor? Hvordan kan du legge ut fake-bilder og legge ut ting slik at det ikke skal ha noen funksjon lenger? Det er jo (uklart)

Mye problemet er jo ikke de tingene du legger ut selv, problemet er jo ting andre legger ut. Når du har vært på fest og de sitter med mobiltelefoner (uklart – latter)

Er det noen siste kommentarer, tanker?

Jeg har en ting som jeg har tenkt på noen ganger i kveld. Jeg synes tidspunktet for denne seansen har vært litt skjev. I forhold til en hektisk hverdag, har jobba og stått på hele dagen, litt kort tid til å ta seg inn igjen. Litt lite opplagt følte jeg personlig, men jeg har ikke vært så mye med, så det har ikke. Men jeg følte meg litt, etter en lang arbeidsdag. Så jeg tenkte at dette kunne vært et dagsseminar og ikke et kveldsseminar.

Hadde det passet bedre på en mandg?

Ja, det hadde det. Helgene er hellige. En hverdag med kompensasjon for lønn.

Det skal vi ta med oss videre. Noen andre kommentarer, tanker?

Jeg lurer på hvordan vi ble valgt ut. De 30 av 2000?

Jeg fikk en liste av folkeregistreret, så hadde vi et selskap som plukket ut tilfeldig og så fikk de tilsendt informasjon.

Og så ble det de som svarte som ble med?

Ja

Jeg synes det var et bra tiltak. (uklart – prating og latter)

Takk for en veldig bra diskusjon, jeg synes det var veldig interessant og bra (mer samtidig prating)

Gruppe 3

Ja, det blir jo interessant med den mangfoldige bakgrunnen også dere har, så der ser jeg frem til gode innspill. Vi har et nokså strengt tidsskjema på dette, så jeg skal prøve å si ifra og holde litt kontroll på at vi får fremdrift og noen ganger kan det hende at vi opplever, at diskusjonen blir sånn at man snakker litt i munnen på hverandre, og da kommer jeg til å be om at jeg får tegnet ned navnene og ført en listen og på den måten ført ordet. Men ellers kan vi ha en fri diskusjon i begynnelsen. Aller først vil jeg bare høre hva som er de umiddelbare tankene dere har gjort dere etter å ha lest dokumenter og hørt det dere har hørt i dag, men den bakgrunnen dere har, hva er de umiddelbare tankene dere gjør dere om de dilemmaene om sikkerhet kontra personvern.

(uklart)

Det er litt bekymring for overvåking?

Jeg tror ikke vi har noe valg utenom heller, uansett om vi sitter her og diskuterer og ikke er enige med dette, så tror jeg at det blir innført uansett. Det sitter noen ovenfor som bare, jeg stoler ikke på dem. Fullstendig, myndigheten, jeg stoler ikke på de, de sier bare «sånn og sånn», det ser du med enkle ting som bompengeringen, de sier bare de skal innføre den, og så aksellerer det. (uklart) vi har ingen kontroll og innsyn i det.

Og så er det jo det at vi ønsker sikkerhet for våre egne penger i banken. Så ønsker vi å sitte hjemme og betale våre egne regninger. Så da er alternativet at vi må reise til banken fortsatt.

Og hvem vokter vokteren?

På banken er det kanskje du selv som passer på dine egne penger.

Men i systemene her, så sitter det noen her og vokter oss. Det er myndighetene. Hvem vokter de igjen? Se Nokas-ranet da, det var en insider der. Det er jo sånne...

Jeg tenker jo, sånn vil det alltid være. Sånn vil det alltid være i samfunnet. (uklart) jeg kjenner på at vi trenger ikke være de første på alt dette (uklart) verden og livet er en trussel i seg selv. Og hvis du tror du kan at du kan være helt sikker med teknologien og at du kan redde verden, så er det helt feil tenker jeg. Mennesket må styre noe av teknologien, teknologien er ikke god nok i seg selv. Derfor er jeg glad for at det må være noen etiske retningslinjer. Jeg jobber jo som sykepleier, jeg tenker taushetsplikt. Det er judaser alle veier. Men alle er ikke judas. (uklart) – men graden av det.

Start bilen, den starter jo ikke uten strøm. Den er jo teknologisk. Har den ikke strøm så starter den ikke, da vil det bli helt texas alle veier. (uklart) – det strømbaserte samfunn.

Jeg vil ha flest mulig kommentarer, er det noen andre som har helt generelle betraktninger om dette?

Jeg ser at du kan ikke få begge deler. Det er det jeg sitter igjen med nå. Jeg trodde det var mye enklere enn det var. Det ble mer komplisert etterhvert som jeg leste spørsmålene. Etterhvert så måtte jeg ta standpunkt i sakene. At det faktisk, du må oppgi ganske mye for å få det sikkert. Men prisen er høy.

Du er enig, nikking som enighet?

Det er så mye som foregår, alt er jo teknologisk, så jeg har ikke peiling på noen ting. (latter)

Det er veldig vanskelig å unngå og. Det er et kappløp mellom de som ønsker å bryte sikkerheten og som ønsker å holde den. Så hvis de som prøver å holde den er akkurat der, og de som prøver å bryte er ett skritt bak, så klarer de jo, så kommer de. Du må alltid ligge hakke foran. Du kan ikke nedtrappe sikkerheten, for skurkene vil jo ikke nedtrappe sin kompetanse.

(uklart) du burde kunne velge selv hvordan du vil ha det.

Ja, for eksempel kontanter. At det fortsatt skal være mulig å betale kontant.

Ja, jeg tror vi går videre til neste spørsmål. Da vil jeg bare høre litt om hva dere tenker om det dere har fått presentert i dag. Bare scenariene i forkant av møtet, der fikk dere tilsendt scenarier som beskrev litt av de dilammaene, illustrert med to figurer. Måten personvern og sikkerhet var presentert på der, ga det et noenlunde et balansert bilde av de dilemmaene vi står ovenfor der?

Ja, det synes jeg(flere samtykker). Det fikk fram både fordeler og ulemper med det. Ja, godt balansert.

Ja, synes du, det var også beskrevet både fordel og ulemper. Var de fordelene for eksempel, er de viktig og oppnå i seg selv?

Ja, absolutt.

Så det er et mål. Er det noen som har noen andre tanker om det?

Ja, for eksempel han fyren som fikk en fordel på flyplassen, som brukte Fast-Track. Kanskje han litt mer skeptisk ville prøvd å unngå hele flyplassen? Kanskje han ville unngå og reise og kanskje ta et telefonmøte slik at han slapp og reise? For, og kanskje tilogmed ha kryptering på telefonen. Og dermed unngå hele problematikken?

(uklart) det skal så lite til for at det skal skje en feilmargin. Og det får du større straff for den feilen som skjer, enn det positive som skjer. Jeg ser at det er positive ting, men jeg stoler ikke på de som bruker utstyret.

Det som jeg reagerte på, det var hun damen som ble (uklart). Og da kjente jeg at det var min grense. Og det var hun dama som ble, ikke avkledd, men som ble inspisert, men visste at det fantes (uklart) Det ønsker jeg ikke. Jeg kan kle av megselv hvis jeg skulle (latter) (uklart) Men, at hun kunne vært der, at hun kunne søkt etter han sønnen. At hun ga han den telefonen og at hun kunne fulgt med på om han var hjemme om nettene. Altså, hun tenker jo sikkerhet, også visste han ingenting om det. Det er jo det som er cluet i det hele med dette. At vi ihvertfall får vite om ting, at vi blir overvåket i Sandnesgata, og utenfor banken og sånn. Og at det er friplasser. Da vet du ihvertfall at her er et kamera. (uklart) Så det var et par eksempel i det hefte som var litt sånn «javel», det liker jeg ihvertfall ikke. Der går min grense.

Jeg har litt inntrykk av at det er mange som har blitt litt skremt av scenariene. Eller er det litt blanda, er det mange som ser på at dette vil gi muligheter som vi ikke har i dag, at det er litt forlokkende i det også. Hva tenker du? Når jeg hører debatten her, så hører jeg om ulempene, at det er et litt skremmende bilde, selv om det er fordeler også, men at det ikke nødvendigvis sees på som et fremskritt. Men – sees det også på som noe forlokkende, at vi kan få bedre kontroll med kriminalitet, bedre forebygging.

Altså, det er jo det myndighetene har begrunnet det med. At vi får sikkerhet, mot terror og kriminalitet og så videre. Men det er klart at det er et sånn tohodet sverd, at vi på ene siden får sikkerhet, men andre siden så må du gi fra deg mye av den private sfære. Og det er å finne den balansegangen, de skjæringspunktene, hvor mye du er villig til å gi for et varig sikkert samfunn. Det er jo spørsmålet om det kan misbrukes. Sånn som i dag, det er veldig lett med hackere. Bryter seg inn med kodene og så videre og videre. Det er veldig skremmende, det ene eksempelet, hvor man kan få stjålet, at man mister disse identitetene, det er et helt sånn, ihvertfall for meg, et skrekk-scenario. Hva er det vi sitter igjen med da? Man har liksom mistet det man har.

Du kan ha iris-scanning. Men hvis noen stjeler det, og klarer å lage et identisk øye og klarer å lure de. Du kan ikke få *et nytt* irisbilde. Og når det er kopiert, så kan kopien mangfoldiggjøres også.

Hvis vi tenker enda videre på dette. Det kan jo hende det blir en svartebørs industri på dette.

God krim (uklart) – kan vi ta noen bilder? (uklart)

Hva skal du med dem? (uklart og latter)

Vi kan bare gå videre, skal vi ikke det? Nå har vi jo prata litt om skremmebilder, hva ser på vi som de viktigste fordelene ved denne teknologien?

Det er jo forenklinger da.

Det er jo det bekvemmelige. Du tar ikke med deg en papirbunke hver gang du skal bevise hvem du er.

Ikke minst på bussen, hvor du slipper å knote med kontanter, og du faktisk får 25 prosent rabatt for at du ikke har kontanter.

På kortet tenker du?

Ja, men det er ikke mindre jobb for sjåføren. Kortbetaling (uklart) introduksjonsproblemer.

Jeg tenker, at på mange måter, når vi får denne nye teknologien, så stadig vekk så blir vi forbrukere lagt nye oppgaver. Vi gjør selv jobben, ikke sant? Og likevel må vi betale for det, det er ikke gratis, ikke sant?

Det er gratis å bruke nettbanken, men du må ha en pc til 25 tusen.

Men – forenkling og effektivisering, trygghet?

For eksempel sånn overvåking, eller den her barnevakttelefonen. Ungene dine vil kanskje synes det var greit at du visste hvor de befinner seg, men jeg hadde ikke syntes det var greit at mine foreldre hadde visst hvor jeg er. (uklart) Nei, se at jeg hadde hatt en elsker da (latter)

Det er faktisk flere år siden, at det var Reima, den klesprodusenten for barn, som introduserte en sånn packard-vest, med temperatursensor, GPS og GSM.

Men det har du på disse Bergans (latter)

Det var en sånn bevegelsesdetektor. Hvis ungen lå og temperaturen ble kaldere, så sendte mobilen hjem posisjonen til foreldrene.

Wow

Det viktige er at du har muligheten til å si stopp og ha muligheten til å få sperret. Å velge vekk. Det må være alternativer.

Hvis du går i en handlegate og du ikke kan se kameraene, så er det vanskelig å velge dem vekk.

Det dere nevner er stort sett fordeler for den enkelte i hverdagen. Er det verdt å tenke på?

Hvor stort problem er det? Skal du bare lage et vanvittig et system for to, fem, ti prosent? Hvor stort er det? (uklart – latter)

Altså, skal promillen få styre mengden? Skal vi godta det? (uklart) gjør du ikke det, så skjer det.

Er det noen som har noen kommentarer til dette? Det er jo et ganske kontroversielt standpunkt kanskje? Det er jo ikke nødvendigvis? Samfunnet tar jo andre valg før det mener at...

Jeg tenker, at du får lov til å velge det her selv. At du har muligheter og at du kan styre. Slik som det stod i brosjyren, de som ikke greier å bruke dette. Slik som de gamle som ikke har nettbank (uklart)

Hva tenker du om det? Tenker du om positive muligheten rundt det å bruke sånne systemer for å sikre og vite hvem som går inn på flyet? Ser du mye positive muligheter, eller ser du mer uheldige misbruk av det, at det er det store problemet?

That's a long question for meg. What are you looking at?

Hva er de viktigste mulighetene, de positive gevinstene? Det gode du kan få ut av de teknologiene vi har snakket om i dag?

Jeg har språk..

Speak english.

I have different views when it comes to society. I come from a society where security is not ... - even though I used to work for an organization that is security concious. Everywhere I go I

look around and there are people there, watching me or doing something of that kind. And then I come from a society where the kind of security we are talking about, is quite different, when I came to Norway for the first time. It was quite a different matter when it comes to issue of security. You see cameras everywhere. On top of the high (uklart)

Vil noen ha oversetting?

So, I'm questioning myself if the camera, for psychological reasons, that I will think at «somebody is watching me, so I have to be careful» or – I'm not able to do crime completely. And then I read about the robbery in Stavanger, and then I'm like hey, what is going on? And then you start to wonder and think seriously of the issue of security. In Sweden, for example, there was an armed robbery of a bank. And then the the police officer was a (uklart) of the robbery. All the money they stole from the bank, they gave to him. He kept it in the police statio (latter) So, who are you trying to arrest? The police-officer who knows about your robbery? You see, when it comes to this kind of situations, you really have to ask yourself who is the criminal here. The public? The mafias? We need to look at the factors to what actually contributes to security breach. People don't have enough to eat? (uklart) security system. Can we try to manipulate it? (uklart) You know, just to show the public and the government that they are not secure. (uklart) Not that they want to rob the bank. But okay, take the most secure bank in the world. So there will be som boys like «okay, we want to go there!». Not that they want to steal, but they just want to prove to you that you are not just secured. So they are not criminals. So, when it comes to the issue of security, I'm not of chance to the (uklart). For example, they introduced the fingerprint. I studied electronics, so I know that (uklart)
I say, if you tried to put super glue, to cover your thumb. Before you go for your fingerprint. Is this really going to show your fingerprint? No, because you have something on it! So it's not going to show! So this means that you defeated the purpose of the technology. (latter) So, it's, again, there was a time I was looking at the issue of the mobile phone. The only area where you can be safe, the mobile phone security, is maybe for the kids. Small small children, maybe when you kidnap them, (uklart) the authority knows where the person is. That one is good, but if you listen to what I'm talking to on the mobile phone, you don't have nothing to do. You are wasting public money. Everybody is not a terrorist. I know that when I talk to the authorities, I know that, I want to talk even though I not (latter)

Ja, jeg hadde et spørsmål hvor det står «hva synes du er de viktige potensialene for sikkerhetsteknologier», og der har vi jo fått nevnt forskjellig, men samtidig kommer vi jo fort over til at vi sier at det misbrukes lett. Det neste spørsmålet var egentlig hvilke negative effekter vi får av sikkerhetsteknologier er du bekymret for. Vi har jo prata litt om det, men. Forresten, før vi går på det. Er det et bestemt potensiale. Når vi snakker om de positive mulighetene, så var det først dette med effektivisering og bekvemmelighet som ble sagt. Så satt det med kriminalitetsbekjempelse og forebygging litt lenger inne. Er det rett at man da dermed ser denne effektiviseringen og bekvemmeligheten som det viktigste potensialet ved denne teknologien? Eller er det de tingene som samfunnet ønsker å ta vare på med disse teknologiene.

Hvem er samfunnet, er ikke det oss det? (uklart) flertallet!

Jeg heller nok mest til ta det ikke må være så bekvemmelig hvis det er frihet jeg. At du må ikke være så kontrollert og styrt og overvåket og alt det der.

Så bekvemmeligheten teller lite for deg?

Ikke lite, men i verden vil jeg være litt gammeldags? Jeg klarer meg ganske godt uten mobiltelefon. Vi trenger ikke gå tilbake, noe kan vi prøve å styre tenker jeg.

Teknologien går så fort nå, vi tar jo kjempesprang, jeg tenker om 50 år (uklart)

Jeg tror vi har fått et godt sammendrag av hva dere tenker, det er min følelse. Du hadde hånda oppe?

Det ble sagt i sta, men jeg tenkte på dette med London, hvor de hadde avverget flere terrororganisasjoner. Det er klart at det har masse positive.

Har det blitt mindre kriminalitet av dette?

Altså, mindre kriminalitet, du ser ihvertfall i Stavanger er oppklaringsprosenten mye høyere. (uklart) Det er en ting jeg tenker mye på med dette her er at samfunnet blir forferdelig todelt. De som kan teknologi og som mestrer dette. Så er det de andre som ikke kan og klarer å følge med, det blir så forferdelig. Jeg bor på (uklart, stedsnavn i Stavanger). Når jeg går i banken der og skal gjøre ett eller annet. Jeg ser de folkemengdene som sitter, pensjonister, de skal gjøre – ikke sant? Det koster veldig mye for dem, de må betale 50 til 70 kroner fordi, ikke sant?

Det er ikke lenge før vi sitter på denne benken.

Jeg tenker på dette med målbarhet. For eksempel hvis du starter overvåking i et område. Hvor mye mindre kriminalitet er der? Hvor mindre av ditt og datt? Nettopp fordi det er preventet. Jeg jobber innenfor sikker adferd. En bevisstgjøring på dette med sikker adferd som går på dette med å være observant i trafikken. Kan ikke på noen måte nødvendigvis måle hvor mange mindre drepte det blir, det er ikke alt som lar seg måle. Nettopp fordi at det er ting som ikke hender, det at du vil forhindre at ting skjer. Hvis du ikke hadde gjort det, så hadde det steget proporsjonalt.

Dette er bra, jeg tror vi går videre. Da skal vi gå inn på de negative effektene. Selv om vi har diskutert det allerede, så har det kommet mange momenter i forhold til det man kan være redd for. I forhold til at noen kan falle ut, at det kan være utro tjenere som misbruker det, det første jeg mente var at noen faller utenfor, noen får ikke brukt de effektiviserings og bekvemmelighetspotensialene som ligger der. Jeg kommer ikke på alt nå, men det har vært nevnt mye. Er det ett perspektiv dere ser på som spesielt stort negativt konsekvens av å innføre denne type teknologi på forskjellige områder?

Det er jo denne typen identitetstyveri som har vært nevnt. At du på et eller annet vis får tak i personnummer og klarer og lure til deg ting med det, og deretter klarer å skaffe deg store fordeler for degselv som kriminell og enorme ulemper for den uskyldige parten som kanskje må bruke årevis for å rette opp feil og rette opp rykte og rydde opp med kreditorer og ikke minst kredittverdighet. Det er ikke bare bare å ha masse anmerkninger, selv om det ikke er din skyld, så tar det lang ting og masse ressuser å få ryddet opp. Og av og til så er kanskje ikke banken så villig til å hjelpe deg heller.

