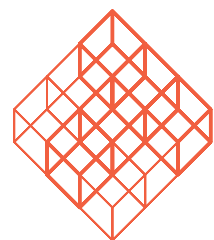


Sikkerhet og personvern

Scenarier



Sikkerhet og personvern

Scenarier

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

Utgitt: Oslo, juni 2007

Omslag: Enzo Finger Design AS

Trykk: ILAS Grafisk

Tekst: Christine Hafskjold

Illustrasjoner: Åsne Flyen

Copyright © Teknologirådet

Elektronisk publisert på: www.teknologiradet.no

Innholdsfortegnelse	side
Forord	4
Innledning	5
<i>Hva er sikkerhetsteknologi?</i>	5
<i>Hva er personvern?</i>	5
Hva mener du om sikkerhetsteknologi?	5
<i>Biometri</i>	8
<i>Videoovervåking</i>	9
<i>Automatisk ansiktsgjenkjenning</i>	9
<i>Lokaliseringsteknologi</i>	10
<i>eCall</i>	11
<i>Automatisk bilsiltgjenkjenning (ANPR)</i>	12
<i>Formålsutglidning (function creep)</i>	12
<i>Total Information Awareness (TIA)</i>	13
<i>Radiofrekvensidentifisering (RFID)</i>	15
<i>Biometriske pass</i>	15
<i>Passasjerskanning (nakenmaskiner)</i>	16
<i>Datalagring</i>	17
<i>Avlytting</i>	18
<i>Personvern fremmende teknologier</i>	18

Forord

Dette dokumentet inngår som en del av PRISE-prosjektet (PRIVacy and Security in Europe). Siktemålet med prosjektet er å bidra til en sikker fremtid for Europa i tråd med europeiske borgeres rettigheter og preferanser, og da særlig retten til personvern. Prosjektet gjennomføres i samarbeid med institusjoner i Danmark (Teknologirådet), Tyskland (Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein) og Østerrike (Institut für Technikfolgen-abschätzung, ITA).

Teknologirådet i Norge har vært ansvarlig for utviklingen av scenariene i dokumentet, og for kartleggingen av de ulike sikkerhetsteknologiene som scenariene bygger på. Hensikten med scenariene er å synliggjøre hvordan de ulike teknologiene for overvåking og sikkerhet kan brukes i samfunnet, og å stimulere til debatt rundt dette.

Teknologirådet jobber prosjektbasert, og involverer ressurspersoner som har særlig kompetanse innenfor de tema prosjektet omfatter. For å sikre at våre scenarier er troverdige og realistiske har vi knyttet til oss en gruppe eksperter innen flere områder som er viktige i forhold til samfunnsikkerhet og personvern. Ekspertgruppen har hatt følgende medlemmer:

- Asle Fossberg, Politiets data- og materielltjeneste
- Marit Gjerde, Politihøgskolen
- Nina Græger, Norsk utenrikspolitisk institutt
- Ove Skåra, Datatilsynet
- Thomas Olsen, Senter for rettsinformatikk

Vi vil også takke Jordi Mas, assisterende direktør ved Den katalanske stiftelsen for forskning og innovasjon (FCRI) for bidrag i prosessen. Arbeidet har vært ledet av Teknologirådets prosjektleder Christine Hafskjold.

Jeg vil på vegne av Teknologirådet takke for det arbeidet som har vært gjort.

Tore Tennøe
Sekretariatsleder, Teknologirådet

Innledning

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 hovedsaklig 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, antiterroriltak, 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.

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 Menneskerettighetserklæringen.

Personvern er et vanskelig område å håndtere fordi det nesten alltid konkurrerer med andre samfunnsgoder, som for eksempel mobilitet, effektivitet, sikkerhet eller bekvemmelighet. 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 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 loyldige borger kan befinne seg i en situasjon hvor han ønsker verken å bli sett eller sporet.

Når det gjelder sikkerhetsteknologier og overvåkning, hevder kritikere at mange av de i verksette 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 antiterroriltak som særlig griper inn i personvernet, slik som telefonavlytting, gjennom søking 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 om 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 kunne vise anvendelsen av enkelte sikkerhetsteknologier eller lovgivning som ikke er innført 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 barna 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 nødvendig!

Biometri

Biometrisk teknologi kan identifisere mennesker automatisk ved hjelp av fysiologiske kjennetegn eller adferdsmønstre. Biometri kan brukes til å kontrollere tilgang til fysiske områder eller informasjon (som datamaskiner). 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 internasjonalt, 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 sammenlignes 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 lagret 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 (*feilakseprate* 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 lane*, burde det gå bra. Fast lane 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 lane 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 bråkede 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

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.

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 behandlingsskapasitet 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.

programvare for ansikts- og mønstergjenkjenning, har hun en følelse av å være mer iaktatt 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 feilaktig har vært mistenkt for å være terrorist. Da teknologien var ganske ny, 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 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!

- o -

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 nødansrop gjennom eCall og en rekke andre sikkerhetssystemer for kjøretøy. Peter er ikke engang sikker på hva alle



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 2012. Det vil være mer nøyaktig enn GPS-systemet, og det vil ha større utbredelse.

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 den faktisk kunne stoppes via 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.

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 ulykkesituasjon - 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 forsikringselskaper), 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.



I kjølvannet av en forskningsrapport om hvor mange liv som kunne ha vært reddet i trafikken dersom bilistene overholdt fartsgrensene, ble det foreslått at sikkerhetsystemer 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 bøtere registeret, og boten trekkes automatisk fra bileierens bankkonto.

Peter trækker 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.

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 stjalne kjøretøy.

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 stjalne kjøretøy.

