



Overvåkning, personvern og sikkerhet

Hva mener du?



surprise

surveillance
privacy
security



Innhold

1	Velkommen til SurPRISE	5
1.1	Hvordan lese informasjonsheftet	6
2	Oppsummering	7
3	En helt vanlig dag...	9
3.1	Overvåkning, personvern og sikkerhet	10
3.1.1	Overvåkning	10
3.1.2	Personvern og datalagring: viktige utfordringer	11
3.1.3	Sikkerhet	11
4	Tre nye typer sikkerhetsteknologi	13
5	Smarte overvåkningskameraer	15
5.1	Hvorfor ble smarte overvåkningskameraer utviklet?	15
5.2	Hvordan blir smarte overvåkningskameraer brukt?	17
5.3	Økt sikkerhet	18
5.4	Utfordringer	18
6	Pakkesniffing og overvåkning på nett	21
6.1	Hvorfor ble pakkesniffing utviklet?	21
6.2	Hva brukes pakkesniffing til?	22
6.2.1	Kommersiell bruk	23
6.2.2	Pakkesniffing og sikkerhet	24
6.3	Økt sikkerhet	24
6.4	Utfordringer	24
7	Lokalisering av smarttelefoner	27
7.1	Hvorfor ble lokalisering av smarttelefoner utviklet?	27
7.2	Hvordan fungerer lokalisering av smarttelefoner?	29
7.2.1	Kommersiell bruk	29
7.2.2	Lokalisering og sikkerhet	30
7.3	Økt sikkerhet	30
7.4	Utfordringer	31
8	Er teknologi den eneste løsningen?	33
8.1	Lokale løsninger	33
8.2	Nasjonale og internasjonale løsninger	33
9	Tilbake til deg...	35
	Om informasjonsheftet	36

1 Velkommen til SurPRISE

SurPRISE er et europeisk forskningsprosjekt. Navnet SurPRISE står for overvåkning, personvern og sikkerhet (Surveillance, Privacy and Security). Målet med prosjektet er å få innbyggernes syn på ny sikkerhetsteknologi. Mye av denne teknologien baserer seg på overvåkning av personer. Den blir brukt av politi eller sikkerhetspersonell for å følge med på hva som skjer, og for å oppdage og avverge kriminelle handlinger.

Når du skal ut på reise og bagasjen din skannes automatisk eller når du blir filmet av et overvåkningskamera på gaten, er du i kontakt med overvåkningsbasert sikkerhetsteknologi. SurPRISE har som mål at slik teknologi skal være effektiv og trygg, og ivareta menneskerettigheter og personvern. For å få til dette trenger vi din hjelp.

Vi har invitert deg til å delta i SurPRISE-prosjektet fordi EU-kommisjonen ønsker å komme i kontakt med innbyggere i hele Europa, og få vite hva de kan gjøre for at du skal føle deg trygg. Ved å delta på folketoppmøtet får du mulighet til å dele dine meninger om sikkerhetsteknologi.

SurPRISE-prosjektet arrangerer folketoppmøter i ni europeiske land: Storbritannia, Østerrike, Danmark, Tyskland, Ungarn, Italia, Spania, Sveits og Norge. Resultatene blir i juni 2014 overlevert til EU og myndighetene i Norge og de andre landene, og blir samtidig gjort tilgjengelig for media og innbyggerne.

Dette heftet inneholder informasjon om de temaene vi skal diskutere på folketoppmøtene, både i Norge og resten av Europa. Det gjelder ny sikkerhetsteknologi, men også mer generell informasjon om overvåkning, sikkerhet og personvern i Europa.

Det kan være en utfordring å lese mye ny informasjon. Vi prøver ikke å gjøre deg til en ekspert på området, og vi kommer ikke til å teste hvor mye du vet. Målet med heftet er bare å vise noe av det vi skal diskutere på møtet, og sette i gang noen tanker om temaet hos dere som skal delta. Det er nettopp fordi du ikke er ekspert på området at det er viktig å få høre din mening. Vi har invitert deg fordi du er en vanlig innbygger som blir påvirket av de beslutningene politikerne våre tar.

SurPRISE-prosjektet vil formidle resultatene fra møtet til folkevalgte og andre beslutningstakere. Bruken av sikkerhetsteknologi kan diskuteres opp mot menneskerettigheter, rettferdighet og troverdigheten og effektiviteten til samfunnsinstitusjoner. Derfor bør diskusjoner om dette involvere befolkningen og ikke bare politikere, industrien eller eksperter. Det er politikere som utformer politikken, men du som innbygger må leve med disse beslutningene. Det gjør din mening viktig.

Vitenskapen gir oss informasjon, men forteller oss ikke hva vi skal gjøre. Valget er vårt. Si din mening!

1.1 Hvordan lese informasjonsheftet

Heftet har fem hovedkapitler. Kapittel 3 gir en kort innføring i overvåkning, sikkerhet og personvern i Europa. Kapittel 5, 6 og 7 tar for seg tre typer sikkerhetsteknologi som skal diskuteres på folketoppmøtene.

På det norske folketoppmøtet vil vi diskutere to av dem:

- pakkesniffing og overvåkning på nett (kap. 6) og
- lokalisering av smarttelefoner (kap. 7).

Teksten beskriver hvorfor teknologien ble utviklet, hvordan den brukes, på hvilken måte den øker sikkerheten og hvilke begrensninger den har. Kapittel 8 gir en kort introduksjon til hvilke alternativer som finnes til sikkerhetsteknologi.

Hvis du ikke ønsker å lese dokumentet i sin helhet, finner du en oppsummering av de viktigste punktene i kapittel 2.

2 Sammendrag

Hensikten med SurPRISE-prosjektet er å forstå hvilke synspunkter europeiske borgere har på ny sikkerhetsteknologi. Europeiske myndigheter er i økende grad bekymret for terrorisme, organisert kriminalitet og nettkriminalitet. Derfor investerer de stadig mer ressurser i ny sikkerhetsteknologi. Sikkerhetsteknologi kan brukes til å analysere informasjon som innbyggerne etterlater seg hver dag, for eksempel data fra mobiltelefoner og internettbruk. I tillegg kan de også bruke «smart» teknologi, som digitaliserte overvåkningskameraer som kan identifisere kriminelle og terrorister, kanskje til og med før de har gjort noe galt.

Fordi denne typen teknologi innhenter og bruker personopplysninger, kalles den «overvåkningsbasert sikkerhetsteknologi».

Overvåkningsbasert sikkerhetsteknologi er:

teknologi som bruker informasjon om befolkningen generelt, innhentet fra forskjellige kilder og i ulike sammenhenger, for å løse en sikkerhetsmessig utfordring.

På SurPRISE-folketoppmøtene rundt i Europa diskuteres tre slike teknologier:

- **Smarte overvåkningskameraer:** Overvåkningskameraer som gjør mer enn passivt å overvåke det offentlige rom. Smarte overvåkningskameraer består av sammenkoblede digitale kameraer som til sammen kan gjenkjenne ansikter, analysere adferd og oppdage gjenstander.
- **Overvåkning av internett med pakkesniffing:** Gjennom spesiell maskin- og programvare, kan meldinger som blir sendt over internett bli lest, analysert og endret.
- **Sporing av smarttelefoner:** Ved å innhente posisjonsdata fra smarttelefoner, kan man analysere hvordan den som bruker telefonen beveger seg. Smarttelefonens posisjonsdata kan angis av GPS-systemer, trådløse nettverk og mobilmaster.

Sikkerhetsteknologi bidrar til økt sikkerhet gjennom å identifisere mistenkte og kriminelle, og avdekke ulovlige aktiviteter. De kan også bidra til å gjøre livet enklere for folk. Men hver teknologi har også ulemper. Smarte overvåkningskameraer fungerer kun under gitte forhold og kan utløse mange falske alarmer. Overvåkning av internett med pakkesniffing bryter ned personvernet knyttet til kommunikasjon på internett. Smarttelefon-sporing er vanskelig å begrense fordi mange applikasjoner sender posisjonsinformasjon uten at brukeren vet det. Mangelen på kontroll over innhenting og bruk av informasjonen er en gjennomgående utfordring ved alle de tre typene teknologi vi skal se på.

Noen innbyggere er usikre på hvordan de skal forholde seg til at personopplysninger brukes i sikkerhetsteknologi. Dersom samfunnet blir tryggere som følge av dette, er det kanskje ok. Men folks holdninger kan være avhengig av hvordan de forholder seg til andre spørsmål, som for eksempel:

- **Fungerer teknologien?**
- **Hvor mye griper den inn i privatlivet?**
- **Har vi tillit til institusjonene som bruker teknologien?**
- **Finnes det lover for å regulere bruken av den?**
- **Hvem holder et øye med dem som administrerer og bruker teknologien?**
- **Hvilke alternativer finnes, og er de hensiktsmessige?**

Dette er noen av spørsmålene vi kommer til å diskutere under folketoppmøtet. Dersom du ønsker å få vite mer om disse problemstillingene, kan du lese videre.