Er det dette med identitetstyveri som dere ser på som hovedsak?

Nei, jeg stoler ikke på de som samler opplysninger, hvordan de samler det og hvordan de bruker det. Nå er det jo dyrere å slette det enn å opprette nye systemer. Nå er det så mye data, det koster en formue å få slettet hver enkelt, selv om du stryker med, så henger det etter i årevis. Den er det verste og det er det som skjer nå.

Jeg har et konkret eksempel og der data har blitt misbrukt. Det går på innregistrering av enheter. Det begynte med at de skulle, i hus med leiligheter, ikke sant? Det er mange som har leiligheter som ikke er godkjent, ikke sant? Det er jo en generell ting. Der vi i første omgang har brannvesenet som trenger å få vite hvor mange enheter det er i et hus, fordi at nettopp på grunn av den brannen. Og i etterkant, så begynner de å bruke de opplysningen for å se, husleie, nettopp sånne ting.

Kan du stole på myndighetenes såkalte sperrer? De henter jo inn overalt.

Noen ganger forventer jo vi, når man sitter med en opplysning i det offentlige, så er det jo det samme med denne bekvemmelighetsverdien, for det er jo enkelt når man sitter på opplysninger på tvers og man slipper å spørre.

Om det er den personen som bruker det, hvordan han bruker det, det kan vi ikke styre. Det kan være misunnelse, det kan være hevn.

Spesielt (uklart) vi kan jo være uenige i et demokratisk samfunn, tenker på sånne ting, når de blir innført, som er totalt (uklart), samfunn hvor makthavere kan misbruke det til de grader, ikke sant?

Er det et relevant tema i Norge?

Det er ikke umulig at det blir det. Sett at vi får en ekstrem høyrevriding. Det at et medlemskap i en nettside, der du har en politisk ytring, eller en seksuell legning eller et eller annet. Der at det blir en database på et kontor i Oslo, så hvis myndighetene faktisk vil, så går de bare til det kontoret, så klipper de ledningene, og så tar de med seg den databasen, og så har de en liste over personer med spesiell legning eller en mening, en oppfatning. Hvis jeg er medlem av en internettside der interessen av å være medlem er en seksuell legning eller et politisk parti eller hva som helst, der det kanskje er akseptert av samfunnet nå å ha den seksuelle legningen eller å være medlem av det partiet. Men hvis vi får en høyrevriding, så kan det være ganske uheldig for deg. Da kan det være vanskelig å bli kvitt det, for du kan jo slette profilen, men det kan hende at det som skjer når du faktisk trykker slett, er ikke at det blir sletta, men at den blir deaktivert.

Facebook.

Ja, Facebook.

Ja. Da har vi fått gått litt igjennom noen hovedmomenter som er store bekymringer. Vi har allerede sagt veldig mye, altså det at det blir pålagt nye oppgaver og forskjellig. Jeg tror vi går videre til å diskutere dilemmaet, avveiningen. Noen plasser er de fleste av oss. Det er jo i bruk, og det er rimelig at det er en viss form for at samfunnet tar teknologien i bruk for å begrense kriminalitet og for å gjøre det enklere for forbrukere. Nå vil jeg ha litt diskusjoner rundt hvor den grensen er, hvor den balansen må gå. Og da vil jeg først at dere tenker litt

gjennom på hvilke steder, eller i hvilke situasjoner, tenk litt på de scenariene dere har sett nå, synes du det er greit at sikkerhetsteknologiene går foran personvernhensynet, altså at du må være så sikker på ting går i orden at folk må gi avkall på personvernhensynet. Hvilke situasjoner kan det være mest aktuelt i?

Det klassiske i dag er flyplassen. Fordi, en persons ganske lille handling, for eksempel å slå ned piloten, kan få store følger, for du kan drepe i alle i flyet. Og kanskje kræsje det inn i en bygning og. Hvis du har med deg en kniv på et tog, hva får du gjort?

Du, hvis du tar (uklart), hvis du tar bilen og fyller den med sprengstoff så hadde det gått 2000 mann. Det er et ensidig fokus på fly, det er en ting, det er bare bare det, det kan være alt annet.

Det er mulig vi ikke behøver å diskutere det, men det at det er mange som er samlet på en plass, det er jo et kjennetegn at mange er samlet på en plass i offentlig transport, og det er jo sårbart.

Fotballbaner. Skoler.

Men, skoler, er det en plass hvor vi ønsker at vi skal måtte gjøre seg til kjenne med fingeravtrykk for at man skulle komme inn på et skoleområde, er det en aktuell ting?

Det er for langt.

Du har jo de episodene fra USA.

Er det av total (uklart) Er vi villig til å oppgi så mye, for noen få episoder? Ja, det er tragisk, *men* ...

Hvem var det som var inne på det? Da er det noen som vil utfordre hele tiden. Som du var inne på med det bankranet. Da er det noen som vil prøve bare for å se om de kan, ikke sant? Da kan det være at noen på en skole vil bare prøve for å se om de kan ...

Det er det jo på en arbeidsplass og. Sykehuset. Skal du ikke kunne komme inn på sykehuset før du har scannet irisen? (uklart)

Hva hvis du får revet ut øyet, så får du ikke brukt denne iris-scanneren?

I Norge faktisk, så er det fly, ennå er vi ikke kommet lenger, og jeg er jeg kjempeglad for. Jeg synes det er overdrevet det også jeg. Veldig overdrevet.

Nedre Karl Johan. Hvis man er der?

Jo, jeg tenker, men litt min sikkerhet. Det er ikke bombetrussel på Karl Johan. Det må jo være for å redusere litt kriminalitet, det er på et annet plan.

Det finnes andre måter å arbeide mot kriminalitet enn med data.

Ja, du kan jo ha mer politi på gatene, men det vil jo koste. Mer arbeidsplasser.

Men på skoler, det er et typisk eksempel på at det skal noe til.

Her i Norge er det jo oljeplatformer og sånn. Det er jo mange ting de kunne gjort i Norge hvis de hadde lyst til det. Så jeg tenker jo, javel, vi får være litt naiv da. Vi er jo ikke der. Hvorfor skal du lage.

Vi kan ikke sikre oss mot alt.

Det er jo en angstrening omtrent, å leve.

Du må bare gripe ordet på engelsk.

Egentlig så er jeg forkjemper for at det skal være mulig å gå rundt. For eksempel neders på Karl Johan. Hvis du vet at det er kamera der, så kan du gå rundt. Det er ingenting du må ha der. Du kan gå inn via taxi-inngangen på nordsia der, og kanskje gå forbi ett kamera, i stedet for å gå forbi 20 utpå jernbanetorget. Eller hvis du vil til Oslo, så kan du ta nattoget fra Stavanger, så er det ingen som vet eller har sett noe at du har kjøpt billetten kontakt. Så kunne du faktisk komme til Oslo uten å ha blitt registrert.

Men det du sa, så lenge det finnes alternative måter å løse den konkrete aktiviteten på, så er det mer akseptabelt, så lenge det ikke finnes. Du brukte jo det eksempelet med telefonmøter tidligere, altså, telefonmøter kan jo være et alternativ til fly. Det finnes noen plasser, arenaer, hvor det finnes alternativ til overvåking.

Men det rettferdiggjør jo ikke all den overvåkingen som er på en flyplass. Det må jo være for å unngå en fare eller å dempe en risiko, at vi har de sikkerhetstiltakene vi har på en flyplass. Det er jo aller best at de blir utsatt for det, og at de er klar over det, og ikke minst at de kan vise til rene forskningsresultater, som viser at vi har unngått det og det og det, selv om det er vanskelig å ofte bevise det. Det er kanskje derfor vi trekker frem disse sakene, at nå har vi funnet en bombe der, og nå har han blitt arrestert. Men, det er faktisk ikke, siden 2005, det er ikke veldig mange saker de har trukket frem. Hvis de vil skryte av hvor gode systemene er, så synes jeg det er rart at ikke det er mange flere eksempler på folk som blir tatt.

Det kan jo ha en preventiv virkning.

Det er jo det som er vanskelig å måle.

Kanskje, så tenker jeg, at de virkelig kriminelle, at de ligger jo gjerne foran sikkerheten uansett. Hvis du vil noe galt, hvis det er cluet, så kan det skapes ufattelig mye helvete i verden, hvis de bare vet det.

Tror du ikke politiet vet dette? Hvorfor bruker man det da likevel?

Jo, det er vel for å si at de gjør noe med dette spørsmålet. For å vise at joda, «her gjør vi noe», «her står vi på». Få politiet ut i gatene. Vi har behov for å kjenne at noe blir gjort. Menneskelige behov for at (uklart)

Hvis du ser på sikkerhet i forhold til nettbanken og pengene dine. Du vil jo at banken skal være på forskudd i forhold til sikkerhetshullene og de kriminelle som prøver å utnytte dem. Du kan jo ikke akseptere at banken sier at «nei, vi gidder ikke å finne nye sikrere måter», for eksempel å installere en fingeravtrykksleser på datamaskinen din. Vi kan jo ikke, hvis det er

det neste trinnet vi må ha for å sikre pengene dine, så ville du nesten gjort det. Vil jeg tro. Der sender de deg nye dingser i posten som du må bruke. En fingeravtrykkscanner, en irisscanner (latter), jaja, for alt jeg vet, fingeravtrykksscanner får du kjøpt på tastaturet i dag, så du kan koble opp til Windows blant annet. Nye Windows Vista har systemer blant annet for fingeravtrykksgjenkjenning. Så hvis du har en sånn fingeravtrykksscanner, så kan du låse opp Windows, sånn at bare du kan bruke det. I stedet for at du bruker et passord slik du gjør i dag. Det er tilfelle, noe i det siste i dag.

(uklart)

Jeg tror vi går videre jeg.

Vi må se nytten av det.

Vi må se nytten og ha alternativer, og så er det noen plasser hvor det er mange folk, hvor det kan være aktuelt å ha ...

Det er konsekvensene, at de kan være for store til at vi kan akseptere at det ikke kan gjøres noe med.

Jeg går videre til neste spørsmål. Nå er det igjen fire. Hvem bør være med å bestemme hvordan sikkerhetsteknologien kan brukes? Er dette noe som er for komplekst til at vanlig folk kan bestemme og stemme over det, eller er det sånn at det må overlates til eksperter?

Hvis det er deler som mannen ikke gaten ikke har en innsikt i, topptopp, så har vi likevel en kvalifisert mening uansett.

(uklart)Jeg mener, hva vil ha? Det tenker jeg, det er et demokrati. Hva vi er villige til (uklart) Derfor tror jeg at endel meningen kan ha en almenn. Det er jo mange som kan mye om det, så de må jo være med.

Detaljene er litt vanskelig å styre for hvermannsen.

Men det er jo en følelse av. Det dreier seg jo ikke bare om å forstå, men det dreier seg også om et verdivalg og forskjellig annet.

Du kan jo ikke sleppe de løs, vi blir jo umyndiggjort hele gjengeng. Du må holde de igjen disse teknokratene.

Samtidig så er det jo politiet, et av de spørsmålene der er jo. Et av spørsmålene der var jo i hvor stor grad kan du akseptere at data blir brukt i forhold til personvern. Når det gjelder politiet, som vi har vært inne på før, så vil de alltid kanskje ligge et hakk bak de som er kriminelle, nettopp fordi de må følge lovene og regler som vi sier at vi synes det skal være. Hvis vi får for stor vekt der, og vi ikke har den peiling på hvordan de for eksempel jobbe, så vil det kunne begrense politiet i sitt arbeid. Netopp fordi at de må følge reglene som vi, almennheten bestemmer.

Det må jo være regler (uklart, diskusjon)

Det er jo det som gjør at politiet alltid kan være et hakk bak, fordi de må forholde seg til reglene.

Hvis vi skal ta dette til ytterste konsekvens, så kan vi si at de kunne fulgt med på hvert enkelt menneske.

Det er jo det det er på vei til å bli (uklart)

Da får du jo styr på alt, all bevegelse, alt du gjør.

Det vil jo bli folk som bestemmer hva mat du skal ha, når du skal leve, når du skal dø.

Vi må iallefall følge med at vi får en sjangs til å (uklart).

Du får jo ikke lov til å kjøre bil engang, de skal bestemme hastigheten, og hvor fort du kan kjøre.

Hva slags arenaer ser, de fleste mener at folk flest faktisk har kvalifiserte meninger rundt det, at det er verdispørsmål, og at det derfor ikke bare må overlates til fagfolk. Men, hva slags arenaer har vi for å nå frem politisk og få påvirka beslutningene? Er det noe som peker seg ut som kan være aktuelle å jobbe gjennom?

Den jobben dere gjør, for eksempel.

Blir en hørt? Eller blir det bare kasta ut penger fordi at det skal høres fint ut for staten? Eller blir det brukt? Det er fasaden som, det er jo dette, «jeg hører hva du sier, men ok».

Dette kan vi diskutere videre.

Det er jo den faren, selv om jeg skjønner hensikten bak det.

Vi blir iallefall aldri bedre enn de folka som vi tar med i det. Så det er dere som gjør oss gode.

Men, altså, det er ikke det jeg mener, det er de folka som tar imot denne greien. Har de vett til å skjønne det, eller lever de på en fjern planet, isolert fra resten av befolkningen, eller er de en del av den?

Jeg har alltid hatt en tanke i forhold til det med DNA iallefall. Hvorfor kunne ikke (uklart) hvorfor kunne det ikke vært slik at når vi ble født så ble det registrert DNA, tenker jeg. For gjør du ikke noe galt, så er det ingen problem. (uklart) Du kan klone det, tenker du? Ikke hviskre.

Det er altså veldig viktig å ta opp disse her spørsmål i forum som dette. Det er klart det at det er veldig få politiske saker som jeg kan huske, som går på dette her, det kan ihvertfall jeg ikke huske på.

Det er for lite på dagsorden?
Ja, absolutt. Dette er veldig bra, hvis det altså (uklart)

Det er jo stort sett det man ser på alle restriksjonene i media. Det er jo for eksempel at politiet

sier at «hvis vi kunne, så kunne vi stoppet den og den». Det andre vi ser er med de tilfellene når Datatilsynet har stoppet eller anmeldt et eller annet foretak for å ha gått over grensa. Ja, for da er det bedrifter som får bøter fordi de har overskredet grenser for hva som er lov å registrere på data. Men et sånn ultimatet, disse etiske reglene som vi har nedfelt i personregisterloven.

Du kommer ikke uten om det, for du trenger ikke oppgi personkodenummeret ditt når du skal ta ut penger fra banken.

Det som vi kan gjøre direkte er jo å velge de politikerene som har de meningene som du har selv. Det er jo sånn vi styrer. Så har vi de hemmlige tjenestene som vi ikke vet så mye om. Hvor mye politisk styring har de?

Akkurat det du nevner med hemmelige tjenester, det ser vi i dag, hvor folk har vært ute på telefonen og sånn, ikke sant? I den kalde krigen. Hele Arbeiderpartiet hadde husa sine fulle av ledninger overalt. Og alle de som tilhørte kommunistpartiet og så videre.

Did you have a question?

No, I was just asking him on what the discussion was about.

We were bringing up so many questions.

The last question was about who should be involved in the decissionmaking about how to manage these technologies. Whether these issues are too complex for just a normal guy to get a grasp of the overall challenges of these issues, or whether these are valueladen questions that can not only be given to experts and central politicans, but have to be given to involve people.

I think everybody should be involved. Because the end-user, the designer and the authority are the three people who should be involved. Somebody is going to use, somebody is going to implement whatever (uklart) the abuse. There is an interesting case, for example, in the US, it's an old man. He has his grandson with him. The grandson went on online on the internet to download some music and videos, and then they got the ID and they traced the adress and they got the boy arrested. And then they said they should plea about 3000, 15000 or 20 000 dollars. These are no money, he hasn't got any money. He said, he is a boy, he is not me, he is under age. They said «no, you are responsible». He leaves under your house. (uklart) so, who is responsible? Everybody should know what is going on. In my own home, we control the internet-connectin ourselves. I want to know precisely what is going on. I don't have the you to go to prison, because I don't have the time to go spend it with you there. So it's my responsibility, it's the responsibility of everybody else.

Jeg tror vi fortsetter. Har folk formeninger om det bør være noen begrensninger om hva slags teknologi som utvikles. En ting er jo hva slags teknologi som finnes og hva som utvikles, en annen ting er faktisk hva slags teknologi som blir tatt i bruk. Er forskning og utvikling av teknologi på området her noe som bør begrenses og vurderes, eller er det i det hele tatt mulig?

Jeg tror det er umulig, du kan ikke hindre noen i å komme på en mekanikk som kan lese. Hvis jeg finner på en eller annen måte å sikre huset mitt på. Hvis jeg lager en irisscanner og bruker på mitt eget hus, hvis jeg lager patent på det. Du kan ikke nekte folk å komme på den tanken.

Er det mulig å for eksempel, å si at den og den, en ting er at du kan lage noen almenne personopplysningslover som begrenser litt hvor mye data du kan lagre, men kan du stoppe visse teknologier? Kan du si bare nei til kameraer, kan du si nei?

Det går an.

Det er utrolig vanskelig da.(uklart)

Jeg vil tro at en teknologi som kan gi en fordel for en eller annen, vil tvinge seg frem uansett. Om det er lovlig eller ikke, så vil det gå under bakken. Så jeg tenker det er en fordel, spesielt i forhold til økonomisk gevinst.

Altså, teknologien er en del av medisinforskningen. (uklart)

Så det er litt determinisme, det skjer uansett. Så da er det reguleringer av bruken som er måten å.

Ja, bestemme ut i det offentlige rom.

Ja, ut i det offentlige er en ting. En del ting gjør jo folk på hjemmebane. Skal det være noen begrensninger på hvor mange videokameraer jeg kan ha på hytta mi?

Eller skal vi gjøre som Kristian Valen som har 14 tv-kameraer hjemme hos seg selv? (latter)

Sånne ting kan jo også være en utfordring noen ganger.

Men det er jo da viktig at da for eksempel Datatilsynet har myndighet nok til å faktisk kunne undersøke et datasystem. Om det er bakveier, om det er ting som blir ulovelig lagret og sånne ting. Det forestiller jeg meg kan være vanskelig. Jeg forestiller meg at for eksempel på en webserver, må de omentrent gå inn på serveren og sette seg ned med teknikere, og sette seg ned og lete etter bakdører og ting som blir logget, sendt til andre servere. Det er *utrolig* vanskelig innenfor datateknologien å finne ut hva som skjer på en server. Selv om det er lover og regler som sier at det er lov til å lagre, sånn og sånn – hvordan kan de sjekke at det blir etterlevd? Det er ofte en utrolig vanskelig.