Han trodde faktisk et slikt system ville være overflødig etter at eCall ble satt i drift, men visstnok vet noen av de organi-

serte 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! Hvorfor virker det som om forbrytere alltid ligger ett skritt foran teknologien?

Peter parkerer bilen og går mot terminalen og inngangen for fast lane. 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”.

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.

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 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!"

Total Information Awareness (TIA)

Total Information Awareness (TIA) var et program utviklet av det amerikanske forsvarsdepartementets forskningsenhet DARPA etter terrorangrepene i New York i 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.

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...

- o -

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 butikkentre og idrettsarenaer. For noen år siden ble en selvmordsbomber anholdt på et butikk-senter i nærheten av der hvor sønnen hennes bor. Senteret hadde visstnok nettopp begynt 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 passasjer-skanning.

Selv er hun ikke så bekymret for butikkentre. 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 butikkentrene hevder at de taper penger fordi de ikke får lov til å sette opp skanneutstyr som for eksempel *nakenmaskiner*.

Carla tar ut passet sitt og går opp til iris-skanneren. Hun vet at noen land fortsatt bruker fingeravtrykk i sine ID-kort og pass, men hun synes at det å bruke iris er tryg-

gere. 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 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.”

kontrolleres ved en annen landegrense. Bli dataene slettet etterpå også der?

Hun husker det var en skandale for noen år siden med en sentral fingeravtrykks-database – 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!



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

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

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.

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 *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.

Biometriske pass

Et biometrisk pass består av selve dokumentet, (den 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 (strek-koden) 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.

Selv om hun er 62, er Carla selvbevisst i forhold til kroppen sin, og hun er glad for at de unge mennene ved sikkerhetssperingen 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.

Peter går gjennom flyplasshallen og over til sikkerhetskontrollen. Fast lane-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 sko-

svette, hjerterytm... 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



ene for forretningsfolk inneholdt metall. Han trekker inn magen og går gjennom *nakenmaskinen*. "Hvorfor holder de alltid så lav temperatur i dette rommet?" tenker han, og rødmer idet han legger merke til at en av sikkerhetsvaktene er en 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 "sper-ring" som noen av passasjerene blir bedt om å gå gjennom. Han husker vagt noe om at et nytt sikkerhetstiltak skulle prøves ut på denne flyplassen. Det registrerer visstnok slikt som kroppsvarme,

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.

hurtigøen? Vet de ikke at folk som velger fast lane 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.

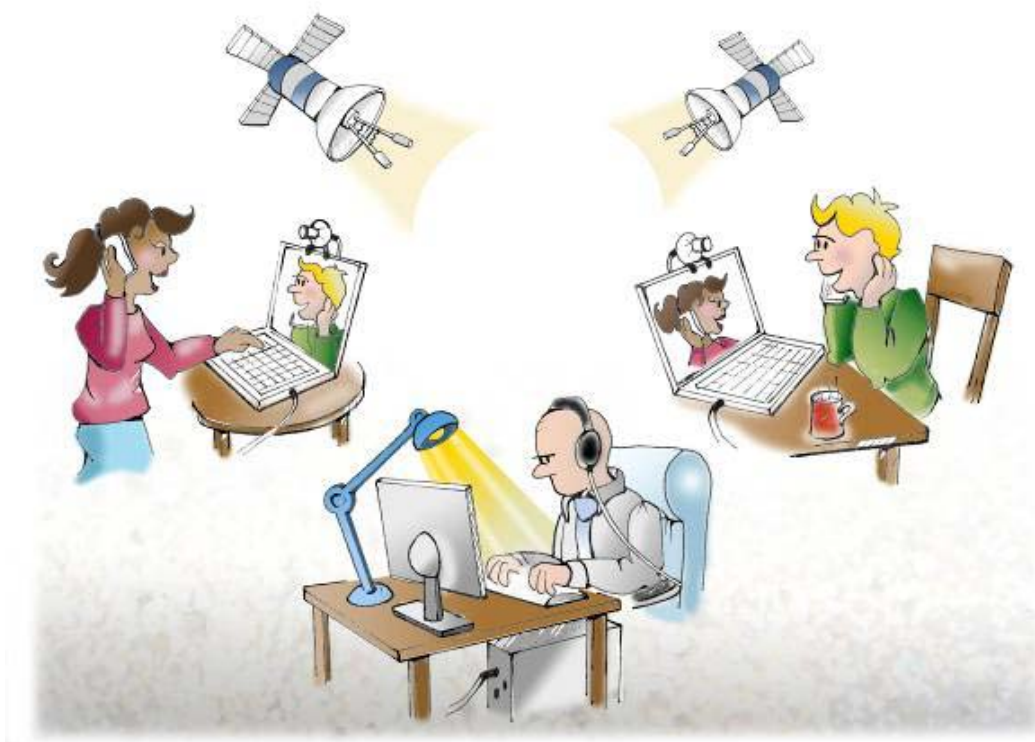
Han ønsker heller ikke å bruke internett. Det er ikke godt å vite hva som blir loggført i flyplassens nettverk. Han er ikke engang sikker på hvordan reglene er nå om dagen. Har politiet direkte tilgang til slike data, eller trenger de en rettskjennelse?

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 personvernsprikk 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. Innholdet i kommunikasjonen lagres ikke. Dataene kan oppbevares i inntil 2 år.



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 gjennomført, 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

Avlytting

Det finnes ulike måter å overvåke folk og deres kommunikasjon på, enten den finner sted over internett, 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 hos 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.

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.

Personvern fremmende teknologier

Teknologi som bidrar direkte til å beskytte personvernet kalles for personvern fremmende 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 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. 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 forvrengte 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.

“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.

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...”