3 En helt vanlig dag...

Like sør for Budapest kjører Aisha inn på europavei E-75, på vei til den internasjonale flyplassen i Budapest. Hun husker da hun kjørte på denne veien for første gang. Da måtte hun betale bomavgiften idet hun passerte; nå blir den automatisk trukket fra bankkontoen hennes. Nummerskiltet på bilen blir lest av et kamera som har teknologi for automatisk skiltgjenkjenning, mens bomavgiftssystemet tar seg av resten. Før la ikke Aisha merke til overvåkningskameraene, men nå lurer hun på hvordan informasjonen blir sendt til hennes bank.

Aisha parkerer bilen og går om bord i bussen som kjører henne til terminalen. Der sjekker hun inn på en automat, legger passet sitt i automaten og den leter frem bookinginformasjonen hennes. Idet hun mottar boardingpasset, innser hun at også denne informasjonen blir lagret et eller annet sted.

Etter å ha vært igjennom sikkerhetskontrollen, setter Aisha seg ned på en kaffebar. Hun bestiller en kaffe, men stopper opp et øyeblikk idet hun skal til å betale. «Veldig praktisk med disse kortene», tenker hun, «men hvem lagrer alle transaksjonene, og hvorfor?»

Mens hun drikker kaffen sin, finner Aisha fram smarttelefonen for å sjekke om hun har fått noen nye meldinger. Når skjermen aktiveres, har den angitte posisjonen skiftet fra Kecskemét, der Aisha bor, til Ferihegy Budapest internasjonale lufthavn. «Hvordan kan den vite det? Det er sikkert en innlysende forklaring, men jeg kommer ikke på noen», funderer hun.

Aisha har akkurat nok tid til å sende en e-post til en kollega før hun må om bord. Mens hun aktiverer flymodus, lurer hun på hva som skjer med e-posten og dens vei gjennom internett.

Aishas erfaringer er ikke utenom det vanlige. Enhver reisende kan nok kjenne seg igjen. Teknologi gjør reisen sømløs og praktisk, men samtidig skaper den utfordringer: «Hvem bruker mine personopplysninger, og hva betyr det for meg at de er «i systemet»?

Mye av den teknologien Aisha møter, finnes også utenfor flyplassen. Mange kan ikke forestille seg et liv uten smarttelefon, bankkort eller internett. Faktisk er det slik at mange hverdagslige aktiviteter generer den type elektroniske spor som Aisha nå tenker på. Kanskje har du de samme spørsmålene som Aisha. Disse sporene kan si noe om hvor vi befinner oss, både i tid og i rom, men også hva vi gjør. Banktransaksjoner, som for eksempel de som gjøres med et bankkort, kan fortelle hva slags kjøp vi gjør og hvem vi handler med. Dette er informasjon som oppbevares i bankenes databaser, og som er synlig på kontoutskriften.

Flyselskapenes bestillingsinformasjon forteller om vi reiser til eller fra et høyrisiko-land. Mobildata kan fortelle hvor vi befinner oss, hvem vi snakker med og hvor ofte vi ringer dem. Teleselskapene oppbevarer denne typen informasjon i faktureringsdatabaser, og derfor er det mulig å identifisere, lokalisere og spore de fleste av oss. Kanskje det er akkurat det som bekymrer Aisha. Samtidig er hun jo positiv til de fordelene teknologien tilbyr.

Andre kan også dra nytte av informasjonen fra denne typen teknologi. I kjølvannet av større terrorangrep i Europa og i verden, har myndighetene i mange land investert i avansert sikkerhetsteknologi. Lover har også blitt endret og vedtatt slik at myndighetene får tilgang til denne type informasjon i sikkerhetsøyemed. Myndigheter har innsett at terrorister og kriminelle kan spores gjennom andre kilder enn de mer «tradisjonelle» etterretningskildene. Kriminelle og terrorister

har også et hverdagsliv som er veldig likt alle andres: de har bankkontoer og identitetspapirer, og bruker internett og mobiltelefoner. De bruker også offentlig transport, de ferdes på offentlige steder og kjøper varer og tjenester. Det kan hende at informasjon om denne type aktiviteter kan være viktig for å spore opp terrorister og kriminelle. Mange myndigheter tror også at denne type informasjon kan gjøre det mulig å stanse terrorister og kriminelle før de handler. Fordi noen sikkerhetsteknologier bruker denne typen informasjon, blir de betegnet som «overvåkningsbasert sikkerhetsteknologi» av SurPRISE-prosjektet.

En overvåkningsbasert sikkerhetsteknologi er:

en type teknologi som bruker informasjon om befolkningen, innhentet fra forskjellige kilder og i ulike sammenhenger i den hensikt å løse en sikkerhetsutfordring.

Dersom Aisha visste at hennes informasjon ble brukt til å løse en sikkerhetsutfordring, ville hun da vært mindre skeptisk til denne type teknologi? Hvis det innebærer økt sikkerhet for henne og alle andre, vil hun kanskje akseptere teknologien? Denne typen teknologi fører med seg en rekke spørsmål om menneskerettigheter, personvern, regulering og tillit. De kan innhente og dele informasjon om en person, uten at vedkommende vet om det. Det er uunngåelig at også informasjon om uskyldige personer blir innsamlet, og i noen tilfeller blir dette gjort med hensikt. Slik teknologi vil derfor ofte bryte med personvernet, noe som er en menneskerettighet i Europa.

En rekke spørsmål oppstår:

- Har vi tillit til institusjonene som bruker slik teknologi?
- Hvor godt regulert er disse institusjonene?
- Blir teknologien brukt i samsvar med loven?
- Er det åpenhet rundt institusjonene, og tar disse ansvar hvis personvernet brytes?
- Gjør denne typen teknologi samfunnet sikrere og tryggere?

Dette er noen av spørsmålene vi skal diskutere på folketoppmøtet.

I de neste tre avsnittene presenterer vi noen nøkkelbegreper og definisjoner. Deretter beskriver vi de tre teknologiene som skal diskuteres på folketoppmøtene.

3.1 Overvåkning, personvern og sikkerhet

3.1.1 Overvåkning

Når vi tenker på overvåkning, dukker en rekke assosiasjoner opp. Kanskje du tenker på «Big Brother» – enten reality-programmet eller Georges Orwells bok «1984». Derfor er det lett å knytte begrepet overvåkning til en uggen følelse av å bli iaktatt av en mektig, men ukjent organisasjon eller person.

Når vi refererer til overvåkning i SurPRISE, tenker vi på det som «å observere mennesker for å regulere eller styre deres adferd », til ulike formål. Overvåkning kan iverksettes av sikkerhetshensyn, som for eksempel at politiet setter opp overvåkningskamera for å finne kriminelle i gatebildet. Overvåkning kan også brukes av private næringsdrivende. Butikker kan for eksempel bruke bonuskort for å samle informasjon om forskjellige kundegruppers innkjøpsmønstre. Denne informasjonen kan i sin tur brukes til å skreddersy tilbud til kundene. Overvåkning kan altså brukes til forebygging og etterforskning av kriminalitet, men også til å tilby mer tilpassede produkter og tjenester til forbrukere.

Dersom overvåkning er så utbredt og integrert i samfunnet, lurer du kanskje på hva som kan være galt? Nyhetsartikler om det som kalles “overvåkningssamfunnet” har ofte en dyster undertone. Å ha kontroll over overvåkningsteknologi medfører mye makt. Derfor er det viktig at de som har denne muligheten, som i politiet eller i næringslivet, bruker makten i tråd med lovene og respekterer våre rettigheter.

Hvem som driver med overvåkning, hvorfor de gjør det og hva de leter etter, kan påvirke ditt syn på overvåkningen. Kanskje du mener at du ikke har noe å skjule, og at det derfor ikke er så nøye? Hvis noen plutselig bestemmer seg for å overvåke deg på grunn av din religion, etnisitet, kjønn eller politiske holdninger, forandrer du kanskje mening. Det er på grunn av dette at overdreven overvåkning kan ha negative konsekvenser for menneskerettighetene, som for eksempel ytringsfriheten. Det kan også svekke tilliten i samfunnet, fordi folk kan bli redde for å være seg selv. Det er derfor en vanskelig balansegang å anvende ulike typer overvåkningsteknologi i sikkerhetsøyemed.

3.1.2 Personvern og datalagring: viktige utfordringer

En av de viktigste utfordringene er balansen mellom personvernet og sikkerhetsteknologienes innsamling og bruk av personopplysninger. Personvern kan bety forskjellige ting for forskjellige mennesker, men det er en viktig del av vårt hverdagsliv. Det kan være mye du ikke alltid vil dele med andre:

- Hva du gjør, tenker og føler
- Informasjon om intime forhold, hvor du befinner deg, hva du kommuniserer til andre, og bilder av deg selv.
- Hvor mye av kroppen din du viser, uønsket kroppsvisitering, og om du kan kontrollere hvordan ditt fingeravtrykk eller DNA blir brukt.