Tilsynsoppgavene er mer utfordrende en lovgivningsoppgavene?

Det tror jeg er tilfelle. Summert opp hvordan jeg tenker.

Nå skal vi begynne å avrunde med hva vi synes om diskusjonen. Da vil jeg spørre om dagens arrangement, om deres deltagelse har endra holdningene deres til teknologi, altså sikkerhet, sikkerhetsteknologier og personvern, om det er noen nye betraktninger en gjør seg, rundt det dilemmaet, hvordan det skal forvaltes? I'm asking whether today's meeting has changed your attitudes towards the dilemma of the balance between security and privacy.

Jeg har ikke forandra meningene mine, men jeg har blitt mer oppmerksom på dem.

Helt enig (flere samtykker)

Og hvor viktig er det for å bevisstgjøre for andre og? Sånn at du kan la være å gå inn i en gate med videoovervåking. At du kan vite at du ikke behøver å registrere betalingskortet ditt på bussen din. Du kan faktisk betale kontant.

Så det er en stor informasjonsoppgave der, det er jo et ganske godt poeng.

Jeg kjenner vel at angst for å svare, at jeg ønsker jo at politiet kan bruke mye i etterforskning, men det må ikke være for å ta alle for sikkerhets skyld, i tilfelle det skal være noen potensielle forbrytere, det må ikke være sånn. Det må være sånn at de kan koble og gjøre endel ting som er mer konkret med. Sånn som det står om rettslig kjennelse, at det er visse regler for det og. Det er ganske viktig for meg.

Hva om du gir dem personkoden og fødselsnummeret ditt, så finner de *alt.*

Men paradoksalt nok, blir jo saker henlagt. Selv om du har filmer av overfallsmann så blir saken henlagt. Du har alt på film, men henlagt på grunn av bevisets stilling.

Der har jeg konkret et eksempel, jeg jobber i butikk og der var det nasking og tjuveri og det var et vitneutsagn som var konkret med navn og adresse på fyren, for vi visste hvem det var, så hva han gjorde på video, men det ble henlagt på grunn av bevisets stilling.

Da er det jo nesten ikke vits i da.

Politiet sendte bare et brev, «henlagt på grunn av bevisets stilling». Det koster en jurist et kvarter og skrive et brev om henleggelse. Hadde de skulle etterforska, dømt fyren og kanskje fått han i fengsel i 15 dager - så haddet det kosta mye. I forhold til den skaden han har forvoldt.

Det er bedre å bruke de pengene på folk som langer narkotika kanskje?

Det er jo et bevisst valg. (uklart)

Hva synes dere er viktig, det er jo opplagt et dilemma, skal vi bruke alle ressurser på vold og kriminalitet og forebygging av alvorlig handlinger i så måte. Altså, alle har jo sine definisjoner av hva som er alvorlig, men, sånne dilemmaer sitter man selvsagt med. Men, dette er ikke snakk om teknologi.

Men hvis det overtar mer og mer, så kunne vi jo risikere et samfunn hvor du som borger vil kunne ta saken i egne hender. Borgervern ja, rett og slett.

Fordi du føler deg urettferdig behandlet. (uklart, mange snakker på en gang)

Teknikken skal forenkle, det er det som ligger til grunn for det hele.

Jeg kom på et moment i forbindelse med det butikktyveriet. Okey, da har du vist for deg selv at video i butikken, greit, vi har det, men det er ikke preventivt. Det hjelper oss heller ikke noe når det faktisk har skjedd noe. Vi må bruke masse tid på å holde det i gang og skifte videokasetter. (uklart)

Bensinsstasjoner spesielt, det står jo bare attenåringer bak kasse.

Hvis det da ikke hjelper, hva er det vitsen med å ha det, hvis det da ikke helper.

Det er jo om det er forebyggende da. (uklart, mange snakker samtidig)

Men jeg tror vi, nå har vi siste spørsmål, og da skal vi ta en runde og hver enkelt av dere får ordet. I forhold til å gi noen sluttkommentarer, noen betraktninger rundt teknologien. Vi kan gjerne formulere det sånn at hvis du har ett minutt til å prate med Jens Stoltenberg, til å prate om noen av de teknologiene her, hva ville du sagt? Og da kan vi, you have one minute for a last appeal. You have meeting with the prime minister, Jens Stoltenberg, and you can give him your final remarks about how to, any remarks, not only about management, but also about how to, how the society should relate to this. You can start.

Okay, I think in a democratic society, that they are disclosing the implementation, that it's a very good step. I think that they should also send out the discussion, and (uklart) that the masses should be aware of what is going on, what is being implemented. So that in the end of the day you know what you are lead into. So if you are going to tap my phone, just let me know that you are tapping my phone, and don't come and use it as an evidence against me. And with this technology, we are in a situation. We are talking about digital, not analogue, alot of things are possible these days, so people should be suspicient about what is going on. Training, learning in the language and everything. There should be alot of investment, especially in educating the masses on what is coming up. Because if a farmer is going to be an engineere, there must be a way to communicate, so that everybody knows what is going on.

Thank you.

Thank you very much.

Jeg tenker igrunn mye at det er viktig at noen hemmelige tjenester må det jo være, av hensyn til rikets sikkerhet og blablabla. De tiltakene som blir gjort ovenfor de større massene er utrolig viktige at vi blir informert om, at vi vet de er der, og at vi vet hvilke typer ting som blir tatt opp. Bevisstgjøring er *så* viktig altså. Synliggjøring, at vi kan *se* at kameraene er nedi gata. Det er lettere for skurker og gå rundt også. Det er nå så. De får ihvertfall stoppa det som er i nedslagsfeltet til kameraet. Men kanskje det er det som er hensikten.

Da tenkte jeg altså at vi har lov å velge en del ting. At vi fremdeles kan velge. Vi kan ikke velge hvis vi ikke vet. Det må være, selvfølgelig kan vi bruke disse teknologiene, men det må være kontroll, det må være endel regler. Og så ikke hoppe på den terrorangsten for alt, at den ikke må styre Norge.

Det jeg mest tenker er at vi må få informasjon. Jeg tenker meg og vennene mine, det er mange som har tusen sider på internett, og vi legger ut informasjon om oss selv. De vet ikke hva det blir brukt til vet du. «kult det», moderne dingser som kommer, men de vet ikke hva det er og hva det gjør på.

Kort og godt bare vi tar litt mer hensyn til folka på gata (uklart). Tar de med på råd, det er da vi kommer lengst. Da får vi gjennomsnittet av gruppene tenker.

Jeg er veldig enig med deg. Informasjon, informasjon, informasjon. Når blir du overvåket. Hva skal det brukes til. Hva er konsekvensene? Hvor lenge lagres det? Vi må bli bevisste på hva som skjer rundt oss.

Det er lurt, alt som er sagt her. Først og fremst, kanskje det altså, at vi hadde tatt det på skolenivå. Hvor gammel er du? Det er kanskje ikke lenge siden du gikk på videregående?

Jeg går på videregående.

Ja, og så kan du ikke mer om dette. Vet du, det er helt skremmende. Det må tas opp, inn i skolen. Det må tas inn i pensjonistforeninger og så videre og videre. Så må det gis penger til teknologisk forskning. Jeg synes det er viktig å være på toppen der, hele veien. Sånn at vi er de som er på toppen og vet og kan, slik at vi ikke følger andre nasjoner, og så sier «hva er det de har?» Så prøver vi liksom å krabbe unna. Altså, da, det er best å (uklart)

Ja, at vi kan styre vår egen utvikling og vite bare.

Jeg var på «Flo og fjære» (?) en gang og da sa han at «vi må styre trærne, ikke at trærne styrer oss». At vi må kappe ned trærne og ha kontroll med planter

Gruppe 4

Sånn, det var det. Jeg har en slags guide for dette her, så vi skal følge en slags plan. Jeg bare lurer på, skulle vi, hadde vi klart oss uten de to bordene der. (organisering av bord, bråking og snakking i munnen på hverandre)

Jeg tenkte, da skal vi bare begynne med en liten runde hvor alle sier hvem de er. Jeg heter Jon Vigsdal, er forskningsleder i Teknologirådet. Jobber til daglig med ikke denne type teknologi, men energi- og miljø-problematikk primært. Kan dere bare si to ord om hvorfor dere synes det er morsomt å være her, det er litt spennende med akkurat hvorfor.

Jeg skal bare si navnet først?

Jeg heter Per Kristian Pettersen, jeg jobber til daglig som pedagogisk leder i barnehage. I og med at jeg jobber med barn, så synes jeg jo dette er viktig inn i framtida, synes det er interessant.

Jeg heter (uklart) og jeg jobber som teknisk tegner og interiørkonsulent. Jeg synes det er interessant sånn fremtidsmessig å være med på en diskusjon om sikkerhet og elektronisk sporing og sånne ting.

Jeg heter Britt Lyberg, jobber i barnehage som assistent. Jeg er mormor til 4 unger og er veldig spent på hvordan det blir i fremtiden med sikkerhet og overvåking.

Jeg heter (uklart – noen kommer inn)

Jeg heter Ragna Sandve Rogne, jeg jobber som økonomisjef i kommunen. Da jeg fikk spørsmål om jeg skulle være med, så tenkte jeg med en gang at dette ville jeg, uten at jeg visste hvorfor.

Har du funnet ut noe om det?

Det er jo egentlig et ganske interessant tema, og det er omfattende og vanskelig.

Jeg (uklart), jeg er statsautorisert translatør til engelsk, og jeg underviser på en videregående skole i engelsk. Jeg er opptatt av informatikken, en viktig problematikk, og enkeltvis fra et humoristisk synspunkt. Jeg har vært det helt siden jeg leste Orwell for femti år siden. Han var forut for sin tid som tok opp dette.

Jeg heter Johan Bergli, bor i Stavanger, jobber i (uklart) som økonom i et eiendomsfirma. (uklart) personvern er utrolig interessant. Det har vært en sånn, siden 2001, en kamp, og det er mange som har blitt irritert. Men det er dette med høringer, hvis man kan få sitt synspunkt fram, så er det fint.

Det er bra. Vi har en intervjuguide med i alt ni spørsmål. Vi begynte på toppen, jeg er helt sikker på at vi kommer til å få litt overlappende svar. Vi har en time på oss, så i overkant er det 7, 6-7 minutter på hvert spørsmål. Dere trenger ikke alle å svare på alt, poenget er at noen kan kommentere, så kan dere samtale med hverandre, hvis dere føler dere har lyst til det. Så tror jeg bare vi begynner, så kan jeg passe progresjonen.

Det første spørsmålet er dine umiddelbare tanker om sikkerhetsteknologier og personvern. Jeg vet ikke om dere har gjort dere noen generelle refleksjoner om det hele. Dere har sagt litt allerede. Har dere noen flere?

Jeg selv ønsker at det skal være veldig mye overvåking. Men jeg føler ofte at jeg står med den tanken at jeg føler sånn motbør når jeg skal diskutere det med bekjente. Da er det liksom, «åå, vi blir overvåket hvor enn vi går, på butikken, når vi går av og på bussen». Jeg fatter egentlig ikke den frykten for å bli overvåket i eget land når du ikke har gjort noe galt. Så jeg er sikkert steindum som ikke fatter hvorfor folk har så mye imot å bli overvåket, jeg fatter det ikke. Altså, motstand mot å bli overvåket, om jeg gikk av og på den bussen og om jeg gikk inn og ut av den butikken. Jeg begriper det ikke, hvorfor folk er så redd for overvåking. Det, er det noen av dere som har noe å si?

Altså, det er to ytterpunkter. Enten så kan du gå tilbake til Stasi i Øst-Tyskland, der du ble kontroller av lederen. Eller du liksom kan ta det andre ytterpunktet, totalt anarki. Så her vi lever nå i dag, så må det bli et visst personvern. Men det må jo være styrt av myndighetene som legger føring og krav til bruken av den sikkerhetsteknologien du snakker om.

Ja, eller de ulike typene.

Ja, jeg lurte jo på når jeg kom til dette sted, om det egentlig passet for meg, fordi det er Teknologirådet, så må det være et teknologisk perspektiv. Jeg er opptatt av det, og imot å ta i bruk all denne teknologien i omfattende dag, for jeg er redd for hva det vil gjøre med oss som mennesker og med samfunnet, hvordan vi skal omgås og være i forhold til hverandre. Allerede nå så bruker du et teknisk instrument for å si det gjør, det binder meg, det er noe annet enn å bli satt sammen (?). Tenk om den teknologien som har blitt presentert, hvis alle de blir tatt i bruk, så blir det det Orwell-samfunnet jeg har der. Jeg skrev som kommentar at jeg er glad for at jeg er (uklart). Å vite at du ikke kan være fri.

Det poenget her er jo at det er ulike meninger, så tar vi jo, vi trenger jo ikke forfølge alle som kommer fram, men at vi har forstått hva du mener?

Jeg synes det må være, som han sa, en viss grad, men – den totale overvåkingen av absolutt, påbudt og når, om du skal kjøre buss kontra det å kjøre fly, om du skal inn i en bank eller... Noen ting er kanskje litt nødvendig, for eksempel scanneutstyr på en flyplass, men - ut over det synes jeg det ikke er nødvendig. Da har du gjort det du kan, sånn at noen ikke skal, hvis det er terror, for å forhindre terror, så har du gjort det du trenger. Du trenger ikke vite alt av (uklart), hvor du har jobbet, hva du har lest i biblioteket de siste ti årene. Det skal i utgangspunktet bare være på fly. At det må mer styring i forhold til hvor behovet er, hvor man trenger det.

Jeg er og av de som er skeptisk til alt for mye bruk av denne teknologien. (uklart) det som er rettet i forbindelse med terror og sånne ting. Og kanskje så kan det være nødvendig med en form for teknologi sånn som det. Det er ikke noe som skal slippes helt løs, sånn at du kan spores opp uansett hvor du går, uansett hva du har gjort. Til slutt så blir du, ja, når du sitter på do. Satt på spissen. Jeg synes det er skremmende, å ikke kunne bevege seg fritt.

All teknologi kan misbrukes uansett. Så det vil være personer som prøver å utnytte den, uansett. Det er mitt utgangspunkt. (uklart) Trenger ikke være kriminell for å skape.

(uklart) kriminell i mine øyne.

Det er jo et paradoks at med en gang teknologi blir kritisert så ser man seg tvunget til å ta den i bruk(uklart ?) Norge er sikkert i forkant der. Sammenlignet med Tunisia så er Norge et trygt land. Jeg synes det er veldig behagelig. Det er jo tross alt det araberverdenen gjør, av skadevirksomhet der. Da kan man kanskje vurdere, selv om det er mer roligere i forhold til en del andre – det er bare så slapt, det satt en mann der og halvsov, så gikk det en trikk av et gammelt system. De passet ikke på. Men her i Norge som er et trygt land så er det denne frykten. Det er et sikkert land og det skjer nesten aldri noe. (uklart) ramaskrik – undergrunnen i New York. Det er denne frykten som styrer oss.
Det er bra, da har vi fått noen umiddelbare kommentarer. Så kan vi komme tilbake til alt dette her. Da er neste spørsmål, om dere har kommentarer til scenariene som ble dere tilsendt. For eksempel om balansen mellom sikkerhet og personvern blir ivaretatt, om det er viktig å kunne få den type fordeler som er skissert i scenariene, om det viser en forlokkende fremtid, eller en skremmende fremtid. Om dere har noen kommentarer av denne sorten?
12:50

(uklart) kontoret – ja, akkurat sånn kan det brukes, misbrukes dette her. Hun var så pliktoppfyllende at hun ringte og ga beskjed, som om det ikke var godt nok (?). Så, det var sånn som jeg satt og tenkte da jeg leste. Da blir jeg skeptiske til den bruken.

Som scenariene beskriver? - Ja

Det er forsåvidt ei side av saken.

Det å sammenligne oss med andre land og full overvåking (uklart). Hvis jeg skulle ha en chips om hvor jeg gikk inn og ut. Det der med videoovervåking i Stavanger, de blir jo overvåka hele veien, det der med at hver eneste kunde skal overvåkes. Det bryr de seg ikke om, men på flyplass, det er så tåpelig, jeg fatter det ikke.

Det er jo en side av saken. Om ting blir tatt bilde av og så sletta, men alle personopplysningene, livet ditt, at alt på en måte skal...

Hvem skal bruke det? Hvem har glede av? Ingen får vite, om det skal brukes, i tilfelle.

Det vet du ikke.

Stoler du ikke på landet? (folk snakker i munnen på hverandre)

Makt korrumperer. Du vet ikke hva det skal brukes til. (uklart – mange flere snakker samtidig – latter)

Siden du nå snakker om scenariene, er det sånn å forstå at du ikke ... ?

Jeg er ikke sjokkert i det hele tatt. Det er så mye dritt i samfunnet, kriminelle og narkomane, folk som slår ned hverandre og blir helseløse. Det skjer så mye dritt, å begynne å snakke om terrorisme og slik, for noe tull. Full overvåking, ingen kan misbrukes, for, hva faen, hvem har glede av å sitte å overvåke hva jeg gjør? Jeg fatter det ikke. Jeg fatter ikke frykten for å bli overvåket. For vanlig folk kan det ikke bli misbrukt hvordan du lever.

Hvis du tenker på bare myndighetene så jeg kan forsåvidt, greit nok. Men du er ikke sikker på om det er bare myndighetene som får de opplysningene. Systemet kan være troverdig, men noen finner alltid ut til syvende og sist. Om de ikke går på deg, så kan de ta naboene, de kan ta hvem som helst. Å ruinere dem, du har ingen garanti.

Hva er vitsen med å bo i Norge hvis du ikke kan stole på ditt eget folk og din egen regjering? Du kan flytte hele gjengen. (folk prater i munnen på hverandre)

Det er ikke bare Norge, du må se litt lenger. Det som gjorde det interessant for meg, det er at jeg har barn som studerer IT. Blant annet en datter som studerte blant annet i New York. Hun skulle hjem en tur fra New York, plutselig blir hun (uklart), de hadde registrert hvor mange ganger hun hadde registrert ut og inn. Det synes jeg er skremmende. De tok henne inn på et rom og de spurte hvordan hun hadde økonomi til å reise så mye ut og inn, sånn frem og tilbake. Da er det litt sånn at det for meg, «hva holder de på med her?» Min datter satt på toget en gang i Frankrike, da fikk hun beskjed om at det var en bombe på toget, sønnen min bodde i London i to år, og han blir programmert til å tenke, og Gud, da tenkte jeg. Og da begynte jeg å tenke sånn at jeg vil ikke at de skal kunne spore meg. (uklart)

Hva med å spore terrorister? (uklart, flere snakker samtidig)
Men altså, jeg spurte om scenariene, kanskje vi burde få noen supplerende kommentarer? Men jeg vet ikke, kanskje noen har noe mer direkte på scenariene?

