PRISE
privacy • security

Security Research

PASR

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

Scenarier om sikkerhedsteknologi og privatlivets fred

Indholdsfortegnelse **side**

Forord

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

Projektet vil:

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

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

Introduktion

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

Hvad er sikkerhedsteknologi?

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

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

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

Hvad er privatlivets fred?

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

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

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

Kritikere af sikkerhedsteknologi og overvågning hævder, at mange af de tiltag, som implementeres, ikke egner sig til terrorbekæmpelse, men kun til at forsikre offentligheden om, at ”der gøres noget”. Grunden er, at disse tiltag kan omgås, eller fordi den trussel, som de adresserer, er for usandsynlig til at retfærdiggøre den handling, som rettes imod den. Et meget anvendt eksempel herpå er forbudet mod anonyme telefonkort i mange lande. Kritikere af dette forbud hævder, at det kun forhindrer opkald fra almindelige mennesker, som gerne vil være anonyme. De kriminelle kan på forskellig måde omgå denne lov ved at registrere sig med en falsk identitet eller ved at anvende stjålne mobiltelefoner.

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

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

Hvad er din holdning til sikkerhedsteknologier?
- Inspirerende scenarier til diskussion.

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

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

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

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

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

hun. Hun vil helt sikkert ikke gøre det oftere end strengt nødvendigt!

Biometri

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

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

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

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

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

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

Peter er 32. Han arbejder som salgsrepræsentant for en bilforhandler. Her til morgen er han stået tidligt op for at tage til en biludstilling i Centraleuropa. Han står op, tager et hurtigt brusebad, snupper sin taske og tager afsted til lufthavnen. Han er som sædvanlig forsinket, men da han er registreret til *hurtig check-in*, skulle alt være i orden. Den hurtige check-in service tillader ham at springe over alt bøvlet, hvor pas skal forevises, passagererne sammenholdes med kriminelles profiler og selvfølgelig det gennemgribende sikkerhedscheck. Med den hurtige check-in service gennemgår man én gang for alle en særligt omfattende indregistreringsprocedure – og lader lufthavnen opvare alle sine data. Til gengæld kan man så slippe for den almindelige check-in og blot ved hjælp af biometrisk teknologi ved indgangen godtgøre, at man er den, man er.

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

- o -

Carla ankommer til hovedbanegården. Som i undergrundsbanen er der kameraer alle vegne. Skærme og højttalere på væggene gentager advarsler om sikkerhed, indtil ingen længere bemærker dem. ”Hold Deres bagage under opsyn.” ”Deres billede vil blive sammenlignet med en database med kendte terrorister.” Der var en debat om dette for et par år siden. Mange lande fortæller ikke, at de tager billeder og checker dem i forskellige databaser og det blev foreslået, at det heller ikke skulle være nødvendigt at gøre det her. Men regeringen udtrykte sig vældigt klart omkring det princip, at folk bør vide hvornår og hvor de bliver checket. ”Det er særligt vigtigt, når man ikke selv er opmærksom på, at det sker. Man kan ikke længere vide, om man bliver fotograferet eller ej,” reflekterer Carla. Hun har hørt, at der er lande, hvor man også screener folks e-mails og telefonsamtaler for ord eller fraser, som er mistænkelige. Men det kan vel helt sikkert kun være rygter!