Ville du vært tilfreds med at forsikrings-selskapet ditt hadde ubegrenset tilgang til pasientjournalen din? Eller om politiet hadde anledning til å avlytte alle samtaler dine? Har du gardiner i huset ditt?

Om du svarer «nei» på de to første spørsmålene og «ja» på det siste, så er du likevel opptatt av personvern! Og du er ikke alene. Studier av unge menneskers nettvaner viser at de er veldig selektive med den informasjonen de legger ut på sosiale medier. Folk ønsker å dele informasjon, men innenfor visse grenser. Det er disse grensene som markerer hvor personvernet gjelder.

I SurPRISE definerer vi personvern som:

et individs mulighet til å være utenfor offentlighetens søkelys, og individets kontroll over sin egen personinformasjon.

Retten til personvern og beskyttelse av personopplysninger, er en grunnleggende menneskerettighet i Europa. Alle har behov for personvern: for å kunne handle fritt, møtes, diskutere og debattere i et demokratisk samfunn. Det er ikke mulig å utøve demokratiske rettigheter hvis andre vet alt om dine tanker, intensjoner og handlinger. Personvernlovgivningen som utvikles i Europa nå, legger vekt på at personvern skal være tenkt inn i ny teknologi. Bedrifter som utvikler ny teknologi oppfordres til å ta hensyn til personvernet fra starten av. Denne nye tilnærmingen kalles "innebygd personvern".

3.1.3 Sikkerhet

SurPRISE-prosjektet defineres sikkerhet som:

en tilstand der en er beskyttet mot, eller ikke utsatt for, fare; en følelse av trygghet eller fravær av fare.

Sikkerhet handler ikke bare om beskyttelse av fysiske ting (som bygninger, informasjonssystemer, nasjonale grenser osv.), men også om menneskers trygghetsfølelse. I en ideell verden ville effektive sikkerhetstiltak ført til en sterkere trygghetsfølelse, men dette er ikke alltid tilfellet.

Siden ny sikkerhetsteknologi kan føre til brudd på personvernet, kan den paradoksalt nok ende opp med å få folk til å føle seg mindre trygge. Men denne følelsen deles ikke nødvendigvis av alle. Også sikkerhet kan bety forskjellige ting for forskjellige mennesker. Hver og en av oss har formeninger om hva vi betrakter som en trussel mot vår egen sikkerhet, og hvor langt vi er villige til å gå for å beskytte det som er viktig for oss.

Dette er også tilfellet for de som har ansvaret for samfunnets sikkerhet. De må identifisere og håndtere de mest alvorlige truslene med begrensede økonomiske, menneskelige og tekniske resurser. Derfor må de gjøre prioriteringer. For EU er de viktigste prioriteringene å:

- Øke sikkerheten på internett for innbyggere og næringer i Europa
- Oppløse internasjonale kriminelle nettverk
- Forebygge terrorisme
- Styrke Europas evne til gjenoppbygging etter en krise eller katastrofe
- Lokaliseringsteknologier, som kan sikre transport og forsendelser, og spore opp mistenkte i kriminalsaker.

Fordi gjenoppbygging er en av EUs prioriteringer, har sikkerhetsbegrepet blitt utvidet utover terror- og kriminalitetsforebygging. EU fokuserer også på trusler mot miljøet, naturressurser, infrastruktur, næring og helse. Sikkerhet er nå noe som inngår i nesten alle saksområder. Denne tilnærmingen finner man i mange europeiske land. Men er det i det hele tatt mulig å etterleve garantien om full sikkerhet og trygghet på alle samfunnsområder? Sikkerhetsindustrien er en ny og raskt voksende industri under utvikling i Europa. Denne industrien inkluderer kjente produsenter som Airbus, BAE Systems og Finmeccanica, men også flere mindre selskaper. Nyere utvikling innen overvåkningsbasert sikkerhetsteknologi inkluderer blant annet:

- Smarte overvåkningskameraer, som fokuserer på å fange opp bilder av kjente kriminelle og å identifisere mistenkelig adferd før en kriminell handling blir begått
- Internettovervåkning og pakkesniffing, som har til hensikt å oppdage virus, hackere eller identitetstyver.
- Biometri, som brukes for å hindre at uvedkommende får adgang til et territorium og for å effektivisere reisen til de som har blitt definert som «sikre» av myndighetene.
- Droner, som fra luften kan filme farlige aktiviteter som ellers ikke ville vært mulig å få øye på fra bakken.
- Avansert innsamling av informasjon om flypassasjerer, med den hensikt å oppdage individer som kan utgjøre en trussel før de reiser inn eller ut av landet.

4 Tre nye typer sikkerhetsteknologi

I SurPRISE-prosjektet skal vi diskutere tre ulike typer sikkerhetsteknologi:

- **Smarte overvåkningskameraer**
- **Pakkesniffing og overvåkning på nett**
- **Lokalisering av smarttelefoner**

Disse sikkerhetsteknologiene er under utvikling, og det er fortsatt mulig å påvirke hvordan bruken av dem skal reguleres.

Vi beskriver hvordan teknologien fungerer, hvorfor den har blitt utviklet, hvem som bruker den og hvordan den brukes. Vi skal også beskrive hvordan den kan bidra til økt sikkerhet, og hvilke utfordringer den

medfører for personvernet og andre viktige problemstillinger.

Det er viktig for SurPRISE-prosjektet og for EU å forstå hvordan folk oppfatter sikkerhetsteknologi og om teknologien blir akseptert av befolkningen. Derfor er din mening viktig. Det kan hende at du allerede har sterke meninger for eller mot sikkerhetsteknologi. Under folketoppmøtet får du flere anledninger til å si hva du mener, og vi ønsker spesielt at du skal tenke på følgende spørsmål:

Hva avgjør om du aksepterer eller ikke aksepterer ny sikkerhetsteknologi?

Er det:

- å ha kjennskap til teknologien, og hvordan den fungerer?
- å vite mer om institusjonene som benytter seg av teknologien, og hva slags type informasjon teknologien gir?
- at bruken er regulert og kontrollert av et lovverk?
- å være bedre informert om de sikkerhetsutfordringene vi står overfor, og som teknologien er skal løse?

Eller kanskje handler det om hvor sterkt teknologien utfordrer personvernet? For eksempel:

- setter den deg i forlegenhet på noen måte?
- bryter teknologien med fundamentale menneskerettigheter?
- blir privat informasjon delt med tredjeparter uten ditt samtykke? Eller påvirker den privatlivet ditt på andre måter?

Kanskje det er et spørsmål om hvor effektiv teknologien er?

- forenkles hverdagen din?
- føler du deg tryggere?
- er den et effektivt virkemiddel for å identifisere kriminelle?

Kanskje du kun tenker på sikkerhetsteknologi når du merker at den er i nærheten av deg, for eksempel på flyplasser, på gata, når du bruker en mobiltelefon eller er på internett. Kanskje du har et avslappet forhold til sikkerhetsteknologi nå, men er bekymret for hvordan de kan brukes i fremtiden.

5 Smarte overvåkningskameraer

Tidligere møtte du Aisha på vei til flyplassen, og så at hun lurte på hvordan kameraene ved bomstasjonen fungerte. Kameraene var en del av et automatisk skiltgjenkjenningssystem, og er et eksempel på bruk av smarte overvåkningskameraer.

De fleste europeere vet hvordan overvåkningskameraer fungerer. Et tradisjonelt overvåkningskamera-system består av flere kameraer som er montert i butikker og i det offentlige rom. Kameraene er tilkoblet et kontrollrom der sikkerhetspersonell overvåker et sett av videoskjermer. Det blir gjort opptak av bildene som deretter lagres og så slettes etter en gitt frist. Systemet er «lukket» i den forstand at bildene ikke blir kringkastet, men kun overført til kontrollrommet. Dersom sikkerhetspersonellet legger merke til noe mistenkelig, kan de kontakte vektere eller politiet som kan undersøke situasjonen nærmere.



5.1 Hvorfor ble smarte overvåkningskameraer utviklet?

Overvåkningskameraer ble opprinnelig utviklet for å overvåke rakettutskytinger under andre verdenskrig, og for å kunne følge med på farlige industrielle prosesser på trygg avstand. Det var først på 1950-tallet i USA at de ble kommersialisert som sikkerhetsteknologi. Bruken av overvåkningskamera i Europa vokste i omfang på 1990-tallet, hovedsakelig i Storbritannia, Frankrike og Nederland. Bilder fra overvåkningskameraer dukker stadig opp i nyhetssendinger, og i 2013 var bildene fra overvåkningskamera sentrale for å få identifisert de skyldige etter bombingene av Boston Marathon.