Altså, jeg kjente meg veldig godt igjen i (uklart), at de skal kunne identifisere oss på trikken. Jeg kjente meg igjen (uklart) Han gleder seg til å reise bort. Det kan føre til at mennesket låser seg inne. At folk ikke vil gå gjennom alt dette spillet. Mange synes dette er ubehagelig. Jeg må alltid ta av meg skoene på flyplassen. Jeg synes ikke det er så kjekt. Kanskje jeg ikke synes jeg har så pene føtter. Denne damen som var middelaldrende, kanskje jeg identifiserte meg med henne. Hun var livredd for å kle av seg, ikke sant? Sånne scenarier som denne ser vi for oss. Jeg synes det er veldig ubehagelig, jeg gruer meg. Det er noe inni meg som hindrer meg for å søke opplevelser til å dra ut, kanskje ikke alle så impregnert og så tøff som noen her som ikke bryr seg om noen ting. Mennesket et forskjellig.

Hvordan synes dere scenariene var balanserte i forhold til sikkerhet og personvern? Kom det fram både fordeler og ulemper, eller hadde de slagsider i noen retninger?

Det var jo litt nyansert med han unge, til slutt så fant han ut de begrensningene, han var jo forelska, tenkte han skulle begynne først. Så skulle han ringe til ei dame, så begynte han å tenke gjennom det. Hun blir lyttet på, det liker ikke hun, da kan hun få problemer. Da kommer det jeg sa om (uklart) Disse menneskene kan ikke leve i relasjoner som ikke kan være naturlig. Det er ikke så enkelt å være menneske og ha gode relasjoner. Så det synes jeg kom veldig godt fram.

Er det noen andre?

Det er jo litt sånn. Han drar jo på en måte, han forandrer ikke mening, men han får dra nytte av det som var positiv med det som var positivt med den raske innsjekkingskøen. At han da, det som var dårlig var at han ikke kunne, av frykt for å få en eller annen reaksjon, nå eller senere. At han ikke kunne snakke med den personen han hadde lyst til. Den jenta som hadde

sent ham triste meldinger. Da er man litt på ville veier. At man kan risikere å ikke få jobb kanskje, at det direkte står på ditt rulleblad at du har snakket med noen som er mistenkt for eller kanskje er sannsynlig for å være terrorist eller hadde sånn tendenser. Nokså interessante scenarier synes jeg.

Noen flere kommentarer? - nei. Hvis vi nå skal prøve å skille litt mellom hva som kan være positivt og hva som kan være negativt først. Hvis vi tar det positive først, hva ser dere at vi kan oppnå med sikkerhetsteknologi, hva er det man kan oppnå, hva kan de positive mulighetene være?

Teknologi går jo alltid fremover, så for meg vil det alltid være positivt. I en setting vil jo teknologi være positivt, fremskritt er positivt. Selve krav til bruk er jo...

Har du noen eksempler på hvordan det kan være positivt?

Dette med bilsystemet, dette med sporingsgreiene. Det kan jo være nyttig. Men det må ikke være et krav at du må ha det i bilen, og at du kan spores til enhver tid. Det kan jo være nyttig å ha det i et gitt tilfelle. Men det må være mulighet til å slå det av. Det må være flere muligheter til å regulere det.

Det er best å ha to muligheter (mye uklart. Tar noen bilder?)

Vi får bare diskutere vi, så kommer – ja. Men, ser du noe positivt utover bilteknologien, er det noe annet du ser?

Jeg får jo ikke satt meg inn i all teknologien, men det er klart noe som folk diskuterer er jo dette å kunne finne seg (uklart), kriminalitet. Hvis det ikke bare er en illusjon at det fører til at det blir... Men jeg tror ikke. Akkurat nå mister jeg litt.

Jeg selv tenker sånn positivt, hvis du kan ha et samfunn der du på en måte kan være sikret der du trenger å være sikret. Og at du ellers av tiden kan være anonym. Hvorfor skal man vite absolutt alt om deg om du skal inn på et kjøpesenter. Om du skal innpå et kjøpesenter, en buss, et bibliotek, eller hvor som helst. Det er ingen vits i. Det er greit at ikke hvem som helst kan ta med seg eksplosiver, kjemikalier eller sånt, det tenker jeg.

Vi har jo positive ting på dette og. For eksempel, i forbindelse med ranet, så har de kamera som følger veistrekningen. (uklart) slik at en mann kan følge bilstrekningen. Hvis du for eksempel ble frastjålet bilen din, at den kunne bli sporet. (uklart) Så visste de hvor den bilen var. Så det *er* jo positive tilfeller også. Men det er noe annet å finne frem og oppsporer også. Men det er noe helt annet enn at, okey, Hanna, nå var jeg der – og nå er jeg *der*.

Men kjører du for fort så kan vi gi deg fartsbøter. (latter, mye snakking)

Det er bra, da spørs det om vi går på det negative. Dere vil jo være litt frem og tilbake her, vet ikke om det er, hva er det som går mer direkte på det negative?

Jeg tror faktisk det gir en falsk trygghetsfølelse. (uklart) I fjor på eksamen, så var det en oppgave der om videokameraer i England. Så skulle lærerne, så var oppgavene at man skulle gi argumenter for og imot. Og dette brukte jeg i vår og dette har lært meg i samtale med vår sånn som er 17-18 år, (uklart). Jeg ble litt skeptisk til noe av de skrev. De så ingen

motforestillinger, for de skrev at (uklart) kjøpesenteret, når man går der, at man følte seg tryggere, at politiet kunne komme å ta dem tidligere. Dette synes jeg er en rar tenkning, det er jo det at når det skjer noe, så er ikke politiet der. Mennesker blir drept i sine hjem når det er kameraer der, så kan politiet sitte på sentralen og høre på skrikene til hun som blir drept og da skjer det på fire minutter, og da er det kjekkere enn å se på video på TV'n. For dette mennesket er dette likevel et faktum. (uklart) på butikken var det en dame som politiet hadde sittet å hørt på en dame som hadde sine siste minutter.

Disse enkelttilfellene får alltid (uklart). Det er jo ikke det som er det negative med teknologien, den fører jo at livet blir lettere for politiet. Skal du ha to kameraer og en mann? I slike tilfeller glipper det jo (uklart)

De elevene har jo ikke livserfaring eller noen ting. Altså, når du ser 17 år, så ser du på bildene at, de har ikke livserfaring, så sier de: «nei, er det sånn?»
Jeg tror at om noen skulle slå meg ned på et kjøpesenter, at hvis det var et kamera der, jeg tror at de skulle kunne slå meg ned likevel og ta mitt kredittkort. Jeg tror at denne tryggheten er illusorisk

Nei, det tror ikke jeg (mye snakking). Det er jo sånne enkelttilfeller som han sier. Sånn som når de overvåket i Havana, det barnet som lå under så lenge. Det ble etterforsket så lenge. De hadde jo forklaring. Det er ikke mulig å få sett alt sammen, det er ikke det.

Vi må jo se alle nyanser, det er jo ikke.

Ser du noe negativt?

Det jeg kan tenke meg er at uvedkommende får tilgang til informasjon. Det scaneriet der de unge folkene som kan se på mobilen, når mor, svigermor kommer på besøk. Det er bare noe tull. Jeg mener så lenge det er politi eller myndigheter som har en grunn for at de skal inne å se på en film eller både telefon, mobil, overvåking må ha en årsak. Sånn som han gutten som ble slått ned på bussen. Det viser jo hvordan (uklart) Det må være rom for å hente frem en opplysning. Allikvel så er det bare bortkasta. Jeg er ikke negativ mot overvåking, men jeg er for personvern, det å passe på folk. Rett og slett. Det eneste negative er uvedkommende som bruker opplysningene til noe helt annet.

Jeg synes heller ikke vi må gjøre oss for avhengige av denne teknologien. Hva om den feiler? Kan den slå feil? Hva gjør man da? Hva om vi slutter å tenke? Slik at vi blir handlingslammet?

Det er sannsynlig at mennesket gjør feil før teknologien gjør det.

Ja, helt enig.

(uklart)

Men er den største trusselen at?

Det at sikkerhetsteknologien blir brukt, den blir så omfattende og det blir lagret så mye at det til syvende og sist går ut over fullstendig alle blir overvåka. Det blir nesten sånn Stasi. Alle informasjon, ikke bare bilder du har vært på en buss engang, sånne ting anser jeg som nokså

uskyldig. Det er greit å vite at det blir sletta etter en viss tid, hvis det ikke skjedde noe på bussen til Sandnes, så blir de sletta. De blir ikke lagra på en harddisk de neste 1000 årene. Så jeg synes dette med personvern, en ting er at myndighetene ikke vil deg egentlig noe vondt – det tror jeg ikke. Men det er nok av andre som vil, som kan bruke de opplysningene til å tjene penger.

At du har, at du går å lever med den følelsen at alle kan fortelle deg hva du har gjort ti år tilbake, det frister ikke meg.

Om jeg er der eller der, eller om jeg har kjørt bilen min sånn. Det er veldig ubehagelig. Vi har jo våre private liv, og de skal vi verne om. Jeg tenker på den populære serien, Sopranos, når de skulle virkelig planlegge noe, gikk de to og to ut i en skog. Uten mobil, uten noen ting. Dette var den enste måten de kunne komme unna på. Men, fremtidssamfunnet er her. Jeg finner meg i, at alt jeg gjør, etterlegger seg spor fra jeg går ut av døren om morgenen til jeg kommer tilbake. Jeg har sitter å lurt på om jeg kan skrive dette i denne mail. Jeg jobber endel for et amerikansk oljeselskap. Selvsagt i det profesjonelle så bruker jeg å være formell, men når jeg skriver til venner så bruker jeg en mer et uformelt språk. Jeg har lurt på om jeg kunne for eksempel skrive for eksempel «kommunist» i denne mailen, for de amerikanerne forteller at de har teknologier som plukker opp sånne ord. Så kanskje de er koblet til amerikanske selskap som jeg jobber. Så kanskje man blir koblet med dette selskapet jeg jobber for, så tenker de at «hun er kommunist», og jeg er ikke kommunist. Dette gjør noe med deg. Og så har jeg tenkt med, «skal jeg si dette på mobilen?» Jeg har jo lest dette med at de kan plukke opp signalene og finne ut hva jeg sier og hvem jeg snakker med. Det er ikke sikkert de er kriminelle, men jeg vil ikke at alle skal vite hvem jeg snakker med.Vi er mennesker og vi må ha en modning som skjer i takt.

Det er bra. Er det noen situasjoner der sikkerhet er viktigere enn personvern?

Hva er det vi skal verne oss mot? Er det Russland, Amerika, muslimer – det høres ut som at vi skal verne oss mot hverandre. Du skal ikke vite hva jeg gjør, og jeg skal ikke vite hva du gjør. Jeg er imot at vi skal verne oss imot hverandre. Jeg lever ikke et liv som har vært fantastisk for andre.

Det kunne jo være en livssituasjon hvor det var andre som var interessert i hva du gjorde? Som du ikke var interessert skulle få vite.

Da får jeg svi for det – ikke du.

Du kan jo bli brukt i et system. Jeg har hørt mange rare historier, både fra utlandet og alt. Det er mange ting (uklart, flere snakker samtidig)

Det finnes situasjoner i den vestlige verden, vi har ikke makt. Vi har ikke opplevd krig. Det er ikke lenger enn 60 år siden det var en krig. En sånn situasjon, hvor det er fare for rikets sikkerhet, så er det klart at man må kunne bruke all den teknologien som er tilgjengelig. Hva med ressursene i Nordsjøen, hva er det de brukes til?

Hvis da tar frem sånn som Politiets Sikkerhetstjeneste, som har bruk for sånne tjenester i dag – synes du det er greit?

Jeg tror ikke det er helt absolutt, det går til en *viss* grad. Det er klart, de sikkerhetsfolka ser på spioner (uklart) Hvem skal passe på de? (latter)

Er det noen andre som har?

Jeg synes for eksempel når det er snakk om flysikkerheten (uklart). Hvis de kan hindre at noen kommer inn med våpen ombord så er det greit. Om vi kommer opp på en skjerm eller ikke hvor vi blir avdekte, men ikke med ansiktene. (uklart) jeg aksepterer at det er nødvendig.

Jeg aksepterer jo ubehageligheten på grunn av det, når jeg går ombord i flyet.

Det er jo akkurat det, at du ikke skal ta av deg på bena og beltespenna.

(uklart)

Vi må jo ikke være så naive. 11. september satt jeg hjemme. Så ringte mannen min og vi så det som vi ikke i vår villeste fantasi trodde kunne skje. Og da tenkte jeg «Gud, så naive vi har blitt».

Du har ei datter som har blitt?(uklart) Dette med at du skal hele tiden se hvor du har reist og hvor du har vært.

(uklart) det viser bare hvor langt amerikanerne har kommet i forhold til oss. Det viser bare hvor naive vi er som sitter her oppe.

Vi må ikke være fornøyde heller. Det er jo viktig å tro at den sikkerhetskontrollen i dag vil få flyene opp i(uklart) De sjekker jo bagasjen og tar ut ting, og det er jo bra. Men du kan jo ha tykt av ting i lommene. Og så kan du ta dem legge dem i korgen og slippe å ha dem i den plastikkposen. Du kan få med deg hva som helst på flyet hvis du vil. Jeg har vært å fløyet for ikke lenge siden. (uklart) Det kan jo være sprengstoff i den såpen. For det er det de er redde for, ikke sant? For de som vil, de kan jo ha med en sånn i en liten plastpose.

Britiske myndigheter er jo kjempeflinke. De avslører mye forskjellig. Nå i USA har du jo en terrorgruppe som planla å eksplodere (uklart) Det er jo klart, for å ta slike ting, så må man jo kunne bruke all teknologien. Det er jo sånne grusomme scenarier.

Kommer unge og uskyldige og får ødelagt livene mot de to, tre som kanskje kan komme til å gjøre noe, jeg vet ikke jeg.

Poenget er jo, hvor mye skal vi beskytte folk mot galinger. Galinger, eller om du kaller de terrorister, som er den fantastiske arbeidstittelen her i Norge. Men, altså, som har sluppet ut av psykiatrisk. Det har alltid vært galinger. Hvor mye kan du beskytte deg mot de? Til en viss grad så må du kunne si at okay, noen ganger kan vi ha uflaks. Det vil alltid være en idiot som vil finne på et eller annet. Uansett hvor mye vi prøver å stoppe dem. Hvor mye innsats skal vi bruke på? (uklart)

Jeg kan gjøre mye galt, hvis jeg vil, alle vi andre i Norge og verden i dag. Hvis vi vil, så kan vi gjøre det, men jeg ser ikke på sikkerhetsteknologien som blir tatt i bruk i USA i dag, er det første steg på å kontrollere hver enkelt. Frihet blir umulig, for å beskytte samfunnet.

Noen ganger vil det oppstå en farlig situasjon som blir overdrevet. De stresser med hvor farlig det er, hvordan kriminaliteten øker, antall mord, og hadde det virka hadde det jo gått ned. Men det passer ikke å si at det hadde gått ned, for da skulle vi lempet på sikkerhetstiltakene. Hvem er det som styrer, som vil dette?

Eller at du faktisk kan invadere et helt land på grunn av at noen galinger kjørte et fly inn i en bygning? Det er politikk. Det er helt greit, for ingen likte Saddam Hussein, for han var ikke spesielt sympatisk, men ingenting, ingen har rett til å invadere et land. For eksempel, det er ingen logisk rundt(uklart – latter).

Dette er politikk.

Der kommer vi inn på naivitet.

Jeg forstår krigen mot terror og en journalist som skrev det at hvis en eller to mennesker hadde gått på sentralbanestasjonen i Oslo med en sånn aksjon, da hadde vi forstått det med en gang. Der, over there, var det bare fire tusen.

(uklart)

Vi tenker liksom at ingenting skjer.

Ting skjer, og kommer til å skje.(latter)

Når vi tenker på frykt. Tenk å vokse opp i Venezuela på 50-tallet. Herregud, tenk på det, det hadde vært farlig det. Det er jo drittfarlig. (uklart) Vi kan ikke stole på myndighetene, de kan misbruke vår identitet. (samtidig snakking, diskusjon) Jeg ble holdt i kvelertak, og ropte på de som gikk forbi. Ingenting gjorde noen ting. Så kommer politiet, så sier de fyfy, skyndt dere ut til de som stor der. Ingen slapp til og hjalp til, de var typisk norske. (uklart)

Nar du får en verden som er overvåka, da får du den falske tryggheten du snakka om, og du tar ikke ansvar selv. Det ser vi jo i dag. Folk blir jo mer og mer (uklart). Vi føler ikke ansvar for andre folk lenger

(uklart) vi skal ikke stole på mobiltelefonen. Det er jo ikke alltid det er dekning på den, vi vet jo at det ikke alltid er dekning.

Det er ingen som har sagt at Norge er et farlig samfunn. Jeg synes Norge er det tryggeste samfunn, det beste land å bo i. Å fly fra Bodø til (uklart). Hvor farlig kan det være? (mange snakker)

Det er som at vi ikke trenger denne teknologien, fordi det er såpass trygt. Men det er de store, store sakene som krever. Og hvis du føler frykt fra noe usikkert noe. Med det yngste barnet mitt bodde vi i Frankrike. Her kan du jo (uklart) klokken syv, det kan du ikke i Marseilles. Så sier jeg, at nå tar du med mobilen i lommen hvis det er noe problem. Da har jeg mobilen og da har jeg trygghet. (uklart – latter)

Det vil jo føre til på at det blir en stor mangel på kvelden til, visste du at det har vært et kamera der. Jeg har vært på metroen i Paris ganske sent, og der var det mange forskjellige grupperinger skal jeg fortelle deg. Vi satt sånn livredde og engstelig for at de skulle komme.

De hadde jo kamera der. Og så var jeg i Roma, så sa de at «der må dere ikke gå». Og vi vet du, full fart, vi skulle dra dit turistene ikke er. Det skjedde ikke en dritt. Jeg tror kanskje jeg er litt motsatt av det behovet for å være redd for ting. Det er forskjellige oppfatninger. (uklart – mange snakker på en gang)

(diskusjon, flere prater på samme tid) – NOKAS-ranet - biler

Det er ikke teknologi, men der får vi inn det med overvåkingen. (uklart) Overvåking – helt i orden.