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

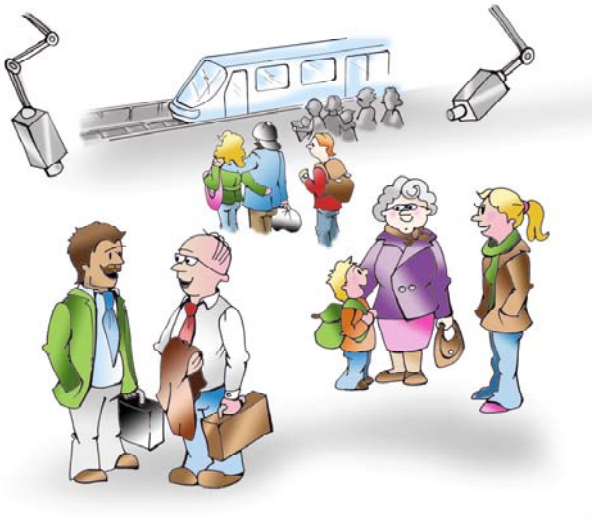
Det er ikke fordi, at hun ikke er vant til kameraer. De har været en del af bybilledet hele hendes voksenliv, men er de ikke blevet en smule mere nærgående på det sidste? Efter man begyndte at anvende software til både ansigts- og mønstergenkendelse, føler hun sig mere observeret og evalueret end før: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

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

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

Kameraovervågning - Closed Circuit Television (CCTV)

CCTV overvågning med *aktive kameraer* fungerer på den made, at en operatør betragter skærmen og kontrollerer kameraet (ved at dreje og zoome), så det følger et individ eller en situation, som udvikler sig. Aktive kameraer



kan anvendes med automatiske visuelle overvågningsprogrammer, som anvender algoritmer til at spore mistænkelige bevægelser eller identificere mennesker ved at sammenligne deres billede med billeder i en database.

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

Automatisk Ansigtsgenkendelse

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

Automatisk Nummerplade Genkendelse (ANPR)

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

"Når du er blevet arresteret af et antiterrorkorps i skudsikre veste og du ser ud, som jeg gør, så ser folk anderledes på dig bagefter – også selvom du får en undskyldning, når du bliver løsladt." Carla ved, at han i tiden derefter holdt sig væk fra områder med megen kameraovervågning, især når han havde sine børn med sig.

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

- o -

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

Gennem de seneste år har der været forslag om, at teknologien skulle anvendes til

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

Efter en forskningsrapport, der beskrev, hvor mange liv, der kunne reddes i trafikken, hvis fartgrænserne blev respekteret af bilisterne, blev det foreslået, at sikkerhedssystemerne burde indeholde et modul, som kunne sammenholde fartgrænserne med bilens speedometer. Det oprindelige forslag var, at en chip i motoren skulle sikre, at ingen biler kunne overskride fartgrænsen, men dette blev mødt med stærke protester både fra bilindustrien og fra bilejerforeninger. For øjeblikket er systemet udformet sådan, at hver gang en bil overskrider fartgrænsen, foretages der et opkald til det centrale bøderegister, hvor bøden automatisk betales via bilejerens konto.

Lokaliseringsteknologi

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

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

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

anvende fire satellitter kan GPS også bestemme højden.

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

eCall

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

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

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

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

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

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

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

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

”Function Creep”

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

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

For nogle få år siden, lige efter at et stort terrorangreb blev forhindret i USA, blev

det rent faktisk foreslået, at sikkerhedsorganisationer skulle have lov til at søge i alle databaser. Det var ikke blot databaser, som indeholdt data om folk, der var mistænkt for forbrydelser og terror. De ønskede også at analysere alt materialet i biblioteksdatabaserne, elektricitets- og gasforbrugsmønstre, data vedrørende telefon og Internet, rejsedata og indkøbsmønstre. Ved at søge efter mistænkelige mønstre ville de identificere mulige terrorister.

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

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

”Total Information Awareness” (TIA)

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

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

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

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

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

Carla tager sit pas frem og går op til iris scanneren. Hun ved, at nogle lande stadig anvender fingeraftryk i deres ID og pas. Men hun synes at iris scanningen er sikrere. Aflæseren sammenligner hendes

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

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

Radio Frekvens Identifikation (RFID)