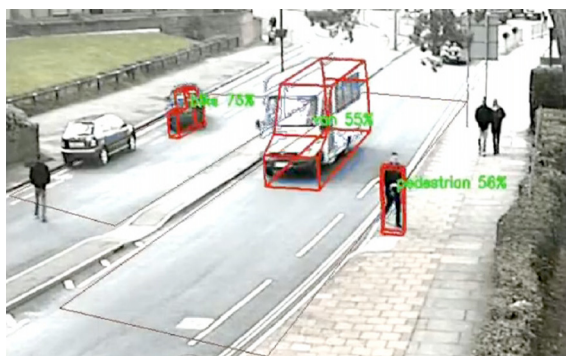
Smarte overvåkningskameraer ble utviklet for å håndtere den svakheten som tradisjonelle kameraovervåknings-systemer alltid har hatt: sikkerhetspersonellens begrensede kapasitet til å få med seg hva som foregår på hver enkelt av de mange skjermene, til enhver tid. Smarte overvåkningskameraer er derfor koblet til hverandre og til et system som analyserer bildene automatisk. Hvis analyseprogrammet oppdager noe mistenkelig, varsles sikkerhetspersonellet som deretter kan vurdere hva som foregår på bildene. Varslene og de tilhørende bildene blir lagret og kan enkelt bli hentet ut eller delt.

Smarte overvåkningskameraer kan utføre en rekke oppdrag. Oftest går disse ut på:

- Identifisering av gjenstander, for eksempel biler, ved å lese av bilskilt og sammenligne dem med informasjon fra en database.
- Ansiktsgjenkjenning. Dette fungerer best mot en ensfarget, flat bakgrunn. Ansiktet sammenlignes deretter med en database av registrerte personer.
- Identifisering av bagasje uten tilsyn. Dette fungerer kun dersom bagasjen er i et åpent og tomt område

Utviklere jobber for at smarte overvåkningskameraer skal kunne utføre flere oppgaver. Dette inkluderer:

- Identifisering av enkeltpersoner i en folkemengde ut fra klærne de har på seg
- Identifisering av mistenkelig adferd, eller adferd som er uvanlig sammenlignet med hva som kan forventes, for eksempel forsøpling. Adferden sammenlignes med kjente adferdsmønstre i en database.



Alle smarte overvåkningskameraer er imidlertid ikke like. Hvor «smart» et system er avhenger av hvor godt programvaren analyserer bildene og hva som skjer med bildene etter at de har blitt delt. Ulike systemer blir satt opp for ulike hensyn, og hvert enkelt system kan derfor ikke utføre alle oppgaver.

Hvordan fungerer smarte overvåkningskameraer?

Smarte overvåkningskameraer benytter seg av spesielle algoritmer for å gjenkjenne forskjellige typer adferd. Adferd som skiller seg fra det som er vanlig, blir kalt triggerhandlinger. Dette kan for eksempel være en person som holder et våpen eller noen som står stille i en ellers bevegelig folkemengde. En algoritme er et sett med matematiske beregninger som leter gjennom informasjonen i et digitalt bilde. En intelligent algoritme lærer seg hva den bør lete etter, basert på tidligere analyser.

Algoritmene i smarte overvåkningskameraer er bygget for å etterligne hvordan øyet og hjernen fungerer. Programvaren bryter bilder ned i mindre deler, kalt piksler. Du kjenner sikkert igjen begrepet hvis du har et digitalt kamera eller en smarttelefon. Når et kamera har «3 megapiksler», består hvert bilde av 3 millioner piksler.

Algoritmen kan beregne mengden bevegelse for hver piksel, slik at programmet kan identifisere de aktive områdene i hvert bilde. Ut fra dette lærer den å gjenkjenne bevegelsesmønstre. Systemet kan identifisere og klassifisere hendelser etter hvilke mønstre den allerede kjenner til. Programvaren kan for eksempel skille mellom stillestående og hoppende tilskuere på en fotballkamp.

5.2 Hvordan blir smarte overvåkningskameraer brukt?

Smarte overvåkningskameraer er kommersielle produkter som selges av selskaper innenfor sikkerhet og forsvar. Det er allerede utviklet mange forskjellige systemer, og de viktigste brukerne finnes innenfor samferdsel slik som bomselskaper, flyplasser eller jernbane. Systemene brukes også av politi og myndigheter.

I 2012 begynte politiet i Budapest å bruke smarte overvåkningskamera for å overvåke bussfelt på veiene. Politiet kan bruke disse bildene så lenge passasjerene ikke filmes og hvis det informeres tydelig om overvåkingen. I 2003 ble det installert smarte overvåkningskameraer med ansiktsgjenkjenning på flyplassen i Zürich. Dette var aller første gang slik teknologi ble brukt for å kontrollere et lands grenser.

EU har finansiert 16 forskjellige prosjekter for å utvikle algoritmer og funksjoner for smarte overvåkningskameraer. Myndighetene i Roma, London, Paris, Brussel, Milano og Praha har nylig gjennomført prøveprosjekter for å teste intelligente systemer rettet mot overvåking av fotgjengere. Disse systemene varsler sikkerhetspersonell hvis noen etterlater seg mistenkelige pakker eller oppfører seg unormalt i menneskemengden. Dette er fortsatt under utprøving.

Den mest utbredte bruken av smarte overvåkningskameraer er å automatisk identifisere bilskilter. Informasjon som blir innhentet fra kameraene blir sammenlignet med bilregistre og databasene til forsikringsselskap og politiet.



Slik kan systemene enkelt knytte individer til et spesifikt sted og til en gitt tid. Systemet kan også brukes til å identifisere stjålne biler, fartsovertredelser og biler som kjører uten forsikring.

Et viktig spørsmål er om alle former for kriminalitet bør overvåkes på samme måte. Skal smarte overvåkningskameraer brukes for å avsløre alle former for kriminalitet, eller bare de mest alvorlige lovbruddene? I Europa er det ulike holdninger knyttet til dette. I Tyskland for eksempel, innskrenket høyesteretten politiets bruk av automatisk skiltgjenkjenning av hensyn til personvernet. Retten insisterte på at politiet skulle lagre digital informasjon fra de smarte kameraene kun dersom sammenligninger opp mot andre databaser blir gjort umiddelbart. Automatisk skiltgjenkjenning blir også brukt ved bompasseringer, men også dette har blitt kritisert, fordi det eksisterer mindre personvernkretnende teknologi som kan utføre samme oppgave. I Storbritannia har imidlertid automatisk skiltgjenkjenning ikke bare blitt brukt ved bompasseringer, men også blitt integrert i lokale og nasjonale politimyndigheters strategier. Siden 2010 har 5000 kameraer for skiltgjenkjenning blitt installert i Storbritannia, og politiets nasjonale datasenter analyserer mellom 10 og 14 millioner bilder hver dag. Strid om smarte overvåkningskameraer:

Automatisk bilskiltgjenkjenning i Birmingham, Storbritannia

I 2011 måtte politiet i Birmingham fjerne skiltgjenkjenningskameraer fra tre områder der andelen muslimske innbyggere er høy. Kameraene ble finansiert gjennom anti-terror programmet «Project Champion», men ble presentert som vanlige sikkerhetstiltak for innbyggerne. Lokale talspersoner og politikere protesterte kraftig mot kameraene, og forholdet mellom myndighetene og den muslimske befolkningen ble svekket. 200 kamera ble installert, men aldri slått på. 64 kamera var skjult og satt opp uten innbyggerne ble informert. Kameraene ble enten ødelagt eller brukt av andre politimyndigheter, og det mislykkede prosjektet kostet til sammen 3 millioner kroner.

5.3 Økt sikkerhet

Smarte overvåkningskameraer kan øke sikkerheten på flere måter:

Sikkerhetsutfordringer blir identifisert i sanntid:

- Systemet identifiserer ting som virker unormalt og varsler automatisk personalet. Dette gjør det enklere å følge med på bildene.
- Varslene gjør det mulig for operatøren å ta hurtigere beslutninger, og vurdere om andre tiltak bør settes i gang.
- Algoritmene er i stand til å behandle langt større mengder informasjon enn personalet, og kan derfor fange opp detaljer som ellers ville blitt oversett.

Redusert frykt og styrket personvern:

- Når sikkerhetsteknologi fungerer optimalt, vil folk føle seg tryggere av at hendelser utenom det vanlige blir fanget opp av smarte overvåkningskameraer
- Smarte overvåkningskameraer kan fange opp mer detaljert informasjon enn de tradisjonelle overvåkningskameraene. Dette innebærer at færre kameraer kan overvåke større områder. Færre kameraer kan oppleves mindre krenkende på personvernet.
- Personvernet kan styrkes ved at de delene av kameraets synsvinkel som dekker privat eiendom kan «sladdes», slik at det forblir skjult for sikkerhetspersonalet.