Ok, vi får gå litt videre. Hvem skal da bestemme hvordan sikkerhetsteknologi skal brukes?

Myndighetene.

Folket.

Et uavhengig (latter, folk prater på en gang)

Det skulle kanskje vært en kontrollinstans som kunne følge det opp (uklart) uavhengig rolle i dette her. Det fungerer jo rimelig greit har jeg inntrykk av.

Jeg vet ikke hvem som er den rette instansen til å avgjøre det. Men det skal jo ha en riktig undersøkelse på forhånd. De skal jo ikke bare si det og det har skjedd, de må jo gå og følge med på et eller annet hvis. Og det skal ikke være de som utvikler denne teknologien. (uklart)

Jeg vil bare si at man kan på en måte si at hva man synes, men det hjelper jo veldig lite når man ikke vet når nordmenn ikke kommer inn i USA. Hvem er det som bestemmer det, sånn kommer det til å bli med pass og andre ting. Da blir vi jo på en måte isolert, da er det ikke myndighetene som kan bestemme, da må de bare godta at det blir sånn, de har ikke noe valg. Reelt sett. Fakta er at det er bare, alle bakdeler, ingen fordeler omentrent.

Er det noen interessegrupper som bør bli hørt i dette spørsmålet om hvordan det skal brukes, menneskerettighetsorganisasjoner.

Det er sammensatt, om de er uavhengige, om objektivitet. Det er en ideell tanke, men nå er det mange og da blir det sånn. Det burde være sammensatt ut fra hvordan det er å være menneske. Teologi og alt. Hvordan får vi det til i praksis, det er ikke så lett.

Så, på en måte, det er få ting man kan utrette på en måte?

(uklart)

Jeg er veldig glad i teknologi og (uklart)

Jeg er ingeniør og sosiolog (uklart), men jeg har mange mener, men jeg vet ikke om de er så interessante i dag.

Poenget mitt er om det er noen vits i ha sånne store utvalg som skal sitte og synse masse om noe som blir tredd ned over hodet på en. Det blir bare for å rettferdiggjøre å lage et studie som er med på å bestemme dette. Det har ingenting å si, du får det enten du vil eller ikke

(uklart)

Vi får jo lyst å snakke om det. Du sier jo samtidig at du kommer til å få denne hatten til å bli tredd ned over deg uansett. (uklart)

Jeg skrev noen kommentarer, jeg tror faktisk det kommer opp snart. Men det er klart at en restriksjon er verdifull at det kan være bra og passe på selv og min egen situasjon, jeg tror vi må gjøre det. Jeg tror dette med personvern, jeg er glad for å høre. Jeg tror man bør passe seg. Jeg er bevisst i forhold til sønnen min på 20, vi snakker om hva han legger ut, på Facebook og sånn, jeg sier at det kommer til å ligge ute for alltid. Hva om ting kommer på omveier. Men han bryr seg ikke.

Men tenker du at hvis du brukte en anonym server på nett, bare at du bruker den, så kan du få trøbbel. Det at du i seg selv har gjort det gjør at du kan få (uklart)

Ok, da har vi noen minutter igjen. Regulering – altså, hvordan bør det, dere sier jo det er myndighetene som avgjør dette – hvordan bør den nye teknologien håndteres og reguleres?

Det vet vi jo egentlig ikke. Det ligger jo der ute. Vi blir sånn «dette må vi ta», (uklart) Det tar litt om gangen.

Bør det være en begrensning på utvikling av teknologi, eller bør selskapene få utvikle teknologien som de selv finner for godt?

De må få lov til å utvikle, men det er jo ikke alt som bør få lov til å komme på markedet. Det er ikke alt en trenger å ta i bruk. Men når en forsker, så bør jo fokus være at det er lov til alt.

Med håndtering, mener du for eksempel hvor lenge data skal være lagret, hvor mye som skal bli lagret? Som du snakket om i stad, hvis du er over 18 år, så må du få tilgang, godkjennelse av staten Norge for å få tilgang til den sektoren. Jeg mener at du ikke trenger å lagre åpent (uklart) buss 3 til stavanger. Så er det greit at det ikke skjedde noe på bussen, men det behøver ikke ligge der i tjue år.

Burde myndighetene få lov til å bruke den teknologien som de mener er viktig, eller burde det være mer generelle begrensninger på hva som er lov til å ta ibruk?

Det er viktig å skjønne begrensningen for dette med telefonavlytting og så vi dere. Det finnes jo begrensninger, det er jo ikke fritt fram. Men – å snakke om hvilke typer begrensning man skal bruke, det er vanskelig. Det må jo være visse regulering sånn noen lunde.

Det virker som at teknologien blir mer og mer kompleks, og at den teknologi som blir tatt i bruk, den blir ikke demontert, for å si det på den måten. Og dessuten, er det veldig mange humane interesser blant utviklet bak det. Og med min bakgrunn som translatør, (uklart) – velge en type fly, det vil også gjelde ved valg av teknologi. Jeg kan ikke noe om detaljene, men det er vestlige interesser bak utviklingen av teknologien. Tenkemakten har en tendens til å vinne fram.

Norge er jo et rikt land, så (uklart – latter)

Det er jo ikke lenge siden vi var det fattigste landet i Europa (uklart)

Ok, da var vi gjennom det meste. Har deres deltagelse i dagens arrangement endret deres holdninger til sikkerhetsteknologi og personvern?

nei (latter)

Nei, men det har gjerne gjort meg mer reflektert. (uklart)

Reflektert rundt de scenariene.

Får mer interesse for å følge med (uklart) interessen for området er vekket. Å følge med hvor det går videre. Jeg er ikke den som er begeistret og da kan jeg fortelle om han i 1984, så blir han fulgt av kameraer hele tiden og det eneste stedet han kan være fri fra kameraene er når han kryper langs veggen og legger seg i et hjørne, til og med hjemme i hans egen leilighet. Den eneste mulighetene han har til å være seg selv er å krype langs veggen slik at kameraene ikke ser han. Det skrev Orwell i 1944, det er ganske dyster forskning. Jeg har ikke lyst å ha et kamera hjemme hos meg. (uklart)

Tenk når de ikke vet ... (uklart) vi har egen skyld i det systemet.

Kunder og personvern, de må få tilgang. (uklart)

Ok, noen sluttkommentarer? Av enhver sort?

(latter)

(uklart)

Jeg har blitt mer reflektert rundt det.

Men, spørsmålene på bakgrunn av diskusjonen her. Har bekymringene dere blitt tatt til et mer overordnet samfunnsnivå eller er det mer i forhold til hver enkelt teknologi?

Det er mer overordnet.

Nei, det ikke hver enkelt teknologi som er viktig, det er det overordnede.

(uklart)

Da sier vi at det er det.

Annex 6

Frequency tables

Frequencies
country = NO
Frequency Table

q1sex[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	male	11	42,3	42,3	42,3
	female	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q2age[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	17	1	3,8	4,0	4,0
	19	1	3,8	4,0	8,0
	25	1	3,8	4,0	12,0
	28	1	3,8	4,0	16,0
	31	1	3,8	4,0	20,0
	33	1	3,8	4,0	24,0
	35	1	3,8	4,0	28,0
	36	1	3,8	4,0	32,0
	37	1	3,8	4,0	36,0
	40	1	3,8	4,0	40,0
	45	1	3,8	4,0	44,0
	46	1	3,8	4,0	48,0
	47	2	7,7	8,0	56,0
	49	1	3,8	4,0	60,0
	50	2	7,7	8,0	68,0
	51	1	3,8	4,0	72,0
	54	1	3,8	4,0	76,0
	56	3	11,5	12,0	88,0
	58	1	3,8	4,0	92,0
	59	1	3,8	4,0	96,0
	60	1	3,8	4,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q3household Persons in houshold ink self[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	3,8	3,8	3,8
	2	8	30,8	30,8	34,6
	3	6	23,1	23,1	57,7
	4 or more	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q4children[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	21	80,8	80,8	80,8
	no	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q5childhome1 No children[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	76,9	76,9	76,9
	yes	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q5childhome2 14 or younger[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	61,5	61,5	61,5
	yes	10	38,5	38,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q5childhome3 15 or older[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	69,2	69,2	69,2
	yes	8	30,8	30,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q6edu[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	3	11,5	11,5	11,5
	3	4	15,4	15,4	26,9
	4	5	19,2	19,2	46,2
	5	2	7,7	7,7	53,8
	6	6	23,1	23,1	76,9
	7	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q7occupstring[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Accountant	1	3,8	3,8	3,8
	Aviation technician	1	3,8	3,8	7,7
	Building technician	1	3,8	3,8	11,5
	Consultant/house wife	1	3,8	3,8	15,4
	Director	1	3,8	3,8	19,2
	Economist	1	3,8	3,8	23,1
	Financial advisor	1	3,8	3,8	26,9
	Financial consultant	1	3,8	3,8	30,8
	Head of department	2	7,7	7,7	38,5
	Illustrator/postal worker	1	3,8	3,8	42,3
	IT consultant	1	3,8	3,8	46,2
	Medical secretary	1	3,8	3,8	50,0
	Operations assistant	1	3,8	3,8	53,8
	Parental advisor	1	3,8	3,8	57,7
	Primary school teacher	1	3,8	3,8	61,5
	Psychiatric nurse (ongoing pedagogic edu.)	1	3,8	3,8	65,4
	Self employed	1	3,8	3,8	69,2
	Software developer	1	3,8	3,8	73,1
	Student/part time sales clerk	1	3,8	3,8	76,9
	Student/sales clerk	1	3,8	3,8	80,8
	Study consultant	1	3,8	3,8	84,6
	System consultant	1	3,8	3,8	88,5
	Teacher	1	3,8	3,8	92,3
	Technical Drafter	1	3,8	3,8	96,2
	Translator/teacher	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q8district[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Metro	18	69,2	69,2	69,2
	Provincial town	2	7,7	7,7	76,9
	Rural	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q9phone[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	25	96,2	96,2	96,2
	at least once a week	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q10email[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	22	84,6	84,6	84,6
	at least once a week	3	11,5	11,5	96,2
	at least once a month	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q11internet[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	23	88,5	88,5	88,5
	at least once a week	1	3,8	3,8	92,3
	at least once a month	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q12publictransport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	1	3,8	3,8	3,8
	at least once a week	3	11,5	11,5	15,4
	at least once a month	3	11,5	11,5	26,9
	less than once a month	17	65,4	65,4	92,3
	never	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q13plane[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	more than 5 times a year	6	23,1	23,1	23,1
	3-5 times a year	9	34,6	34,6	57,7
	1-2 times a year	9	34,6	34,6	92,3
	less than 1 time a year	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q14car[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	at least once a day	16	61,5	61,5	61,5
	at least once a week	7	26,9	26,9	88,5
	at least once a month	2	7,7	7,7	96,2
	never	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q15general The security of society is absolutely dependent on the development and use of new security technologies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	34,6	34,6	34,6
	partly agree	12	46,2	46,2	80,8
	neither agree nor disagree	2	7,7	7,7	88,5
	partly disagree	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q16general Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	23,1	23,1	23,1
	partly agree	14	53,8	53,8	76,9
	neither agree nor disagree	5	19,2	19,2	96,2
	partly disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	5	19,2	19,2	19,2
	partly agree	7	26,9	26,9	46,2
	partly disagree	2	7,7	7,7	53,8
	completely disagree	12	46,2	46,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q18general When security technology is available, we might just as well make use of it[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	23,1	23,1	23,1
	partly agree	8	30,8	30,8	53,8
	neither agree nor disagree	1	3,8	3,8	57,7
	partly disagree	5	19,2	19,2	76,9
	completely disagree	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q19general Privacy should not be violated without reasonable suspicion of criminal intent[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	17	65,4	65,4	65,4
	partly agree	5	19,2	19,2	84,6
	neither agree nor disagree	1	3,8	3,8	88,5
	partly disagree	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	42,3	42,3	42,3
	partly agree	6	23,1	23,1	65,4
	neither agree nor disagree	3	11,5	11,5	76,9
	partly disagree	5	19,2	19,2	96,2
	completely disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q21general New security technologies are likely to be abused by governmental agencies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	5	19,2	19,2	19,2
	partly agree	7	26,9	26,9	46,2
	neither agree nor disagree	7	26,9	26,9	73,1
	partly disagree	2	7,7	7,7	80,8
	completely disagree	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q22general New security technologies are likely to be abused by criminals[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	22	84,6	84,6	84,6
	partly agree	1	3,8	3,8	88,5
	neither agree nor disagree	2	7,7	7,7	96,2
	partly disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q23biom1 Facial characteristics[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	84,0	84,0
	yes	4	15,4	16,0	100,0
	Total	25	96,2	100,0	
Missing	System	1	3,8		
Total		26	100,0		

a. country = NO

q23biom2 Fingerprints[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	53,8	53,8	53,8
	yes	12	46,2	46,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q23biom3 Iris recognition[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	65,4	65,4	65,4
	yes	9	34,6	34,6	100,0
	Total	26	100,0	100,0	

a. country = NO

q23biom4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	73,1	73,1	73,1
	yes	6	23,1	23,1	96,2
	2	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q23biom5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	4	15,4	15,4	96,2
	2	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom1 Bank[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	73,1	73,1	73,1
	yes	7	26,9	26,9	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom2 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	46,2	46,2	46,2
	yes	14	53,8	53,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom3 Store[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q24biom4 Border[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	26,9	26,9	26,9
	yes	19	73,1	73,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom5 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	92,3	92,3
	yes	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom6 Stadium and crowded[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom7 Other private service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q24biom8 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q24biom9 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	92,3	92,3
	yes	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q25biom Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	8	30,8	30,8	30,8
	partly agree	9	34,6	34,6	65,4
	neither agree nor disagree	1	3,8	3,8	69,2
	partly disagree	4	15,4	15,4	84,6
	completely disagree	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q26biom The use of the biometric passport makes me feel insecure because of the risk of my biometric data being stolen[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	26,9	26,9	26,9
	partly agree	9	34,6	34,6	61,5
	neither agree nor disagree	4	15,4	15,4	76,9
	partly disagree	4	15,4	15,4	92,3
	completely disagree	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q27visual1 Store[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	53,8	56,0	56,0
	yes	11	42,3	44,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual2 Dressing room[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	92,0	92,0
	yes	2	7,7	8,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual3 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	38,5	40,0	40,0
	yes	15	57,7	60,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual4 Bank[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	30,8	32,0	32,0
	yes	17	65,4	68,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual5 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	19,2	20,0	20,0
	yes	20	76,9	80,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual6 Stadium and crowded[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	46,2	48,0	48,0
	yes	13	50,0	52,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual7 All public[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	69,2	72,0	72,0
	yes	7	26,9	28,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual8 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	88,0	88,0
	yes	3	11,5	12,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q27visual9 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	92,0	92,0
	yes	2	7,7	8,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q28visual How do you feel about the number of CCTV cameras in public spaces in general?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	there should be more	7	26,9	41,2	41,2
	the number is appropriate	5	19,2	29,4	70,6
	there should be less	3	11,5	17,6	88,2
	there should be no	2	7,7	11,8	100,0
	Total	17	65,4	100,0	
Missing	d.k.	8	30,8		
	99	1	3,8		
	Total	9	34,6		
Total		26	100,0		

a. country = NO

q29visual1 School[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual2 Central bus and train station[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual3 Airport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	15,4	15,4	15,4
	yes	22	84,6	84,6	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual4 Shopping mall[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual5 Public buildings[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q29visual7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual1 Reveal everything[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual2 Mannequin projection[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual3 Body heat, sweat & heart rate[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual4 Metal[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	7	26,9	26,9	26,9
	yes	18	69,2	69,2	96,2
	4	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual5 Luggage x-ray[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	19,2	19,2	19,2
	yes	19	73,1	73,1	92,3
	4	1	3,8	3,8	96,2
	5	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q30visual6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	96,0	96,0
	yes	1	3,8	4,0	100,0
	Total	25	96,2	100,0	
Missing	System	1	3,8		
Total		26	100,0		

a. country = NO

q30visual7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q31visual CCTV surveillance makes me feel more secure[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	4	15,4	15,4	15,4
	partly agree	12	46,2	46,2	61,5
	neither agree nor disagree	3	11,5	11,5	73,1
	partly disagree	2	7,7	7,7	80,8
	completely disagree	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q32visual CCTV surveillance infringes my privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	23,1	23,1	23,1
	partly agree	14	53,8	53,8	76,9
	neither agree nor disagree	2	7,7	7,7	84,6
	partly disagree	1	3,8	3,8	88,5
	completely disagree	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q33visual Scanning of persons for detection of hidden items is an acceptable tool for preventing terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	8	30,8	30,8	30,8
	partly agree	12	46,2	46,2	76,9
	partly disagree	3	11,5	11,5	88,5
	completely disagree	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q34local1 Terrorists and criminals w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	19,2	19,2	19,2
	yes	21	80,8	80,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q34local2 Any w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q34local3 Emergency[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	2	7,7	7,7	7,7
	yes	24	92,3	92,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q34local4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	96,0	96,0
	yes	1	3,8	4,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q34local5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q35local1 Terrorists and criminals w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	19,2	19,2	19,2
	yes	21	80,8	80,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q35local2 Any w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q35local3 Stolen vehicles[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	34,6	34,6	34,6
	yes	17	65,4	65,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q35local4 Speeding[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q35local5 Automatic accident reporting[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	30,8	30,8	30,8
	yes	18	69,2	69,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q35local6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q35local7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q36local Should eCall automatically be installed in all new cars?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes	4	15,4	16,0	16,0
	yes but possible to deactivate	6	23,1	24,0	40,0
	no, optional	15	57,7	60,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q37local The possibility of locating all mobile phones is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	12	46,2	46,2	46,2
	partly agree	10	38,5	38,5	84,6
	partly disagree	2	7,7	7,7	92,3
	completely disagree	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q38local The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	15	57,7	57,7	57,7
	partly agree	6	23,1	23,1	80,8
	neither agree nor disagree	2	7,7	7,7	88,5
	partly disagree	1	3,8	3,8	92,3
	completely disagree	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q39local The possibility of locating all cars is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	42,3	42,3	42,3
	partly agree	10	38,5	38,5	80,8
	neither agree nor disagree	1	3,8	3,8	84,6
	partly disagree	3	11,5	11,5	96,2
	completely disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