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

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

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

Biometrisk Pas

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

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

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

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

For at tage hånd om disse spørgsmål er der udviklet et program for grundlæggende adgangskontrol (*basic access control* (BAC)). I BAC anvender aflæsningssystemet en "nøgle", som er lavet ud fra numeriske dataelementer i den maskinelle aflæsningszone (stregkoden), til at "oplåse" chippen, således at systemet kan aflæse det. BAC er blevet kritiseret for ikke at være sikkert nok og sikkerhedseksperter har på meget kort tid kunnet knække krypteringen .Hun husker, at der var en skandale for et par år siden vedrørende en central database for fingeraftryk – var det i USA? En del fingeraftryk blev stjålet af en ansat og solgt til internationale kriminelle. Tusinder af mennesker fik deres identiteter stjålet og oplevede alle mulige problemer – fra at blive sortlistet ved grænser til at deres bankkonti blev tømt. Det var specielt vanskeligt, fordi det tog så lang tid før regeringen ville indrømme, at den havde mistet de omtalte data. I mellemtiden troede ingen på, at deres identitet var blevet stjålet – eller at det overhovedet var muligt at bruge en anden persons fingeraftryk til at stjæle vedkommendes identitet!

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

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

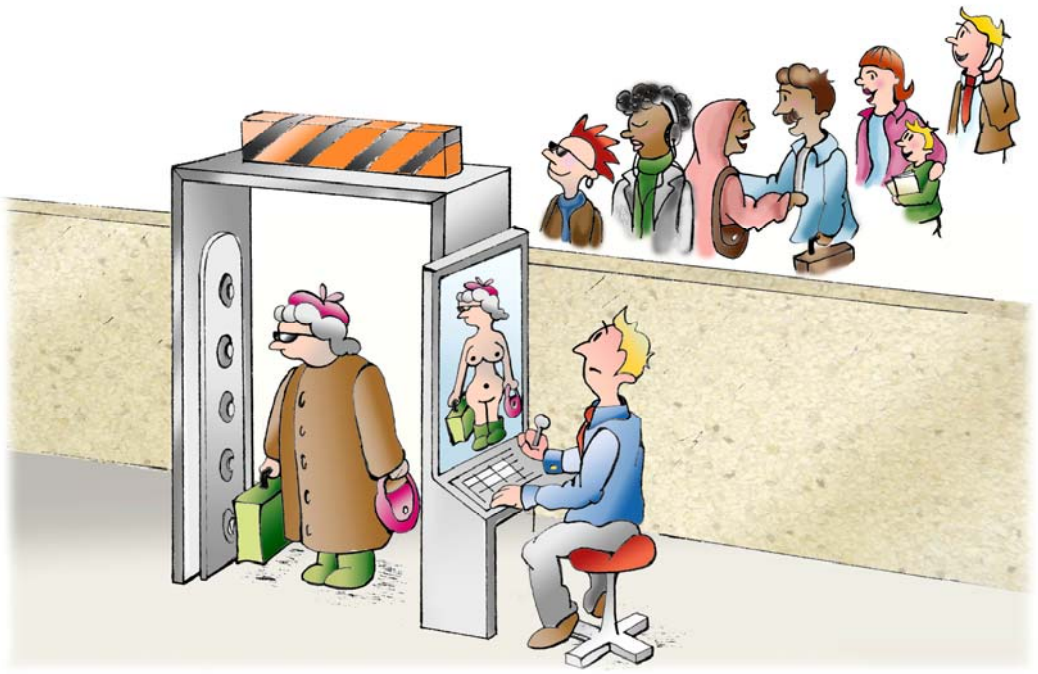
til lufthavne og internationale togterminaler i hendes hjemland. Sikkerhedsautoriteterne evaluerede forskellige maskiner, men besluttede, at det var lige så sikkert at have en type maskine,

Scanning af passagerer (*Naked machine*)