5.4 Utfordringer

Det er flere ulemper ved smarte overvåkningskameraer som må vurderes:

1. Algoritmene som brukes i dag har flere svakheter. De kan lage falske alarmer som utløses når en hendelse feilaktig blir registrert som en trussel. I verste fall kan dette føre til at uskyldige får status som mistenkte når ingen lovbrudd har blitt begått. Svakheterne til algoritmene består av følgende:

- Det er kun enkelte typer gjenstander som kan gjenkjennes med stor treffsikkerhet, for eksempel bilskilt eller bagasje uten tilsyn.
- Kameraenes evne til å identifisere adferdsmønstre og hendelser i folkemengder er begrenset
- Skult kriminalitet som lommetyveri, nasking og lignende er også vanskelig å identifisere
- Fordi det er mennesker som definerer hva som skal være normalt eller unormalt i systemet, kan algoritmene aldri bli helt nøytrale. Dermed er den fare for at systemet kan, enten bevisst eller ubevisst, rettes spesifikt mot minoriteter.
- Det er også enkelt for personer å unnslippe de smarte overvåkningskameraene, for eksempel ved å skifte klær, da algoritmene identifiserer enkeltindivider blant annet ved klærne de bruker.
- Det høye antallet falske alarmer kan svekke tilliten operatørene har til systemet, og føre til at alarmer etter hvert ignoreres.

2. Smarte overvåkningskameraer er både mindre og kraftigere:

- De kan fange opp mer informasjon. Terskelen for å bryte personvernet er dermed lavere. Dette skyldes at sannsynlighet er høy for at adferden til tilfeldig forbipasserende blir analysert og kanskje lagret.
- Kameraene er mindre synlige, slik at det er vanskeligere for folk å vite når og hvor de blir overvåket. Det blir dermed vanskeligere å unngå overvåkning.
- Ytringsfriheten kan bli utfordret dersom folk innser at deres adferd blir overvåket og analysert av programvare og sikkerhetspersonell.

Man trenger fortsatt mennesker til å styre systemene:

- Systemene kan identifisere hendelser utenom det vanlige, men de kan ikke forklare hvorfor det skjer. Personalets analyse er en uunnværlig del av systemet.
- Det bør være strengt regulert hvordan institusjoner kan bruke smarte overvåkningskameraer slik at man forhindrer misbruk av informasjonen som blir samlet inn.

4. Det lagres informasjon om hvor og når noe har skjedd. Denne informasjonen kan senere bli brukt til helt andre ting, som ikke har noe med sikkerhet å gjøre.



Det bør være åpenhet om hvorfor smarte overvåkningskameraer blir installert. Folk bør ha mulighet til å kontakte de som forvalter systemene og få svar på dette. Folk må kunne føle seg sikre på at kameraenes tilstedeværelse er velbegrunnet og at teknologien ikke vil bli misbrukt.

Chris Tomlinson, Sikkerhetskonsulent

6 Pakkesniffing og overvåkning på internett

Da Aisha satt ved kaffebaren på flyplassen, lurte hun på hva som skjedde med e-posten hun hadde sendt. Kanskje ble den utsatt for en overvåkningsteknologi kalt "pakkesniffing"?

Internettleverandører, teleselskaper og nettverksoperatører har alltid hatt mulighet til å overvåke sine nettverk. Å vite hvem som kommuniserer med hvem, hvilke nettsider som blir besøkt og hvilke tjenester som blir benyttet, legger grunnlaget for å kunne fakturere brukerne, forvalte nettverket og legge en markedsføringsstrategi. Teknologien som brukes i pakkesniffing går enda lenger, og gjør det mulig for selskaper, sikkerhetstjenester og regjeringer å lese innholdet i kommunikasjon på internett. Som en sammenlikning kan man si at pakkesniffing tilsvarer en postmann som åpner og leser alle brev, og som kan endre eller slette innholdet, eller la være å levere brevene til mottakeren. Pakkesniffing kan overvåke alt av digital kommunikasjon: tekster du leser på nett, nettsidene du besøker, videoene du ser på, og hvem du kommuniserer med, enten det er via e-post, chat eller på sosiale medier. Pakkesniffing fungerer ved å oppdage og styre hvordan meldinger blir sendt gjennom et nettverk. De åpner og analyserer meldinger mens de er på vei gjennom nettverket, og identifiserer de som kan utgjøre en risiko. Du trenger ikke være mistenkt for noe for å bli utsatt for pakkesniffing – hvis pakkesniffing først brukes, undersøkes all kommunikasjon som går via dette nettverket.



6.1 Hvorfor ble pakkesniffing utviklet?

Pakkesniffing ble opprinnelig utviklet for å oppdage virus og ondsinnet programvare som kunne skade nettverkene. Ved å bruke pakkesniffing til å analysere innholdet i meldinger som sendes over nettet, kan også andre former for kriminalitet oppdages og stoppes.

Hvordan fungerer pakkesniffing?

Når du sender eller mottar informasjon over internett, går informasjonen gjennom en svært kompleks prosess via mange forskjellige datamaskiner.

Datamaskinene bryter ned informasjonen du sender og mottar i mindre deler som kalles «pakker». Hensikten er å gjøre det enklere for informasjonen å reise gjennom internett. Hver pakke har en overskrift som beskriver hva pakken er, hvem den er fra og hvor den skal, akkurat som et brev i posten. Selve innholdet blir ikke beskrevet i overskriften. Når pakkene ankommer bestemmelsesstedet, settes de sammen til den opprinnelige meldingen.

Hver pakke består av flere lag som inneholder ulik informasjon om meldingen. Lagene ligger inni hverandre, på samme måte som en russisk dukke. Internettleverandørene må inspisere noen av pakkene for å kunne sende den videre. I de aller fleste tilfeller trenger de kun å se på overskriften, og ikke innholdet, for å sende meldingen videre. Pakkesniffing derimot, innebærer en grundigere undersøkelse av selve innholdet i samtlige pakker.



Ved pakkesniffing blir meldingene inspisert av et system som leter etter spesifikke typer data. I presentasjonen av smarte overvåkningskameraer beskrev vi algoritmer som sorterer og analyserer data. Slike algoritmer brukes også i pakkesniffing, men på en annen måte. I pakkesniffing blir algoritmene programmerte til å søke etter nøkkelord, på samme måte som når du søker etter informasjon på Google eller en annen søkemotor. Typen data som det søkes etter bestemmes av de som leter. Nøkkelordene kan være knyttet til kriminelle eller mistenkelige aktiviteter, til et nytt datavirus, eller om et spesifikt produkt har blitt kjøpt.

Pakkesniffing foregår i rutere. En ruter er en datamaskin som dirigerer meldinger gjennom forskjellige nettverk, som til sammen utgjør internett. Disse ruterne eies av internett-selskapene. Disse selskapene kan kontrollere hvordan internett fungerer lokalt, regionalt, nasjonalt og internasjonalt. Disse selskapene har vært pionérer innen pakkesniffing. Selskapene benytter seg selv av denne teknologien, for eksempel for å forhindre spredning av virus, men de kan også tjene penger på å selge teknologien til andre. Det finnes også andre selskaper som utvikler slik teknologi, noe som gjør at det etter hvert har blitt et marked for pakkesniffing.

6.2 Hva brukes pakkesniffing til?

I Europa er bruk av pakkesniffing kun lovlig for å hindre spredning av virus og ondsinnet programvare. I tillegg kan internettleverandører bruke det til å håndtere trafikkflyten i nettverkene sine. Det blir også brukt til å oppdage spesifikke typer kriminalitet, som for eksempel spredningen av barnepornografi. Selv om dette er lovlig, er det fortsatt kontroversielt å gjøre såpass detaljert pakkesniffing fordi de gjeldende EU-lovene som regulerer informasjonsinnhenting og kommunikasjon ble opprettet før pakkesniffing ble utviklet. Myndighetene i EU har tolket nåværende lovverk slik at de kun regulerer overflatisk analyse av internettrafikk. Nye lover må utvikles før man kan regulere mer detaljert pakkesniffing på en ordentlig måte. Et resultat av dette er at pakkesniffing i Europa ikke kan brukes til å identifisere brudd på opphavsrett, sensur av politiske meninger eller målrettet markedsføring, selv om

teknologien kan utføre slike analyser.

Europeisk personvern- og menneskerettighetslovgivning beskytter retten til privat kommunikasjon. Pakkesniffing bryter med Den europeiske menneskerettighetskonvensjonen fordi det innebærer overvåkning av store grupper mennesker uten at det er tatt ut tiltale. I USA er bildet litt annerledes: pakkesniffing er ikke regulert på samme måte, og mange selskaper bruker det for eksempel til målrettet markedsføring. Hvis du har en Yahoo- eller Gmail-adresse er det sannsynlig at epostene dine blir sendt via amerikanske servere, og dermed utsettes for pakkesniffing og at du blir eksponert for reklame basert på innholdet i epostene dine. Det ser også ut som at pakkesniffing ble brukt i forbindelse med de amerikanske (NSA) og britiske (GCHQ) etterretningstjenestenes masseovervåkningsprogram som ble avslørt sommeren 2013.