40local The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	10	38,5	38,5	38,5
	partly agree	6	23,1	23,1	61,5
	neither agree nor disagree	3	11,5	11,5	73,1
	partly disagree	1	3,8	3,8	76,9
	completely disagree	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data1 Prevention of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	46,2	46,2	46,2
	yes	14	53,8	53,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data2 Investigation of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	34,6	34,6	34,6
	yes	17	65,4	65,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data3 Prevention of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	50,0	50,0	50,0
	yes	13	50,0	50,0	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data4 Investigation of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	10	38,5	38,5	38,5
	yes	16	61,5	61,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q41data7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	92,3	92,3
	yes	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data1 Prevention of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data2 Investigation of terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	30,8	30,8	30,8
	yes	18	69,2	69,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data3 Prevention of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	53,8	53,8	53,8
	yes	12	46,2	46,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data4 Investigation of crime[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	8	30,8	30,8	30,8
	yes	18	69,2	69,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q42data6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q42data7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

43data Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	23,1	23,1	23,1
	partly agree	6	23,1	23,1	46,2
	neither agree nor disagree	1	3,8	3,8	50,0
	partly disagree	4	15,4	15,4	65,4
	completely disagree	9	34,6	34,6	100,0
	Total	26	100,0	100,0	

a. country = NO

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	26,9	26,9	26,9
	partly agree	11	42,3	42,3	69,2
	neither agree nor disagree	2	7,7	7,7	76,9
	partly disagree	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q45data Scanning of and combining data from different databases containing personal information is privacy infringing[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	13	50,0	50,0	50,0
	partly agree	8	30,8	30,8	80,8
	neither agree nor disagree	1	3,8	3,8	84,6
	partly disagree	2	7,7	7,7	92,3
	completely disagree	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q46data Scanning of and combining data from different databases is a good tool for police to prevent terror[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	11	42,3	42,3	42,3
	partly agree	7	26,9	26,9	69,2
	neither agree nor disagree	5	19,2	19,2	88,5
	partly disagree	2	7,7	7,7	96,2
	completely disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q47data Databases being used for something else than the original purpose is a serious privacy problem[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	20	76,9	76,9	76,9
	partly agree	2	7,7	7,7	84,6
	neither agree nor disagree	1	3,8	3,8	88,5
	partly disagree	2	7,7	7,7	96,2
	completely disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire1 Prevention and investigation of terrorism w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	5	19,2	19,2	19,2
	yes	21	80,8	80,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire2 Prevention and investigation of terrorism w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	76,9	76,9	76,9
	yes	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire3 Prevention and investigation of crime w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	4	15,4	15,4	15,4
	yes	22	84,6	84,6	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire4 Prevention and investigation of crime w/o court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	73,1	73,1	73,1
	yes	7	26,9	26,9	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire5 Commercial[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q48wire6 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q48wire7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q49wire What methods of eavesdropping is acceptable?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	all communication lines	2	7,7	10,0	10,0
	persons that suspect is expected to contact	6	23,1	30,0	40,0
	suspects	10	38,5	50,0	90,0
	totally unacceptable	2	7,7	10,0	100,0
	Total	20	76,9	100,0	
Missing	d.k.	2	7,7		
	99	4	15,4		
	Total	6	23,1		
Total		26	100,0		

a. country = NO

q50wire Eavesdropping is a good tool for police investigation[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	13	50,0	52,0	52,0
	partly agree	6	23,1	24,0	76,0
	neither agree nor disagree	3	11,5	12,0	88,0
	partly disagree	2	7,7	8,0	96,0
	completely disagree	1	3,8	4,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q51wire Eavesdropping is a serious violation of privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	9	34,6	36,0	36,0
	partly agree	11	42,3	44,0	80,0
	neither agree nor disagree	1	3,8	4,0	84,0
	partly disagree	3	11,5	12,0	96,0
	completely disagree	1	3,8	4,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q52protect1 Anonymous calling cards[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	53,8	53,8	53,8
	yes	12	46,2	46,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q52protect2 Encryption programmes[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q52protect3 Identity management[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	50,0	50,0	50,0
	yes	13	50,0	50,0	100,0
	Total	26	100,0	100,0	

a. country = NO

q52protect4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q52protect5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	76,9	76,9	76,9
	yes	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	14	53,8	53,8	53,8
	partly agree	8	30,8	30,8	84,6
	neither agree nor disagree	2	7,7	7,7	92,3
	partly disagree	1	3,8	3,8	96,2
	completely disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q54protect Privacy enhancing technologies should not be legal if they make police investigation and prevention of terror and crime more difficult[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	6	23,1	23,1	23,1
	partly agree	5	19,2	19,2	42,3
	neither agree nor disagree	4	15,4	15,4	57,7
	partly disagree	6	23,1	23,1	80,8
	completely disagree	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem1 Accept registration of travel and fingerprints[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem2 Accept only if template[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem3 Accept only if deleted[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	69,2	69,2	69,2
	yes	8	30,8	30,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem4 Accept only if not exclusive[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	17	65,4	65,4	65,4
	yes	9	34,6	34,6	100,0
	Total	26	100,0	100,0	

a. country = NO

q55dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q56dilem1 Accept database and biometrics[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	57,7	57,7	57,7
	yes	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q56dilem2 Accept naked machine[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	20	76,9	76,9	76,9
	yes	6	23,1	23,1	100,0
	Total	26	100,0	100,0	

a. country = NO

q56dilem3 Accept sweat, body heat and heart rate scanning[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q56dilem4 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	57,7	57,7	57,7
	yes	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q56dilem5 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	92,3	92,3
	yes	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem1 Accept all consequences[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem2 Accept only low rate of false positives[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem3 Accept only no false positives[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	18	69,2	69,2	69,2
	yes	8	30,8	30,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem4 Accept only in exposed places[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	34,6	34,6	34,6
	yes	17	65,4	65,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q57dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	24	92,3	92,3	92,3
	yes	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q58dilem1 Accept all access for counter terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	19	73,1	73,1	73,1
	yes	7	26,9	26,9	100,0
	Total	26	100,0	100,0	

a. country = NO

q58dilem2 Accept only if anonymous and w court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	9	34,6	34,6	34,6
	yes	17	65,4	65,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q58dilem3 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q58dilem4 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q59dilem1 Accept locate car to prevent crime or terrorism[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	12	46,2	48,0	48,0
	yes	13	50,0	52,0	100,0
	Total	25	96,2	100,0	
Missing	99	1	3,8		
Total		26	100,0		

a. country = NO

q59dilem2 Accept speeding tickets[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q59dilem3 Accept register all movements[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	23	88,5	88,5	88,5
	yes	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q59dilem4 Accept only accidents[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	57,7	57,7	57,7
	yes	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q59dilem5 Accept only if voluntary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	11	42,3	42,3	42,3
	yes	15	57,7	57,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q59dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	26	100,0	100,0	100,0

a. country = NO

q60dilem1 Accept calling cards[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	16	61,5	61,5	61,5
	yes	10	38,5	38,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q60dilem2 Accept encryption[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	57,7	57,7	57,7
	yes	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q60dilem3 Accept Internet anonymity - bomb[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	14	53,8	53,8	53,8
	yes	12	46,2	46,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q60dilem4 Accept Internet anonymity - child pornography[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q60dilem5 Never[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	15	57,7	57,7	57,7
	yes	11	42,3	42,3	100,0
	Total	26	100,0	100,0	

a. country = NO

q60dilem6 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem1 Accept exclusion of refusers from public service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	88,0	88,0
	yes	3	11,5	12,0	100,0
	Total	25	96,2	100,0	
Missing	System	1	3,8		
Total		26	100,0		

a. country = NO

q61dilem2 Accept exclusion of unabled from public service[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	25	96,2	96,2	96,2
	yes	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem3 Accept refusers are impended when public transport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	50,0	50,0	50,0
	yes	13	50,0	50,0	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem4 Accept unabled are impended when public transport[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem5 Accept no consequences for refusers[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	21	80,8	80,8	80,8
	yes	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem6 Accept no consequences for unabled[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	13	50,0	50,0	50,0
	yes	13	50,0	50,0	100,0
	Total	26	100,0	100,0	

a. country = NO

q61dilem7 d.k.[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	no	22	84,6	84,6	84,6
	yes	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

q62demo Politicians must always submit important questions to public debate and public hearings before making decisions on implementing new security technologies[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	19	73,1	73,1	73,1
	partly agree	6	23,1	23,1	96,2
	partly disagree	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

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[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	1	3,8	3,8	3,8
	partly agree	4	15,4	15,4	19,2
	neither agree nor disagree	1	3,8	3,8	23,1
	partly disagree	4	15,4	15,4	38,5
	completely disagree	16	61,5	61,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q64demo Human rights organisations are always entitled to be heard when important decisions on security and privacy are made[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	17	65,4	65,4	65,4
	partly agree	5	19,2	19,2	84,6
	neither agree nor disagree	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

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[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	7	26,9	26,9	26,9
	partly agree	5	19,2	19,2	46,2
	neither agree nor disagree	6	23,1	23,1	69,2
	partly disagree	1	3,8	3,8	73,1
	completely disagree	7	26,9	26,9	100,0
	Total	26	100,0	100,0	

a. country = NO

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[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	completely agree	23	88,5	88,5	88,5
	partly agree	3	11,5	11,5	100,0
	Total	26	100,0	100,0	

a. country = NO

q67suggest Collection of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	21	80,8	80,8	80,8
	some importance	4	15,4	15,4	96,2
	little importance	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

q68suggest Only authorized personnel can have access to collected personal data[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	24	92,3	92,3	92,3
	some importance	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

q69suggest Prior to implementing, new security technologies must be checked for privacy impact[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	21	80,8	80,8	80,8
	some importance	5	19,2	19,2	100,0
	Total	26	100,0	100,0	

a. country = NO

q70suggest Funding of research projects on new security technologies should be dependent on a thorough analysis of privacy impacts[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	high importance	15	57,7	68,2	68,2
	some importance	6	23,1	27,3	95,5
	not important at all	1	3,8	4,5	100,0
	Total	22	84,6	100,0	
Missing	d.k.	3	11,5		
	99	1	3,8		
	Total	4	15,4		
Total		26	100,0		

a. country = NO

q71end Have you changed your attitude towards security technologies in general ir the course of completing this questionnaire?[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	yes, more positive	3	11,5	11,5	11,5
	yes, more worried	3	11,5	11,5	23,1
	no	20	76,9	76,9	100,0
	Total	26	100,0	100,0	

a. country = NO

q72endstring [a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		15	57,7	57,7	57,7
	1) The opportunity to provide information across country borders is an area I think it is important to have clear limitations on. 2) The possibility to ask for information after the person gives his/her consent (for example insurance companies that wants	1	3,8	3,8	61,5
	I believe most people have limited awareness about this, earlier it was very scary to give your personal number, now everyone does it every day, for example at online banking. Technology is moving faster than the knowledge and awareness of the consequence	1	3,8	3,8	65,4
	I have no objections to complete collection of information as long as this can reduce the amount of time used to solve criminal activities. However, it is important that the information does not become available to non-authorized personell.	1	3,8	3,8	69,2
	I might want more of the humanist/individual element in this. What is most frightening about technology and the possibilities it gives, is imagening what kind of society it might lead us into, and what it can do to us as people, human relations at all lev	1	3,8	3,8	73,1
	I think the introduction of the different theories was very good. However, I think the explainations of anonymization services was somewhat onesided (negative). A good example is Chinese people who use these to avad ithe great fire wall of China". Very g	1	3,8	3,8	76,9
	If someone "googles" a name they will be able to find this persons date of birth, personal number, bank account number, address. Access to minutes and protocols for example from NGOs. I have even read excerpts from a protocol froma meeting where someones	1	3,8	3,8	80,8
	One cannot stop technology, but authorities must provide direction/demands to the use. In this session we have witnessed lots of inspiration from abroad, and Norway as a different country does not always need to follow what others do. Qu. 27. Alernative a	1	3,8	3,8	84,6
	Regarding qu. 24. Biometrics in accesscontrol. Might be used towards staff on a particular workplace, but not on customers, travelers etc.	1	3,8	3,8	88,5
	Security technology should not take over the human ability to think/react in given situations. For example our behaviour to respect speed limits. If technology takes over, for example that the car has a built in speed limit, we allow ourselves to be doped	1	3,8	3,8	92,3
	That everyone takes DNA at birth and collect it in a registry (obligatory) - easier to solve many crimes. "Others" that today does not have taken a DNA test should have the opportunity/be encouraged to do this.	1	3,8	3,8	96,2
	The security of the general population must be more important than to protect criminals. If one has nothing to hide, one as nothing to worry about.	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

eduISCED97 [a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	lower secondary level of education	3	11,5	11,5	11,5
	upper secondary level of education	9	34,6	34,6	46,2
	first stage of tertiary education	14	53,8	53,8	100,0
	Total	26	100,0	100,0	

a. country = NO

eduISCED97binary Tertiary[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Shorter than tertiary	12	46,2	46,2	46,2
	Tertiary	14	53,8	53,8	100,0
	Total	26	100,0	100,0	

a. country = NO

AgeBinary Age over and under 50[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-49	14	53,8	58,3	58,3
	50+	10	38,5	41,7	100,0
	Total	24	92,3	100,0	
Missing	System	2	7,7		
Total		26	100,0		

a. country = NO

PhoneBinary Daily[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	1	3,8	3,8	3,8
	Daily	25	96,2	96,2	100,0
	Total	26	100,0	100,0	

a. country = NO

EmailBinary Daily[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	4	15,4	15,4	15,4
	Daily	22	84,6	84,6	100,0
	Total	26	100,0	100,0	

a. country = NO

InternetBinary Daily[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	3	11,5	11,5	11,5
	Daily	23	88,5	88,5	100,0
	Total	26	100,0	100,0	

a. country = NO

PublicBinary Daily[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	25	96,2	96,2	96,2
	Daily	1	3,8	3,8	100,0
	Total	26	100,0	100,0	

a. country = NO

CarBinary Daily[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less	10	38,5	38,5	38,5
	Daily	16	61,5	61,5	100,0
	Total	26	100,0	100,0	

a. country = NO

PlaneBinary Less than once a year[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 times a year or more	24	92,3	92,3	92,3
	Less than 1 time a year	2	7,7	7,7	100,0
	Total	26	100,0	100,0	

a. country = NO

PublicBinary2 Weekly[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	22	84,6	84,6	84,6
	at least once a week	4	15,4	15,4	100,0
	Total	26	100,0	100,0	

a. country = NO

CarBinary2 Weekly[a]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than once a week	3	11,5	11,5	11,5
	at least once a week	23	88,5	88,5	100,0
	Total	26	100,0	100,0	

a. country = NO

Crosstabs

q15general The security of society is absolutely dependent on the development and use of new security technologies * q1sex Crosstabulation

			q1sex		
			male	female	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	3	6	9
		% within q1sex	27,3%	40,0%	34,6%
	partly agree	Count	5	7	12
		% within q1sex	45,5%	46,7%	46,2%
	neither agree nor disagree	Count	0	2	2
		% within q1sex	,0%	13,3%	7,7%
	partly disagree	Count	3	0	3
		% within q1sex	27,3%	,0%	11,5%
Total		Count	11	15	26
		% within q1sex	100,0%	100,0%	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 * q1sex Crosstabulation

			q1sex		
			male	female	Total
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	5	1	6
		% within q1sex	45,5%	6,7%	23,1%
	partly agree	Count	6	8	14
		% within q1sex	54,5%	53,3%	53,8%
	neither agree nor disagree	Count	0	5	5
		% within q1sex	,0%	33,3%	19,2%
	partly disagree	Count	0	1	1
		% within q1sex	,0%	6,7%	3,8%
Total		Count	11	15	26
		% 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		
			male	female	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	2	3	5
		% within q1sex	18,2%	20,0%	19,2%
	partly agree	Count	2	5	7
		% within q1sex	18,2%	33,3%	26,9%
	partly disagree	Count	1	1	2
		% within q1sex	9,1%	6,7%	7,7%
	completely disagree	Count	6	6	12
		% within q1sex	54,5%	40,0%	46,2%
Total		Count	11	15	26
		% 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		
			male	female	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	2	4	6
		% within q1sex	18,2%	26,7%	23,1%
	partly agree	Count	4	4	8
		% within q1sex	36,4%	26,7%	30,8%
	neither agree nor disagree	Count	0	1	1
		% within q1sex	,0%	6,7%	3,8%
	partly disagree	Count	2	3	5
		% within q1sex	18,2%	20,0%	19,2%
	completely disagree	Count	3	3	6
		% within q1sex	27,3%	20,0%	23,1%
Total		Count	11	15	26
		% within q1sex	100,0%	100,0%	100,0%

19general Privacy should not be violated without reasonable suspicion of criminal intent * q1se Crosstabulation

			q1sex		
			male	female	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	7	10	17
		% within q1sex	63,6%	66,7%	65,4%
	partly agree	Count	2	3	5
		% within q1sex	18,2%	20,0%	19,2%
	neither agree nor disagree	Count	1	0	1
		% within q1sex	9,1%	,0%	3,8%
	partly disagree	Count	1	2	3
		% within q1sex	9,1%	13,3%	11,5%
Total		Count	11	15	26
		% 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		
			male	female	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	5	6	11
		% within q1sex	45,5%	40,0%	42,3%
	partly agree	Count	2	4	6
		% within q1sex	18,2%	26,7%	23,1%
	neither agree nor disagree	Count	1	2	3
		% within q1sex	9,1%	13,3%	11,5%
	partly disagree	Count	3	2	5
		% within q1sex	27,3%	13,3%	19,2%
	completely disagree	Count	0	1	1
		% within q1sex	,0%	6,7%	3,8%
Total		Count	11	15	26
		% within q1sex	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q1sex Crosstabulation

			q1sex		
			male	female	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	3	5
		% within q1sex	18,2%	20,0%	19,2%
	partly agree	Count	3	4	7
		% within q1sex	27,3%	26,7%	26,9%
	neither agree nor disagree	Count	3	4	7
		% within q1sex	27,3%	26,7%	26,9%
	partly disagree	Count	0	2	2
		% within q1sex	,0%	13,3%	7,7%
	completely disagree	Count	3	2	5
		% within q1sex	27,3%	13,3%	19,2%
Total		Count	11	15	26
		% within q1sex	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q1sex Crosstabulation

			q1sex		
			male	female	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	8	14	22
		% within q1sex	72,7%	93,3%	84,6%
	partly agree	Count	0	1	1
		% within q1sex	,0%	6,7%	3,8%
	neither agree nor disagree	Count	2	0	2
		% within q1sex	18,2%	,0%	7,7%
	partly disagree	Count	1	0	1
		% within q1sex	9,1%	,0%	3,8%
Total		Count	11	15	26
		% 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		
			18-49	50+	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	4	5	9
		% within AgeBinary Age over and under 50	28,6%	50,0%	37,5%
	partly agree	Count	6	4	10
		% within AgeBinary Age over and under 50	42,9%	40,0%	41,7%
	neither agree nor disagree	Count	1	1	2
		% within AgeBinary Age over and under 50	7,1%	10,0%	8,3%
	partly disagree	Count	3	0	3
		% within AgeBinary Age over and under 50	21,4%	,0%	12,5%
Total		Count	14	10	24
		% 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		
			18-49	50+	Total
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	3	2	5
		% within AgeBinary Age over and under 50	21,4%	20,0%	20,8%
	partly agree	Count	10	4	14
		% within AgeBinary Age over and under 50	71,4%	40,0%	58,3%
	neither agree nor disagree	Count	1	3	4
		% within AgeBinary Age over and under 50	7,1%	30,0%	16,7%
	partly disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	10,0%	4,2%
Total		Count	14	10	24
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