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

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

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



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

- o -

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

Opbevaring af data

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

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

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

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

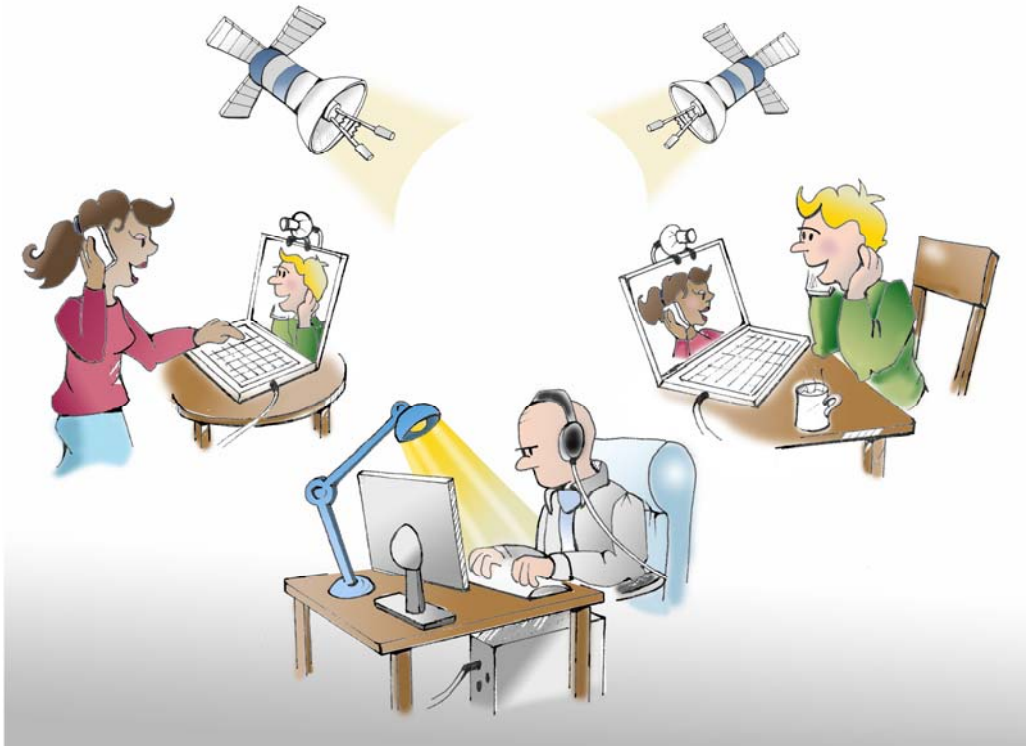
den *rigtige* naked machine. Det føles på en eller anden måde sikrere.

Peter bemærker et supplement til sikkerheds-checket, som han ikke har set før. Efter *the naked machine* er der endnu en scanner, som nogle af passagererne anmodes om at passere igennem. Han husker svagt noget om, at et nyt sikkerhedselement er ved at blive afprøvet i denne lufthavn. Det skulle kunne registrere værdier for kropsvarme, sved, puls... værdier, der kan være indikationer på sygdomme såsom SARS eller fugleinfluenza eller vise, at en person er nervøs. Nogle af de undersøgte personer eskorteres til nærliggende afhøringsrum. Han er glad for, at han ikke blev udtaget til denne test, selvom han er sund og rask og har ren samvittighed. ”Men at afprøve den ved hurtig check-in? Ved de ikke, at folk, der anvender denne indgang, har travlt?”

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

Aflytning

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



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

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

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

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

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

- o -

”Min mor er på vej,” siger Carla’s søn til sin kone, efter at han har modtaget en besked på sin mobil. ”Hun burde være her om cirka tre timer.” Hans mor ved det ikke, men den nye mobiltelefon, hun fik i julegave, er forbundet til en børneovervågningsservice (*Kid-watch*). Teknologien er en ny version af de sporesystemer, som man kunne se i gamle spionfilm, hvor overvågerne kunne se deres mistænkte som små prikker på et kort. Den største forskel er, at ved at anvende den indbyggede Galileo teknologi

Privatlivsfremmende Teknologier

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

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

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

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

i mobilenheden kan han følge sin mors bevægelser på et kort,

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

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