Hvordan pakkesniffing kan oppdages, begrenses, eller kontrolleres, er uklart. Teknologien utvikles så raskt at det er vanskelig å lage regelverk som holder følge. Det er også vanskelig å vite omfanget av pakkesniffing. Enhver melding du sender på nett kan reise jorda rundt før den kommer fram til adressaten, og kan dermed ha vært gjenstand for pakkesniffing hos hvilken som helst internettleverandør eller sikkerhetstjeneste. Det er nærmest umulig å avgjøre om det har funnet sted eller ikke. Pakkesniffing genererer informasjon som kan deles mellom internettleverandører og sikkerhetstjenester fra forskjellige land. Uten regulering kan det bli «ville-vesten»-tilstander, der styresmakter, sikkerhetstjenester og private selskap utnytter gråsoner i regelverket.

Det vi kan fastslå, er at svært mange forskjellige institusjoner og selskap benytter seg av pakkesniffing, deriblant nettleverandører, markedsføringsselskap, politiet og sikkerhetsmyndigheter. Bortsett fra den omfattende overvåkingen som ble avslørt i USA i 2013, er det kun rapportert om en håndfull saker hvor pakkesniffing har blitt brukt. Dette inkluderer både kommersiell og sikkerhetsorientert bruk.

6.2.1 Kommersiell bruk

- **Nettverkssikkerhet:** Meldinger inspiseres for å være sikker på at de ikke inneholder virus, ondsinnet programvare eller feil.
- **Målrettet markedsføring:** Innsamlet informasjon blir brukt for å kartlegge avsenderens produktpreferanser. Dette er ulovlig i Europa, men ønskes velkommen av enkelte forbrukere i USA. Det vektlegges at målrettet markedsføring gir forbrukerne enklere tilgang til produkter og tjenester som er tilpasset deres behov.
- **Beskyttelse av opphavsrett:** Meldinger blir inspisert for å identifisere ulovlig fildeling og brudd på opphavsretten.

Pakkesniffing-debatten i Storbritannia: Phorm og forbrukerinformasjon

I 2008 forsøkte det amerikanske selskapet Phorm å lansere et system i Storbritannia som, sammen med britiske teleoperatører, skulle benytte seg av pakkesniffing for å kartlegge britiske forbrukeres produktpreferanser. Deretter skulle denne informasjonen selges videre til markedsføringsselskap.

Teleselskapene fortalte kundene sine at hensikten med pakkesniffing var å bekjempe kriminalitet på nett og unnløt å fortelle at de også planla å bruke det til markedsføring. Da de i hemmelighet testet systemet, fanget en av leverandørene opp over 18 millioner meldinger. Etter hvert som dette ble kjent blant britiske forbrukere, ble det igangsatt protestaksjoner fordi de ikke hadde gitt sitt samtykke til den egentlige hensikten bak pakkesniffingen. Phorm-teknologien ble til slutt forkastet av alle nettleverandører, og EU-kommisjonen gikk til rettslige skritt mot den britiske regjeringen for å ha tillatt iverksettelsen av Phorm-programmet.

Saken ble avsluttet i januar 2012 etter at Storbritannia gjorde det straffbart å overvåke kommunikasjon ulovlig.

6.2.2 Pakkesniffing og sikkerhet

Overvåkning av kriminell aktivitet:

Pakkesniffing har blitt foreslått som verktøy i etterforskning av visse typer forbrytelser, men dette er veldig kontroversielt (og kan være ulovlig). Eksempler på tilfeller der pakkesniffing kan benyttes inkluderer etterforskning av:

- angrep mot datasystemer eller der datamaskiner blir brukt for å utføre kriminelle handlinger (for eksempel spredning av barnepornografi)
- rasistiske trusler og ytringer
- oppfordringer til terror eller terrorplanlegging
- ytringer som støtter folkemord eller forbrytelser mot menneskeheten

Sensur: Det blir spekulert i om pakkesniffing har blitt brukt for å villedde opposisjonen i regimer over hele verden. Et amerikansk forsvarsselskap, NARUS (en underleverandør av Boeing), solgte teknologi for pakkesniffing til Libya som deretter ble brukt til å slå ned på opposisjonelle under den arabiske våren. Storbritannia derimot, trakk tilbake eksportlisenser for pakkesniffing til Egypt, Bahrain og Libya. Iran bruker pakkesniffing for å overvåke og sensurere internett, men også for å forandre på innhold på nett eller i eposter. Kina bruker pakkesniffing på samme måte. Hvorvidt slik sensur også foregår i Europa, vet vi fortsatt ikke.

6.3 Økt sikkerhet

Pakkesniffing kan bedre sikkerhet ved å identifisere og blokkere skadelig og ulovlige meldinger, slik som det ble beskrevet i avsnittet over.

Pakkesniffing kan ikke forhindre kriminalitet, det kan kun oppdage at noe ulovlig skjer og eventuelt bidra med bevismateriale i rettsaker. Derimot kan pakkesniffing stoppe spredning av virus og annen ondsinnet programvare.

6.4 Utfordringer

Bruk av pakkesniffing reiser flere utfordringer:

1. Pakkesniffing fanger opp all kommunikasjon

- Pakkesniffing analyserer alle meldinger og all data de inneholder, noe som innebærer at elektronisk kommunikasjon aldri er garantert privat.
- Vissheten om at all kommunikasjon kan overvåkes, kan medføre omfattende «chilling effekt», som innebærer at folk blir redde for å kommunisere og uttrykke seg fritt.
- Pakkesniffing er svært inngripende, og det er behov for streng regulering av bruken.

2. Teknologien utvikler seg langt raskere enn regelverket

- Det foreligger ikke tydelige regler om hva pakkesniffing kan og ikke kan brukes til.
- Bruken av pakkesniffing avhenger i dag av brukerens egne etiske vurderinger. Det kan brukes til alt fra identifisering av virus til politisk undertrykkelse.
- I stater der det er tette forbindelser mellom myndighetene og teleselskap, kan informasjon enkelt deles slik at staten får tilgang til samtlige innbyggers elektroniske kommunikasjon.

3. Det er vanskelig å kartlegge nøyaktig hvem som benytter seg av pakkesniffing, og hvorfor de gjør det.

- Fremtidig regulering av pakkesniffing bør være internasjonal
- Et tilsyn for pakkesniffing bør være et internasjonalt organ som har myndighet til å straffeforfølge de som bryter reglene.

Mange selskap som bruker pakkesniffing befinner seg ikke i Europa, men analyserer likevel data om europeiske innbyggere. Så lenge selskapene ligger utenfor Europas grenser, kan ikke europeisk myndigheter pålegge dem å stanse bruken av pakkesniffing.



Eva Schlehahn, Datatilsynet i Schleswig Holstein, Tyskland

7 Lokalisering av smarttelefoner

Da Aisha brukte smarttelefonen sin på flyplassen, la hun merke til at beliggenheten som ble angitt på mobilen hadde blitt endret til der hun befant seg. Hun visste at det sikkert var en enkel forklaring bak dette, og det hadde hun rett i. Alle typer mobiltelefoner må kunne registrere hvor de befinner seg for at de skal fungere. Smarttelefoner har tatt dette til et helt nytt nivå.

Smarttelefonen har overtatt plassen til den sveitsiske lommekniven som det perfekte «alt-i-ett»-verktøyet. I Europa er det gjennomsnittlig 1,3 mobiltelefoner per innbygger, noe som er enormt mange når mobiltelefoner slik vi kjenner dem i dag ikke var i salg før 1990-tallet.

7.1 Hvorfor ble lokalisering av smarttelefoner utviklet?

Smarttelefoner er et relativt nytt produkt. De er veldig populære fordi de kan utføre svært mange oppgaver. På mange måter er de mer som små datamaskiner som også fungerer som telefoner.

Som en vanlig datamaskin har hver smarttelefon et operativsystem som tilrettelegger for bruken av e-post, chat og surfing på nett. De kjører programvare som kan tilby tjenester som spill, kart og nettaviser. De har også digitalkamera, medieavspillere og store, fargerike berøringsskjermer.



Mobiltelefonens historie går tilbake til andre verdenskrig. En mobiltelefon er først og fremst en trådløs radio som kan både sende og motta meldinger. Den første trådløse radioen, «walkie-talkie», ble først brukt for å hjelpe soldater å holde kontakten med hverandre på fronten. På 70- og 80-tallet muliggjorde utviklingen av mikroprosessorer de første håndholdte mobiltelefonene. Den første modellen var like stor og veide like mye som en murstein. Batteriet varte kun i 20 minutter. Tidene forandrer seg, og fra og med 80-tallet forbedret et stadig voksende mobilmast-nettverk både lokale og internasjonale telefonsignaler.

Mobilmaster er svært viktige for å lokalisere mobiltelefoner. En mast dekker et gitt geografisk område. For å kunne være tilknyttet et nettverk, må mobiltelefonen kobles til nærmeste mast. Dersom personen som bærer på telefonen forflytter seg inn i rekkevidden til en annen mast, vil telefonen tilkobles denne masten i stedet. På denne måten kan teleselskap lokalisere en person. Lovgivningen i EU krever at teleselskapene lagrer denne informasjon i minst seks måneder, og maksimalt 24 måneder.