¡17general If you have nothing to hide you don't have to worry about security technologies that infringe youı privacy * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	1	3	4
		% within AgeBinary Age over and under 50	7,1%	30,0%	16,7%
	partly agree	Count	3	3	6
		% within AgeBinary Age over and under 50	21,4%	30,0%	25,0%
	partly disagree	Count	2	0	2
		% within AgeBinary Age over and under 50	14,3%	,0%	8,3%
	completely disagree	Count	8	4	12
		% within AgeBinary Age over and under 50	57,1%	40,0%	50,0%
Total		Count	14	10	24
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

¡18general 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		
			18-49	50+	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	2	4	6
		% within AgeBinary Age over and under 50	14,3%	40,0%	25,0%
	partly agree	Count	3	3	6
		% within AgeBinary Age over and under 50	21,4%	30,0%	25,0%
	neither agree nor disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	7,1%	,0%	4,2%
	partly disagree	Count	5	0	5
		% within AgeBinary Age over and under 50	35,7%	,0%	20,8%
	completely disagree	Count	3	3	6
		% within AgeBinary Age over and under 50	21,4%	30,0%	25,0%
Total		Count	14	10	24
		% within AgeBinary Age over and under 50	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * AgeBinary Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	7	8	15
		% within AgeBinary Age over and under 50	50,0%	80,0%	62,5%
	partly agree	Count	4	1	5
		% within AgeBinary Age over and under 50	28,6%	10,0%	20,8%
	neither agree nor disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	7,1%	,0%	4,2%
	partly disagree	Count	2	1	3
		% within AgeBinary Age over and under 50	14,3%	10,0%	12,5%
Total		Count	14	10	24
		% 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 * AgeBinar Age over and under 50 Crosstabulation

			AgeBinary Age over and under 50		
			18-49	50+	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	6	3	9
		% within AgeBinary Age over and under 50	42,9%	30,0%	37,5%
	partly agree	Count	3	3	6
		% within AgeBinary Age over and under 50	21,4%	30,0%	25,0%
	neither agree nor disagree	Count	2	1	3
		% within AgeBinary Age over and under 50	14,3%	10,0%	12,5%
	partly disagree	Count	3	2	5
		% within AgeBinary Age over and under 50	21,4%	20,0%	20,8%
	completely disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	10,0%	4,2%
Total		Count	14	10	24
		% 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		
			18-49	50+	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	3	5
		% within AgeBinary Age over and under 50	14,3%	30,0%	20,8%
	partly agree	Count	5	2	7
		% within AgeBinary Age over and under 50	35,7%	20,0%	29,2%
	neither agree nor disagree	Count	4	1	5
		% within AgeBinary Age over and under 50	28,6%	10,0%	20,8%
	partly disagree	Count	2	0	2
		% within AgeBinary Age over and under 50	14,3%	,0%	8,3%
	completely disagree	Count	1	4	5
		% within AgeBinary Age over and under 50	7,1%	40,0%	20,8%
Total		Count	14	10	24
		% 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		
			18-49	50+	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	13	8	21
		% within AgeBinary Age over and under 50	92,9%	80,0%	87,5%
	partly agree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	10,0%	4,2%
	neither agree nor disagree	Count	0	1	1
		% within AgeBinary Age over and under 50	,0%	10,0%	4,2%
	partly disagree	Count	1	0	1
		% within AgeBinary Age over and under 50	7,1%	,0%	4,2%
Total		Count	14	10	24
		% 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		
			Shorter than tertiary	Tertiary	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	5	4	9
		% within eduISCED97binary Tertiary	41,7%	28,6%	34,6%
	partly agree	Count	5	7	12
		% within eduISCED97binary Tertiary	41,7%	50,0%	46,2%
	neither agree nor disagree	Count	0	2	2
		% within eduISCED97binary Tertiary	,0%	14,3%	7,7%
	partly disagree	Count	2	1	3
		% within eduISCED97binary Tertiary	16,7%	7,1%	11,5%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	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 * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
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	3	3	6
		% within eduISCED97binary Tertiary	25,0%	21,4%	23,1%
	partly agree	Count	4	10	14
		% within eduISCED97binary Tertiary	33,3%	71,4%	53,8%
	neither agree nor disagree	Count	5	0	5
		% within eduISCED97binary Tertiary	41,7%	,0%	19,2%
	partly disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	7,1%	3,8%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	4	1	5
		% within eduISCED97binary Tertiary	33,3%	7,1%	19,2%
	partly agree	Count	4	3	7
		% within eduISCED97binary Tertiary	33,3%	21,4%	26,9%
	partly disagree	Count	2	0	2
		% within eduISCED97binary Tertiary	16,7%	,0%	7,7%
	completely disagree	Count	2	10	12
		% within eduISCED97binary Tertiary	16,7%	71,4%	46,2%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q18general When security technology is available, we might just as well make use of it * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	5	1	6
		% within eduISCED97binary Tertiary	41,7%	7,1%	23,1%
	partly agree	Count	3	5	8
		% within eduISCED97binary Tertiary	25,0%	35,7%	30,8%
	neither agree nor disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	8,3%	,0%	3,8%
	partly disagree	Count	2	3	5
		% within eduISCED97binary Tertiary	16,7%	21,4%	19,2%
	completely disagree	Count	1	5	6
		% within eduISCED97binary Tertiary	8,3%	35,7%	23,1%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q19general Privacy should not be violated without reasonable suspicion of criminal intent * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	8	9	17
		% within eduISCED97binary Tertiary	66,7%	64,3%	65,4%
	partly agree	Count	2	3	5
		% within eduISCED97binary Tertiary	16,7%	21,4%	19,2%
	neither agree nor disagree	Count	0	1	1
		% within eduISCED97binary Tertiary	,0%	7,1%	3,8%
	partly disagree	Count	2	1	3
		% within eduISCED97binary Tertiary	16,7%	7,1%	11,5%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	5	6	11
		% within eduISCED97binary Tertiary	41,7%	42,9%	42,3%
	partly agree	Count	1	5	6
		% within eduISCED97binary Tertiary	8,3%	35,7%	23,1%
	neither agree nor disagree	Count	2	1	3
		% within eduISCED97binary Tertiary	16,7%	7,1%	11,5%
	partly disagree	Count	3	2	5
		% within eduISCED97binary Tertiary	25,0%	14,3%	19,2%
	completely disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	8,3%	,0%	3,8%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	1	4	5
		% within eduISCED97binary Tertiary	8,3%	28,6%	19,2%
	partly agree	Count	2	5	7
		% within eduISCED97binary Tertiary	16,7%	35,7%	26,9%
	neither agree nor disagree	Count	4	3	7
		% within eduISCED97binary Tertiary	33,3%	21,4%	26,9%
	partly disagree	Count	1	1	2
		% within eduISCED97binary Tertiary	8,3%	7,1%	7,7%
	completely disagree	Count	4	1	5
		% within eduISCED97binary Tertiary	33,3%	7,1%	19,2%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

¡22general New security technologies are likely to be abused by criminals * eduISCED97binary Tertiary Crosstabulation

			eduISCED97binary Tertiary		
			Shorter than tertiary	Tertiary	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	9	13	22
		% within eduISCED97binary Tertiary	75,0%	92,9%	84,6%
	partly agree	Count	1	0	1
		% within eduISCED97binary Tertiary	8,3%	,0%	3,8%
	neither agree nor disagree	Count	1	1	2
		% within eduISCED97binary Tertiary	8,3%	7,1%	7,7%
	partly disagree	Count	1	0	1
		% within eduISCED97binary Tertiary	8,3%	,0%	3,8%
Total		Count	12	14	26
		% within eduISCED97binary Tertiary	100,0%	100,0%	100,0%

Crosstabs

¡15general The security of society is absolutely dependent on the development and use of new security technologies * q4children Crosstabulation

			q4children		
			yes	no	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	8	1	9
		% within q4children	38,1%	20,0%	34,6%
	partly agree	Count	10	2	12
		% within q4children	47,6%	40,0%	46,2%
	neither agree nor disagree	Count	2	0	2
		% within q4children	9,5%	,0%	7,7%
	partly disagree	Count	1	2	3
		% within q4children	4,8%	40,0%	11,5%
Total		Count	21	5	26
		% within q4children	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 * q4children Crosstabulation

			q4children		
			yes	no	Total
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	5	1	6
		% within q4children	23,8%	20,0%	23,1%
	partly agree	Count	12	2	14
		% within q4children	57,1%	40,0%	53,8%
	neither agree nor disagree	Count	3	2	5
		% within q4children	14,3%	40,0%	19,2%
	partly disagree	Count	1	0	1
		% within q4children	4,8%	,0%	3,8%
Total		Count	21	5	26
		% within q4children	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 * q4children Crosstabulation

			q4children		
			yes	no	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	4	1	5
		% within q4children	19,0%	20,0%	19,2%
	partly agree	Count	6	1	7
		% within q4children	28,6%	20,0%	26,9%
	partly disagree	Count	1	1	2
		% within q4children	4,8%	20,0%	7,7%
	completely disagree	Count	10	2	12
		% within q4children	47,6%	40,0%	46,2%
Total		Count	21	5	26
		% 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		
			yes	no	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	5	1	6
		% within q4children	23,8%	20,0%	23,1%
	partly agree	Count	6	2	8
		% within q4children	28,6%	40,0%	30,8%
	neither agree nor disagree	Count	1	0	1
		% within q4children	4,8%	,0%	3,8%
	partly disagree	Count	4	1	5
		% within q4children	19,0%	20,0%	19,2%
	completely disagree	Count	5	1	6
		% within q4children	23,8%	20,0%	23,1%
Total		Count	21	5	26
		% within q4children	100,0%	100,0%	100,0%

l9general Privacy should not be violated without reasonable suspicion of criminal intent * q4childre Crosstabulation

			q4children		
			yes	no	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	14	3	17
		% within q4children	66,7%	60,0%	65,4%
	partly agree	Count	4	1	5
		% within q4children	19,0%	20,0%	19,2%
	neither agree nor disagree	Count	1	0	1
		% within q4children	4,8%	,0%	3,8%
	partly disagree	Count	2	1	3
		% within q4children	9,5%	20,0%	11,5%
Total		Count	21	5	26
		% 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		
			yes	no	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	9	2	11
		% within q4children	42,9%	40,0%	42,3%
	partly agree	Count	5	1	6
		% within q4children	23,8%	20,0%	23,1%
	neither agree nor disagree	Count	1	2	3
		% within q4children	4,8%	40,0%	11,5%
	partly disagree	Count	5	0	5
		% within q4children	23,8%	,0%	19,2%
	completely disagree	Count	1	0	1
		% within q4children	4,8%	,0%	3,8%
Total		Count	21	5	26
		% within q4children	100,0%	100,0%	100,0%

q21general New security technologies are likely to be abused by governmental agencies * q4children Crosstabulation

			q4children		
			yes	no	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	5	0	5
		% within q4children	23,8%	,0%	19,2%
	partly agree	Count	6	1	7
		% within q4children	28,6%	20,0%	26,9%
	neither agree nor disagree	Count	4	3	7
		% within q4children	19,0%	60,0%	26,9%
	partly disagree	Count	2	0	2
		% within q4children	9,5%	,0%	7,7%
	completely disagree	Count	4	1	5
		% within q4children	19,0%	20,0%	19,2%
Total		Count	21	5	26
		% within q4children	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q4children Crosstabulation

			q4children		
			yes	no	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	18	4	22
		% within q4children	85,7%	80,0%	84,6%
	partly agree	Count	0	1	1
		% within q4children	,0%	20,0%	3,8%
	neither agree nor disagree	Count	2	0	2
		% within q4children	9,5%	,0%	7,7%
	partly disagree	Count	1	0	1
		% within q4children	4,8%	,0%	3,8%
Total		Count	21	5	26
		% 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		
			no	yes	Total
q15general The security of society is absolutely dependent on the development and use of new security technologies	completely agree	Count	7	2	9
		% within q5childhome1 No children	35,0%	33,3%	34,6%
	partly agree	Count	8	4	12
		% within q5childhome1 No children	40,0%	66,7%	46,2%
	neither agree nor disagree	Count	2	0	2
		% within q5childhome1 No children	10,0%	,0%	7,7%
	partly disagree	Count	3	0	3
		% within q5childhome1 No children	15,0%	,0%	11,5%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

16general Many security technologies do not really increase security, but are only being applied to show tha something is done to fight terror * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
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	4	2	6
		% within q5childhome1 No children	20,0%	33,3%	23,1%
	partly agree	Count	12	2	14
		% within q5childhome1 No children	60,0%	33,3%	53,8%
	neither agree nor disagree	Count	3	2	5
		% within q5childhome1 No children	15,0%	33,3%	19,2%
	partly disagree	Count	1	0	1
		% within q5childhome1 No children	5,0%	,0%	3,8%
Total		Count	20	6	26
		% within q5childhome1 No children	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 * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q17general If you have nothing to hide you don't have to worry about security technologies that infringe your privacy	completely agree	Count	4	1	5
		% within q5childhome1 No children	20,0%	16,7%	19,2%
	partly agree	Count	5	2	7
		% within q5childhome1 No children	25,0%	33,3%	26,9%
	partly disagree	Count	2	0	2
		% within q5childhome1 No children	10,0%	,0%	7,7%
	completely disagree	Count	9	3	12
		% within q5childhome1 No children	45,0%	50,0%	46,2%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

18general When security technology is available, we might just as well make use of it * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q18general When security technology is available, we might just as well make use of it	completely agree	Count	4	2	6
		% within q5childhome1 No children	20,0%	33,3%	23,1%
	partly agree	Count	6	2	8
		% within q5childhome1 No children	30,0%	33,3%	30,8%
	neither agree nor disagree	Count	1	0	1
		% within q5childhome1 No children	5,0%	,0%	3,8%
	partly disagree	Count	5	0	5
		% within q5childhome1 No children	25,0%	,0%	19,2%
	completely disagree	Count	4	2	6
		% within q5childhome1 No children	20,0%	33,3%	23,1%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

19general Privacy should not be violated without reasonable suspicion of criminal intent * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q19general Privacy should not be violated without reasonable suspicion of criminal intent	completely agree	Count	12	5	17
		% within q5childhome1 No children	60,0%	83,3%	65,4%
	partly agree	Count	4	1	5
		% within q5childhome1 No children	20,0%	16,7%	19,2%
	neither agree nor disagree	Count	1	0	1
		% within q5childhome1 No children	5,0%	,0%	3,8%
	partly disagree	Count	3	0	3
		% within q5childhome1 No children	15,0%	,0%	11,5%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q20general It is uncomfortable to be under surveillance, even though you have no criminal intent * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q20general It is uncomfortable to be under surveillance, even though you have no criminal intent	completely agree	Count	9	2	11
		% within q5childhome1 No children	45,0%	33,3%	42,3%
	partly agree	Count	4	2	6
		% within q5childhome1 No children	20,0%	33,3%	23,1%
	neither agree nor disagree	Count	3	0	3
		% within q5childhome1 No children	15,0%	,0%	11,5%
	partly disagree	Count	4	1	5
		% within q5childhome1 No children	20,0%	16,7%	19,2%
	completely disagree	Count	0	1	1
		% within q5childhome1 No children	,0%	16,7%	3,8%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

ı21general New security technologies are likely to be abused by governmental agencies * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q21general New security technologies are likely to be abused by governmental agencies	completely agree	Count	2	3	5
		% within q5childhome1 No children	10,0%	50,0%	19,2%
	partly agree	Count	7	0	7
		% within q5childhome1 No children	35,0%	,0%	26,9%
	neither agree nor disagree	Count	6	1	7
		% within q5childhome1 No children	30,0%	16,7%	26,9%
	partly disagree	Count	2	0	2
		% within q5childhome1 No children	10,0%	,0%	7,7%
	completely disagree	Count	3	2	5
		% within q5childhome1 No children	15,0%	33,3%	19,2%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q22general New security technologies are likely to be abused by criminals * q5childhome1 No children Crosstabulation

			q5childhome1 No children		
			no	yes	Total
q22general New security technologies are likely to be abused by criminals	completely agree	Count	17	5	22
		% within q5childhome1 No children	85,0%	83,3%	84,6%
	partly agree	Count	1	0	1
		% within q5childhome1 No children	5,0%	,0%	3,8%
	neither agree nor disagree	Count	1	1	2
		% within q5childhome1 No children	5,0%	16,7%	7,7%
	partly disagree	Count	1	0	1
		% within q5childhome1 No children	5,0%	,0%	3,8%
Total		Count	20	6	26
		% within q5childhome1 No children	100,0%	100,0%	100,0%

q24biom2 Airport * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		
			1-2 times a year or more	Less than 1 time a year	Total
q24biom2 Airport	no	Count	11	1	12
		% within PlaneBinary Less than once a year	45,8%	50,0%	46,2%
	yes	Count	13	1	14
		% within PlaneBinary Less than once a year	54,2%	50,0%	53,8%
Total		Count	24	2	26
		% within PlaneBinary Less than once a year	100,0%	100,0%	100,0%

q56dilem1 Accept database and biometrics * PlaneBinary Less than once a year Crosstabulation