Smarttelefoner kan også lokaliseres på andre måter, for eksempel ved å bruke GPS-funksjonen på telefonen, eller ved å koble seg til trådløse nettverk. Dette har ført til en enorm utvikling av tjenester som bruker posisjonsdata. Disse er vanligvis tilgjengelige som applikasjoner («apper»)

som kan installeres på telefonen. En app er en programvare som utfører gitte funksjoner eller tjenester. Posisjonsbaserte apper kan gjøre det enklere for en bruker å finne informasjon om nærliggende restauranter og butikker, eller til og med finne ut om venner befinner seg i nærheten. Det finnes også spill som

bruker disse funksjonene. Tjenester basert på posisjonen til brukeren er trolig et marked som vil fortsett å vokse de neste årene.

Hvordan lokalisering av smarttelefoner fungerer



Både vanlige mobiltelefoner og smarttelefoner kan spores. Det finnes tre forskjellige måter å spore mobiltelefoner på: via mobilmaster, GPS og trådløse nettverk. Alle mobiltelefoner kan spores via mobilmaster, mens de to siste metodene gjelder kun for smarttelefoner.

Mobilmaster: alle telefoner registreres ved den nærmeste mobilmasten slik at anrop, tekstmeldinger og e-poster kan sendes og mottas via mobilnettet. Hver telefon bærer på et unikt referansenummer som knytter telefonen til en konto hos teleselskapet, og derfor også til brukeren. Dette

gjør det mulig å tilpasse forskjellige løsninger og sende regninger til hver enkelt bruker. Hvis myndighetene eller sikkerhetstjenester forsøker å spore opp personer, kan de be teleselskapene å avgi denne type informasjon. Ved å samle informasjon om én telefon fra flere forskjellige master, vil brukeren være mulig å spore.

GPS: Smarttelefoner inneholder kart-programvare og applikasjoner som må være tilkoblet GPS for å fungere. Når funksjonaliteten for GPS er slått på, vil posisjonen beregnes ut fra avstanden til nærmeste GPS-satellitt. Telefonen kan ikke kobles til GPS-satellitten dersom denne funksjonen er avslått. Imidlertid finnes det applikasjoner som fjernstyrer denne funksjonen uten å informere brukere. Dette kan for eksempel være apper som kan lokalisere en stjålet telefon. Produsenter av applikasjoner innhenter posisjonsdata fra telefonene, og noen selger dem videre til markedsføringsselskap. Dersom myndigheter og sikkerhetstjenester ønsker å spore noen, kan de be teleselskap om GPS-data.

Trådløst nettverk: Smarttelefoner kan kobles til trådløse nettverk som virker innenfor et gitt område. Å koble telefonen til et slikt nettverk gjør det mulig å lokalisere den innenfor nettverkets rekkevidde. Dersom funksjonen slås av, er det ikke mulig å spore telefonen på denne måten. Et trådløst nettverk vil vanligvis ha en rekkevidde på 20 meter innendørs, og noe større rekkevidde utendørs.

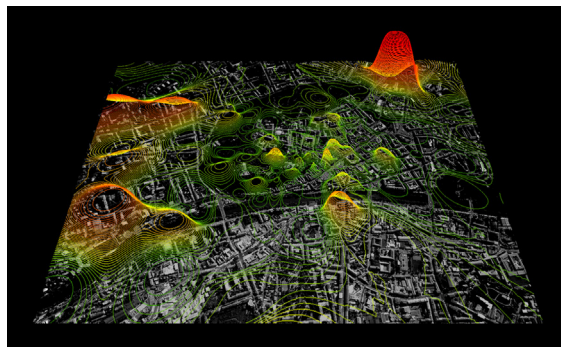
Andre "smarte" mobile enheter, som nettbrett og bærbar datamaskiner kan spores på samme måte.

Posisjonsbaserte tjenester tilbyr mange praktiske funksjoner. For noen personvernforkjempere er det likevel bekymringsverdig at det kan innhentes så mye informasjon om hvor en person befinner seg. Da den tyske politikeren Malte Spitz fra De grønne forsøkte å få tak i data som mobilselskapet hadde om ham, måtte det en rettsak til før selskapet utleverte dokumentene. Ved første øyekast var det ikke mer en lang og meningsløs strøm av tall. Men etter at en statistiker fikk sett på tallene, innså Spitz at tallene kunne gi en svært detaljert oversikt over livet hans. SMalte ble spesielt bekymret for hvor detaljert informasjon man kunne få ved å sammenstille posisjonsdataene fra telefonen med informasjon fra sosiale medier som Twitter og Facebook.

Den amerikanske høyesteretten konkluderte nylig at GPS-data kan gi svært detaljert informasjon om private ærend, som for eksempel «turer til psykologen, til en plastisk kirurg, en abortklinikk, til et AIDS-senter, en strippeklubb, forsvarsadvokaten [...], fagforeningen, synagogen, moskéen eller kirken, homobaren osv».

Twitter, AngryBirds eller CandyCrush, samler inn posisjonsdata og informasjon om kontaktlisten på telefoner for så å selge dem til markedsføringselskap. Markedsførerne bruker deretter informasjon til å skreddersy reklame som er tilpasset vanene og interessene til forskjellige typer kundegrupper. Over 50 prosent av alle apper samler inn posisjonsdata selv om de ikke trenger det for å fungere.

Byplanlegging: Posisjonsdata kan benyttes for å kartlegge bruken av byrom. Siden det er flere mobilmaster i byer enn på landet, er det også enklere å spore telefoner i byer. Dette litt merkelige bildet er et kart over hvordan mobiltelefoner brukes i Graz i Østerrike. Forskere ved Massachusetts Institute of Technology sporet opp mobiltelefoner anonymt for å kunne tegne et bilde av hvordan innbyggerne forflytter seg. Hensikten er å gi bedre bakgrunnsinformasjon til byplanleggere og transportmyndigheter om hvordan byen benyttes.



7.2 Hva brukes lokalisering av smarttelefoner til?

Det er både kommersielle og sikkerhetsmessige bruksområder for posisjonsdata fra smarttelefoner.

7.2.1 Kommersiell bruk

Telefonregninger: Teleselskap trenger posisjonsdata og telefonens identifikasjonsnummer for å kunne fakturere kundene sine.

Målettet markedsføring: IT-utviklere som produserer applikasjoner som

7.2.2 Lokalisering og sikkerhet

- **Finne savnede og skadede personer:**
I USA og Canada har nødnummer-tjenesten E-911 fullmakt til å benytte seg av GPS i mobiltelefoner, slik at brukerne skal kunne lokaliseres i nødsituasjoner. Omkring 60 til 70 prosent av de 180 millioner telefonsamtalene som gjøres i Europa hver dag, blir gjort fra mobiltelefoner. Telefonene avgir posisjonsdata til den det felles europeiske nødnummeret 112. I motsetning til amerikanerne og canadierne, må ikke europeerne ha GPS-tjenestene påslått til enhver tid.
- **Oppsporing av mistenkte**
forbrytere: Teleselskap må gi politi og sikkerhetstjenester tilgang til posisjonsdata etter rettskjennelse. I Europa blir denne type forespørsler vurdert ut fra personvernlovgivning. Når teleselskap først mottar en slik kjennelse, er de pålagt å levere all data som kan knyttes til den mistenkte. Sikkerhetstjenester har også andre metoder for å spore opp mistenktes mobiltelefoner.
- **Sporing av familiemedlemmer:**
Enkeltpersoner kan også ha nytte av posisjonsdata. Dette kan for eksempel være foreldre som ønsker å vite hvor barna deres befinner seg.

Debattene om bruken av posisjonsdata og smarttelefoner

Under "Occupy Wall Street"-protestene i New York ble selskapet Twitter pålagt å avgi posisjonsdata til amerikanske myndigheter for å identifisere demonstrantene. Nylig lanserte Twitter en ny tjeneste, «Please Don't Stalk Me». Tjenesten brukes til å knytte feilaktig posisjonsdata til meldinger. Brukerne velger selv ut hvor de ønsker å gi inntrykk av å befinne seg via kartene til Google Maps. Det finnes også andre apper som tilbyr lignende tjenester, som «My Fake Location», «Fake GPS Location» og «GPS Cheat».

7.3 Økt sikkerhet

Lokalisering av smarttelefoner bidrar til økt sikkerhet på flere måter:

1. De som befinner seg i nødsituasjoner er enklere å spore opp og kan dermed få hjelp raskere
2. Familier kan enklere vite hvor sårbare eller pleietrengende slektninger befinner seg
3. Myndighetene kan bruke posisjonsdata for å knytte mistenkte til en forbrytelse, eller tvert i mot å utelukke dem fra etterforskningen.

7.4 utfordringer

Lokalisering av smarttelefoner skaper utfordringer knyttet til personvern, reguleringer og menneskerettigheter:

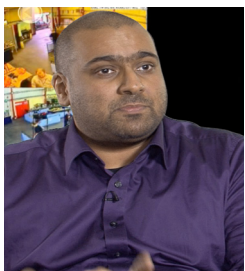
1. Brukere har ikke kontroll over informasjonen som produseres og videreføres av smarttelefoner. Dette kan skape vansker for personer i utsatte situasjoner, for eksempel vitner, som ikke ønsker å dele sin posisjon, men likevel vil beholde fordelene ved mobilbruk. Noen telefoner, deriblant Apples iPhone, lagrer posisjonsdata automatisk uten at denne funksjonen kan slås av.
2. Noen apper lagrer posisjonsdata uten at dette er nødvendig for at appen skal fungere. Uten press fra forbrukerne er det lite sannsynlig at selskapene vil gi brukerne bedre kontroll over sine posisjonsdata.

3. Mange app-utviklere befinner seg utenfor Europa og er derfor ikke underlagt europeisk personvernlovgivning. Det er derfor vanskelig for EU å kreve at apper skal være mer personvernvennlige. En endring av ePrivacy-direktivet understreker imidlertid at brukere må ha muligheten til å gi sitt samtykke til at apper behandler data fra telefonen, uansett hvor i verden utviklere befinner seg.

4. I stater der det er et tett forhold mellom teleselskap og myndighetene kan informasjon deles slik at staten får oversikt over posisjonsdata til samtlige innbyggere.

5. Siden lokasjonsdata har blitt brukt for å identifisere demonstranter, kan systematisk bruk føre til at folk ikke lenger ønsker å demonstrere eller utøve sine demokratiske rettigheter.

Lokalisering av smarttelefoner vil både skape muligheter og overvåke oss.



Posisjonsdata legger til rette for tjenester som gjør det lettere å være sosial. Samtidig er innstillingene for lagring av posisjonen din og bruk av disse dataene ikke nødvendigvis brukervennlige eller enkle å endre.

Gus Hosein, Privacy International

8 Er teknologi den eneste løsningen?

Du lurer kanskje på om sikkerhetsteknologi er den eneste løsningen. Til tider kan det virke som om sikkerhet handler kun om sporing og identifisering av mistenkte. Dette stemmer i en viss forstand, men viser ikke hele bildet.

EUs sikkerhetsprioriteringer, som vi så på tidligere, viser at sikkerhet er relevant på mange ulike samfunnsområder, og de omhandler ofte de «klassiske» sikkerhetsutfordringene kriminalitet og terrorisme. De forrige kapitlene i dette heftet viser at det er mulig å bruke sikkerhetsteknologi for å finne og spore opp de som driver med slike aktiviteter. Men det er mange underliggende årsaker som fører til at slike sikkerhetsutfordringer oppstår, som for eksempel fattigdom, nasjonale eller internasjonale konflikter eller politiske og religiøse forskjeller. Sikkerhetsteknologi kan ikke brukes for å løse disse problemene.

Typiske sikkerhetsutfordringer for EU kan også være mat- og vannmangel, finanskriser, epidemier eller naturkatastrofer. Der kan sikkerhetsteknologi heller ikke bidra til en løsning.

Selv om sikkerhetsteknologi kan brukes for å finne kriminelle og terrorister, og til og med få informasjon om hva de har tenkt å gjøre, finnes det altså andre løsninger. Kanskje har du også egne tanker om hvordan man kan jobbe for å bedre sikkerheten? Eller synes du at Europas sikkerhetsfokus burde flyttes vekk fra terror til andre områder?

8.1 Lokale løsninger

- Fremme et tryggere miljø gjennom oppgradering av gatebelysning, nødtelefoner og mer synlig politi.
- Knytte kontakter og bedre forholdene mellom lokalsamfunn og politi gjennom kriminalitetsforebyggende tiltak.
- La trossamfunn eller andre grupper løse konflikter lokalt for å øke den sosiale tilliten.
- Sørge for at politiet er åpne om arbeidsmetodene sine, og at de blir holdt ansvarlig hvis de går for langt.
- Skape jobbmuligheter, tilby opplæring og veiledning for folk i miljøer med mye kriminalitet.

8.2 Nasjonale og internasjonale løsninger

- Fremme et mer rettferdig globalt handelssystem, bistand og gjeldssletting
- Øke ressursene til katastrofeberedskap
- Utbedre infrastruktur og tilgang til vann, kommunikasjon og informasjon i de delene av verden der dette er nødvendig
- Bruke bærekraftige og alternative energikilder mer effektivt.
- Løse problemer knyttet til ulikhet og diskriminering.

9 Tilbake til deg...

Du har nå fått presentert de tre sikkerhetsteknologiene som skal diskuteres på folketoppmøtene i SurPRISE-prosjektet. På det norske folketoppmøtet skal vi konsentrere oss om to av dem: pakkesniffing og lokalisering av smarttelefoner. Vi har forklart hvordan de fungerer, hvordan de brukes, hvordan de bidrar til økt sikkerhet og hvilke utfordringer de medfører. Vi har også beskrevet i hvilken kontekst teknologiene har utviklet seg: i et Europa som er svært bekymret for sikkerhet og der sikkerhet blir en del av hverdagen. Personvern og overvåkning er også viktige tema, blant annet på grunn av mengden persondata som i dag benyttes i sikkerhetsøyemed. Avslutningsvis så vi på ikke-teknologiske tilnærminger for å øke sikkerheten i et samfunn.

Det er nå opp til deg å gjøre deg opp en mening om disse spørsmålene. Ville det vært akseptabelt om disse teknologiene ble benyttet rutinemessig? Kanskje tenker du at sikkerhetsteknologi utgjør et effektivt virkemiddel for å bekjempe kriminalitet? Eller at ikke-teknologiske løsninger er mer effektive? Er det bedre å bruke tradisjonelle etterforskningsmetoder enn ny overvåkningsbasert teknologi? Eller kanskje du synes sikkerhetsutfordringene er overdrevet og at vi ikke trenger å bekymre oss?

Noen mener at slik teknologi er i trygge hender fordi de brukes av offentlige etater og

myndigheter som må stå til ansvar for sine beslutninger og handlinger. Andre tviler på at disse myndighetene er i stand til å bruke slik teknologi på en kompetent og etisk måte, med befolkningens beste i tankene.

Kanskje synes du ikke at slik teknologi angår eller påvirker deg personlig: de er tross alt utviklet og rettet mot kriminelle og blir utplassert i områder der du vanligvis ikke ferdes. Likevel kan det hende at alle bør bekymre seg over mengden persondata som disse teknologiene behandler, og fordi de gjør alle og enhver til mistenkte. Du er kanskje tilfreds med hvordan sikkerhetsteknologi brukes i dag, men bekymret for hvordan de kan brukes i fremtiden.

Å frasi seg deler av personvernet i bytte mot økt sikkerhet er uansett ingen enkel avveining. SurPRISE ønsker å forstå bredden av folks holdninger til ny sikkerhetsteknologi.

Vi ser fram til å møte deg på folketoppmøtet om noen uker. Dersom du vil vite mer om SurPRISE-prosjektet og dets partnere kan du besøke SurPRISE-nettsiden på <http://surprise-project.eu>.

Om informasjonsheftet

Dette heftet er produsert for å gi informasjon til SurPRISE-folketoppmøtets deltakere. Heftet er distribuert til samtlige partnere i SurPRISE-samarbeidet av det Østerrikske Vitenskapsakademiets Institutt for Teknologivurdering (Strohgasse 45/5, A-1030 Wien).

Les mer om prosjektet og partnerne på nettsiden <http://surprise-project.eu/>.

Informasjonen som fremgår heftet er skrevet av SurPRISE-partnerne, basert på forskning og rapporter skrevet av politikere, forskere og teknologer fra hele verden.

Forfatter: Dr Kirstie Ball, The Open University

Scientific Advisory Board: Dr Monica Areñas, Professor Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Mr Jean Marc Suchier, Ms Nina Tranø

Layout: Mr Peter Devine, Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University

Grafikk/Bilder: Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University. Page 17 © iStockPhoto.com / EdStock, page 28 © iStockPhoto.com / dpmike, page 29 © iStockPhoto.com / alexsl, page 30 Senseable City Lab, Massachusetts Institute of Technology.

SurPRISE sponsorer: European Commission Framework 7 Programme, project no. 285492

Dokumentet er tilgjengelig på <http://surprise-project.eu>

Informasjonsheftet er forfattet av Kirstie Ball i tett samarbeid med det danske Teknologirådet, SurPRISE-partnerne og dets rådgivende gruppe (Advisory board). Heftet ble gjennomgått fire ganger internt, og én gang eksternt. En tidlig versjon ble testet på grupper i Danmark, Ungarn og Storbritannia.

Partnere i prosjektet

- > Institut für Technikfolgen-Abschätzung/Österreichische Akademie der Wissenschaften, Coordinator, Austria (ITA/OEAW)
- > Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
- > Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)
- > Teknologirådet - The Danish Board of Technology Foundation, Denmark (DBT)
- > European University Institute, Italy (EUI)
- > Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- > Medián Opinion and Market Research Limited Company, Hungary (Median)
- > Teknologirådet - The Norwegian Board of Technology, Norway (NBT)
- > The Open University, United Kingdom (OU)
- > TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- > Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.