			PlaneBinary Less than once a year		
			1-2 times a year or more	Less than 1 time a year	Total
q56dilem1 Accept database and biometrics	no	Count	14	1	15
		% within PlaneBinary Less than once a year	58,3%	50,0%	57,7%
	yes	Count	10	1	11
		% within PlaneBinary Less than once a year	41,7%	50,0%	42,3%
Total		Count	24	2	26
		% within PlaneBinary Less than once a year	100,0%	100,0%	100,0%

q24biom5 Central bus and train station * PublicBinary Daily Crosstabulation

			PublicBinary Daily		
			Less	Daily	Total
q24biom5 Central bus and train station	no	Count	23	1	24
		% within PublicBinary Daily	92,0%	100,0%	92,3%
	yes	Count	2	0	2
		% within PublicBinary Daily	8,0%	,0%	7,7%
Total		Count	25	1	26
		% within PublicBinary Daily	100,0%	100,0%	100,0%

q55dilem1 Accept registration of travel and fingerprints * PublicBinary Daily Crosstabulation

			PublicBinary Daily		
			Less	Daily	Total
q55dilem1 Accept registration of travel and fingerprints	no	Count	21	1	22
		% within PublicBinary Daily	84,0%	100,0%	84,6%
	yes	Count	4	0	4
		% within PublicBinary Daily	16,0%	,0%	15,4%
Total		Count	25	1	26
		% within PublicBinary Daily	100,0%	100,0%	100,0%

q35local1 Terrorists and criminals w court order * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local1 Terrorists and criminals w court order	no	Count	2	3	5
		% within CarBinary Daily	20,0%	18,8%	19,2%
	yes	Count	8	13	21
		% within CarBinary Daily	80,0%	81,3%	80,8%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local2 Any w/o court order * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local2 Any w/o court order	no	Count	9	13	22
		% within CarBinary Daily	90,0%	81,3%	84,6%
	yes	Count	1	3	4
		% within CarBinary Daily	10,0%	18,8%	15,4%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local3 Stolen vehicles * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local3 Stolen vehicles	no	Count	5	4	9
		% within CarBinary Daily	50,0%	25,0%	34,6%
	yes	Count	5	12	17
		% within CarBinary Daily	50,0%	75,0%	65,4%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local4 Speeding * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local4 Speeding	no	Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q35local5 Automatic accident reporting * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q35local5 Automatic accident reporting	no	Count	4	4	8
		% within CarBinary Daily	40,0%	25,0%	30,8%
	yes	Count	6	12	18
		% within CarBinary Daily	60,0%	75,0%	69,2%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q36local Should eCall automatically be installed in all new cars? * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q36local Should eCall automatically be installed in all new cars?	yes	Count	0	4	4
		% within CarBinary Daily	,0%	25,0%	16,0%
	yes but possible to deactivate	Count	3	3	6
		% within CarBinary Daily	33,3%	18,8%	24,0%
	no, optional	Count	6	9	15
		% within CarBinary Daily	66,7%	56,3%	60,0%
Total		Count	9	16	25
		% within CarBinary Daily	100,0%	100,0%	100,0%

q39local The possibility of locating all cars is privacy infringing * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q39local The possibility of locating all cars is privacy infringing	completely agree	Count	6	5	11
		% within CarBinary Daily	60,0%	31,3%	42,3%
	partly agree	Count	4	6	10
		% within CarBinary Daily	40,0%	37,5%	38,5%
	neither agree nor disagree	Count	0	1	1
		% within CarBinary Daily	,0%	6,3%	3,8%
	partly disagree	Count	0	3	3
		% within CarBinary Daily	,0%	18,8%	11,5%
	completely disagree	Count	0	1	1
		% within CarBinary Daily	,0%	6,3%	3,8%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem1 Accept locate car to prevent crime or terrorism * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem1 Accept locate car to prevent crime or terrorism	no	Count	6	6	12
		% within CarBinary Daily	60,0%	40,0%	48,0%
	yes	Count	4	9	13
		% within CarBinary Daily	40,0%	60,0%	52,0%
Total		Count	10	15	25
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem2 Accept speeding tickets * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem2 Accept speeding tickets	no	Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem3 Accept register all movements * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem3 Accept register all movements	no	Count	9	14	23
		% within CarBinary Daily	90,0%	87,5%	88,5%
	yes	Count	1	2	3
		% within CarBinary Daily	10,0%	12,5%	11,5%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem4 Accept only accidents * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem4 Accept only accidents	no	Count	5	10	15
		% within CarBinary Daily	50,0%	62,5%	57,7%
	yes	Count	5	6	11
		% within CarBinary Daily	50,0%	37,5%	42,3%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem5 Accept only if voluntary * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem5 Accept only if voluntary	no	Count	3	8	11
		% within CarBinary Daily	30,0%	50,0%	42,3%
	yes	Count	7	8	15
		% within CarBinary Daily	70,0%	50,0%	57,7%
Total		Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%

q59dilem6 d.k. * CarBinary Daily Crosstabulation

			CarBinary Daily		
			Less	Daily	Total
q59dilem6 d.k.	no	Count	10	16	26
		% within CarBinary Daily	100,0%	100,0%	100,0%
Total		Count	10	16	26
		% within CarBinary 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 * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
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	6	6
		% within PhoneBinary Daily	,0%	24,0%	23,1%
	partly agree	Count	0	6	6
		% within PhoneBinary Daily	,0%	24,0%	23,1%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
	partly disagree	Count	1	3	4
		% within PhoneBinary Daily	100,0%	12,0%	15,4%
	completely disagree	Count	0	9	9
		% within PhoneBinary Daily	,0%	36,0%	34,6%
Total		Count	1	25	26
		% 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		
			Less	Daily	Total
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	6	6
		% within EmailBinary Daily	,0%	27,3%	23,1%
	partly agree	Count	3	3	6
		% within EmailBinary Daily	75,0%	13,6%	23,1%
	neither agree nor disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
	partly disagree	Count	0	4	4
		% within EmailBinary Daily	,0%	18,2%	15,4%
	completely disagree	Count	1	8	9
		% within EmailBinary Daily	25,0%	36,4%	34,6%
Total		Count	4	22	26
		% 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		
			Less	Daily	Total
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	5	6
		% within InternetBinary Daily	33,3%	21,7%	23,1%
	partly agree	Count	1	5	6
		% within InternetBinary Daily	33,3%	21,7%	23,1%
	neither agree nor disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
	partly disagree	Count	0	4	4
		% within InternetBinary Daily	,0%	17,4%	15,4%
	completely disagree	Count	1	8	9
		% within InternetBinary Daily	33,3%	34,8%	34,6%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	0	7	7
		% within PhoneBinary Daily	,0%	28,0%	26,9%
	partly agree	Count	1	10	11
		% within PhoneBinary Daily	100,0%	40,0%	42,3%
	neither agree nor disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	partly disagree	Count	0	6	6
		% within PhoneBinary Daily	,0%	24,0%	23,1%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	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		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	1	6	7
		% within EmailBinary Daily	25,0%	27,3%	26,9%
	partly agree	Count	2	9	11
		% within EmailBinary Daily	50,0%	40,9%	42,3%
	neither agree nor disagree	Count	1	1	2
		% within EmailBinary Daily	25,0%	4,5%	7,7%
	partly disagree	Count	0	6	6
		% within EmailBinary Daily	,0%	27,3%	23,1%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	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		
			Less	Daily	Total
q44data Data from phone, mobile and Internet communication should not be stored beyond what is needed for billing purposes	completely agree	Count	2	5	7
		% within InternetBinary Daily	66,7%	21,7%	26,9%
	partly agree	Count	1	10	11
		% within InternetBinary Daily	33,3%	43,5%	42,3%
	neither agree nor disagree	Count	0	2	2
		% within InternetBinary Daily	,0%	8,7%	7,7%
	partly disagree	Count	0	6	6
		% within InternetBinary Daily	,0%	26,1%	23,1%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	1	12	13
		% within PhoneBinary Daily	100,0%	48,0%	50,0%
	partly agree	Count	0	8	8
		% within PhoneBinary Daily	,0%	32,0%	30,8%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
	partly disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	completely disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	3	10	13
		% within EmailBinary Daily	75,0%	45,5%	50,0%
	partly agree	Count	1	7	8
		% within EmailBinary Daily	25,0%	31,8%	30,8%
	neither agree nor disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
	partly disagree	Count	0	2	2
		% within EmailBinary Daily	,0%	9,1%	7,7%
	completely disagree	Count	0	2	2
		% within EmailBinary Daily	,0%	9,1%	7,7%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q45data Scanning of and combining data from different databases containing personal information is privacy infringing * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q45data Scanning of and combining data from different databases containing personal information is privacy infringing	completely agree	Count	2	11	13
		% within InternetBinary Daily	66,7%	47,8%	50,0%
	partly agree	Count	0	8	8
		% within InternetBinary Daily	,0%	34,8%	30,8%
	neither agree nor disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
	partly disagree	Count	0	2	2
		% within InternetBinary Daily	,0%	8,7%	7,7%
	completely disagree	Count	1	1	2
		% within InternetBinary Daily	33,3%	4,3%	7,7%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

47data Databases being used for something else than the original purpose is a serious privacy problem * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	1	19	20
		% within PhoneBinary Daily	100,0%	76,0%	76,9%
	partly agree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
	partly disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	completely disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

47data Databases being used for something else than the original purpose is a serious privacy problem EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	3	17	20
		% within EmailBinary Daily	75,0%	77,3%	76,9%
	partly agree	Count	1	1	2
		% within EmailBinary Daily	25,0%	4,5%	7,7%
	neither agree nor disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
	partly disagree	Count	0	2	2
		% within EmailBinary Daily	,0%	9,1%	7,7%
	completely disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q47data Databases being used for something else than the original purpose is a serious privacy problem * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q47data Databases being used for something else than the original purpose is a serious privacy problem	completely agree	Count	2	18	20
		% within InternetBinary Daily	66,7%	78,3%	76,9%
	partly agree	Count	1	1	2
		% within InternetBinary Daily	33,3%	4,3%	7,7%
	neither agree nor disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
	partly disagree	Count	0	2	2
		% within InternetBinary Daily	,0%	8,7%	7,7%
	completely disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q51wire Eavesdropping is a serious violation of privacy * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	0	9	9
		% within PhoneBinary Daily	,0%	37,5%	36,0%
	partly agree	Count	1	10	11
		% within PhoneBinary Daily	100,0%	41,7%	44,0%
	neither agree nor disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,2%	4,0%
	partly disagree	Count	0	3	3
		% within PhoneBinary Daily	,0%	12,5%	12,0%
	completely disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,2%	4,0%
Total		Count	1	24	25
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q51wire Eavesdropping is a serious violation of privacy * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	2	7	9
		% within EmailBinary Daily	50,0%	33,3%	36,0%
	partly agree	Count	2	9	11
		% within EmailBinary Daily	50,0%	42,9%	44,0%
	neither agree nor disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,8%	4,0%
	partly disagree	Count	0	3	3
		% within EmailBinary Daily	,0%	14,3%	12,0%
	completely disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,8%	4,0%
Total		Count	4	21	25
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q51wire Eavesdropping is a serious violation of privacy * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q51wire Eavesdropping is a serious violation of privacy	completely agree	Count	1	8	9
		% within InternetBinary Daily	33,3%	36,4%	36,0%
	partly agree	Count	1	10	11
		% within InternetBinary Daily	33,3%	45,5%	44,0%
	neither agree nor disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,5%	4,0%
	partly disagree	Count	0	3	3
		% within InternetBinary Daily	,0%	13,6%	12,0%
	completely disagree	Count	1	0	1
		% within InternetBinary Daily	33,3%	,0%	4,0%
Total		Count	3	22	25
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	1	13	14
		% within PhoneBinary Daily	100,0%	52,0%	53,8%
	partly agree	Count	0	8	8
		% within PhoneBinary Daily	,0%	32,0%	30,8%
	neither agree nor disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	partly disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
	completely disagree	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,0%	3,8%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	2	12	14
		% within EmailBinary Daily	50,0%	54,5%	53,8%
	partly agree	Count	2	6	8
		% within EmailBinary Daily	50,0%	27,3%	30,8%
	neither agree nor disagree	Count	0	2	2
		% within EmailBinary Daily	,0%	9,1%	7,7%
	partly disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
	completely disagree	Count	0	1	1
		% within EmailBinary Daily	,0%	4,5%	3,8%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q53protect Privacy enhancing technologies are a necessity in today's society to preserve privacy	completely agree	Count	2	12	14
		% within InternetBinary Daily	66,7%	52,2%	53,8%
	partly agree	Count	1	7	8
		% within InternetBinary Daily	33,3%	30,4%	30,8%
	neither agree nor disagree	Count	0	2	2
		% within InternetBinary Daily	,0%	8,7%	7,7%
	partly disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
	completely disagree	Count	0	1	1
		% within InternetBinary Daily	,0%	4,3%	3,8%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	1	18	19
		% within PhoneBinary Daily	100,0%	72,0%	73,1%
	yes	Count	0	7	7
		% within PhoneBinary Daily	,0%	28,0%	26,9%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	4	15	19
		% within EmailBinary Daily	100,0%	68,2%	73,1%
	yes	Count	0	7	7
		% within EmailBinary Daily	,0%	31,8%	26,9%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q58dilem1 Accept all access for counter terrorism * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q58dilem1 Accept all access for counter terrorism	no	Count	2	17	19
		% within InternetBinary Daily	66,7%	73,9%	73,1%
	yes	Count	1	6	7
		% within InternetBinary Daily	33,3%	26,1%	26,9%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

q34local1 Terrorists and criminals w court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local1 Terrorists and criminals w court order	no	Count	0	5	5
		% within PhoneBinary Daily	,0%	20,0%	19,2%
	yes	Count	1	20	21
		% within PhoneBinary Daily	100,0%	80,0%	80,8%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local2 Any w/o court order * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local2 Any w/o court order	no	Count	1	21	22
		% within PhoneBinary Daily	100,0%	84,0%	84,6%
	yes	Count	0	4	4
		% within PhoneBinary Daily	,0%	16,0%	15,4%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local3 Emergency * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local3 Emergency	no	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	yes	Count	1	23	24
		% within PhoneBinary Daily	100,0%	92,0%	92,3%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local4 Never * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local4 Never	no	Count	1	23	24
		% within PhoneBinary Daily	100,0%	95,8%	96,0%
	yes	Count	0	1	1
		% within PhoneBinary Daily	,0%	4,2%	4,0%
Total		Count	1	24	25
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q34local5 d.k. * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q34local5 d.k.	no	Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q52protect1 Anonymous calling cards * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q52protect1 Anonymous calling cards	no	Count	0	14	14
		% within PhoneBinary Daily	,0%	56,0%	53,8%
	yes	Count	1	11	12
		% within PhoneBinary Daily	100,0%	44,0%	46,2%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q37local The possibility of locating all mobile phones is privacy infringing * PhoneBinary Daily Crosstabulation

			PhoneBinary Daily		
			Less	Daily	Total
q37local The possibility of locating all mobile phones is privacy infringing	completely agree	Count	1	11	12
		% within PhoneBinary Daily	100,0%	44,0%	46,2%
	partly agree	Count	0	10	10
		% within PhoneBinary Daily	,0%	40,0%	38,5%
	partly disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
	completely disagree	Count	0	2	2
		% within PhoneBinary Daily	,0%	8,0%	7,7%
Total		Count	1	25	26
		% within PhoneBinary Daily	100,0%	100,0%	100,0%

q52protect2 Encryption programmes * EmailBinary Daily Crosstabulation

			EmailBinary Daily		
			Less	Daily	Total
q52protect2 Encryption programmes	no	Count	3	8	11
		% within EmailBinary Daily	75,0%	36,4%	42,3%
	yes	Count	1	14	15
		% within EmailBinary Daily	25,0%	63,6%	57,7%
Total		Count	4	22	26
		% within EmailBinary Daily	100,0%	100,0%	100,0%

q52protect3 Identity management * InternetBinary Daily Crosstabulation

			InternetBinary Daily		
			Less	Daily	Total
q52protect3 Identity management	no	Count	2	11	13
		% within InternetBinary Daily	66,7%	47,8%	50,0%
	yes	Count	1	12	13
		% within InternetBinary Daily	33,3%	52,2%	50,0%
Total		Count	3	23	26
		% within InternetBinary Daily	100,0%	100,0%	100,0%

Annex 7

Comments from the questionnaire

Below follows comments that were written at the last open comment box in the questionnaire. Some have addressed their comments to specific questions, whereas most of the comments are general reflections.

*****

“One cannot stop technology, but authorities must provide direction/demands to the use. In this session we have witnessed lots of inspiration from abroad, and Norway as a different country does not always need to follow what others do.”

“I have no objections to complete collection of information as long as this can reduce the amount of time used to solve criminal activities. However, it is important that the information does not become available to non-authorized personnel. “

“I might want more of the humanist/individual element in this. What is most frightening about technology and the possibilities it gives, is imagining what kind of society it might lead us into, and what it can do to us as people, human relations at all levels etc. I am glad that I am too old to experience this "brave new world", because that it is approaching there is no doubt. After all, there are strong economic interests behind the technology.”

“The opportunity to provide information across country borders is an area I think it is important to have clear limitations on.”

“The possibility to ask for information after the person gives his/her consent (for example insurance companies that wants your medical file after consent) should be limited.”

“Security technology should not take over the human ability to think/react in given situations. For example our behaviour to respect speed limits. If technology takes over, for example that the car has a built in speed limit, we allow ourselves to be doped down when it comes to security. A "fake" security through knowing that there are surveillance cameras everywhere should not decrease our scepticism/observation when it comes to potential dangerous situations.”

“I think the introduction of the different theories was very good. However, I think the explanations of anonymization services were somewhat one-sided (negative). A good example is Chinese people who use these to avoid #the great fire wall of China". Very good initiative! :-)”

“That everyone takes DNA at birth and collect it in a registry (obligatory) - easier to solve many crimes. "Others" that today does not have taken a DNA test should have the opportunity/be encouraged to do this.”

“I believe most people have limited awareness about this, earlier it was very scary to give your personal number, now everyone does it every day, for example at online banking. Technology is moving faster than the knowledge and awareness of the consequences of this. I am especially worried about children and young people because of the parents' lack of knowledge and awareness about for example use of Internet, … (unclear), use of mobile phones etc.”

The security of the general population must be more important than to protect criminals. If one has nothing to hide, one as nothing to worry about.

If someone "googles" a name they will be able to find this persons date of birth, personal number, bank account number, address, ore access to minutes and protocols for example from NGOs. I have

even read excerpts from a protocol from a meeting where someone's salary was discussed. On the Internet there is little privacy!

Qu. 24: Biometrics in access control.
"This might be used towards staff on a particular workplace, but not on customers, travellers etc."
Qu. 27. Where to accept camera surveillance
"Alternative answer: At publicly run places, like passport controls etc."

Qu. 54: Privacy promoting technologies might be available to all, however it should not increase. crime/contribute to negativity.

Qu. 56: Fast track at airports:
"Only for international flights, not domestic flights."