

Udkast til casesamling om privacy

Version 1.0

Indholdsfortegnelse

Hvad er privacy? (Henning Mortensen)

Hvilken beskyttelse giver loven? (Henning Mortensen)

Hvad gør jeg ved brud på min privacy? (Henning Mortensen)

Hvornår krænkes privacy? (Henning Mortensen)

Casesamling

- TV-overvågning (Stephan Engberg)
- Logning af internetanvendelse (Henning Mortensen, Mikael Hertig)
- Biometri (Stephan Engberg)
- TV-kanalovervågning (Stephan Engberg)
- Google det store dyr i åbenbaringen eller "Big Brother"? (Bjørn Standhart)
- E-handel (Leif Limkilde Bloch, Mikael Hertig, Henrik Biering)
- Man kan ikke trække sine tidligere udtalelser på internettet tilbage (Niels Christian Juul, Niels Madelung, Henrik Biering)
- Demokratiske elektroniske valg (Stephan Engberg)
- Usikker IT-sikkerhed (Preben Andersen, Henrik Biering, Christian Wernberg-Tougaard, Niels Madelung)
- Offentlig forvaltning (Mikael Hertig)
 - CASES vedr. offentlig forvaltning: Quick skranken (Per Henriksen)
 - CASES vedr. offentlig forvaltning: Bibliotekslån (Mikael Hertig)
 - CASES vedr. offentlig forvaltning: Elektronisk Patient Journal (Stephan Engberg)

Indledende bemærkninger

Denne casesamling er udarbejdet til Videnskabsministeriets møderække om privacy af møderækkens arbejdsgruppe om awareness. Det er et af flere produkter fra arbejdsgruppen.

Det skal bemærkes, at de enkelte cases er modtaget og enten uden eller også med en meget begrænset korrektur og vurdering fra "redaktøren" sat ind i dette dokument. Der er ikke foretaget kontrol af, om casen er koordineret indenfor arbejdsgruppen. De enkelte cases detaljeringsniveau er også ganske forskelligt, ligesom de ikke alle følger den vedtagne struktur. Da ikke alle cases var tilvejebragt på det sidste møde i gruppen, er gruppen ikke nået til konsensus om alle cases. Desuden er ikke alle de cases, det er ønskeligt nævnt. Gruppen vil gennem videre arbejde kunne tilvejebringe flere af disse cases ligesom gruppen med mere tid ville kunne konsolidere disse. Case samlingen må på denne baggrund betragtes som en oversigt over emner relateret til privacy, som gruppen anbefaler, at ITST formidler viden til borgerne omkring. Arbejdsgruppen opfordrer til, at der generelt nedsættes en arbejdsgruppe med sekretariatsbistand, som kan arbejde videre med sådanne cases.

På arbejdsgruppens vegne

14. juni 2007

Henning Mortensen

ITEK / Dansk Industri

Hvad er privacy?

Privacy er et begreb, som det er vanskeligt at definere. Ordet er blevet forsøgt defineret i mange forskellige sammenhænge. Dette viser begrebets brede betydning. I en dansk oversættelse ville privacy komme tæt på det, vi forstår ved privatlivets fred.

Internationalt sondres der ofte mellem fire typer privacy¹, som samtidig viser, hvilke forhold privacy er relevant for:

- Informationsprivacy, som vedrører indsamlingen og behandlingen af personlig information - også kaldet databeskyttelse
- Kropslig privacy, som vedrører retten til at beskytte sin fysiske krop mod f.eks. genetiske tests
- Kommunikationsprivacy, som vedrører sikkerhed og privacy i forhold til breve, mail, telefonopkald, internetanvendelse og lignende
- Territorial privacy, som vedrører grænsedragningen mellem det private miljø og andre miljøer f.eks. på arbejdspladsen og i det offentlige rum - herunder f.eks. videoovervågning og ID tjek. Det vedører også grænsedragningen mellem nationalstater og den forskellige lovgivning, som disse er underlagt.

Intuitivt vedrører privacy den risiko² man udsætter sig for ved frivilligt eller ufrivilligt at lade andre mennesker få adgang til informationer om en selv. Risikoen vedrører den reelle mulighed, at dem, der får adgang til informationer, misbruger dem. Risikoen vedrører graden af kontrol med hvem der kan indsamle, vedligeholde, anvende, videregive/transmittere og behandle personlig information³. Risikoen vedrører også, at der stjæles informationer, som kan misbruges til, at man giver sig ud for at være en anden, end den man er.

Der er også mere følelsesmæssige aspekter tilknyttet privacy. Man kan f.eks. føle, at man mister kontrol med sin personlige integritet, hvis andre har adgang til noget man gerne vil holde for sig selv. Man kan også føle sig pinligt berørt, føle sig udstillet eller føle sig uretfærdigt behandlet.

Forskellige standarder for evaluering af computerprogrammer beskæftiger sig med privacy, netop for at sikre at programmerne i et vist omfang opfylder privacy. I Common Criteria, som er en standard til at vurdere om et stykke software opfylder en række sikkerhedskrav, hedder det: Privacy "requirements provide a user protection against discovery and misuse of identity by other users"⁴.

Hvis privacy ikke er til stede eller opfattes som ikke værende til stede, viser undersøgelser, at man ændrer adfærd og ikke tør "være sig selv". Man får en følelse af at miste sin autonomi og individualitet. Man bliver måske tilbageholdende med politiske og religiøse tilkendegivelser, økonomiske transaktioner, hjælp til håndtering af sygdomme og seksualitet samt påklædning og generelt det at konstruere sig selv.

1 Privacy & Human Rights, udgivet af EPIC, 2003, p. 3. EPIC står for Electronic Privacy Information Center, og er formodentlig USA's mest indflydelsesrige privacyorganisation.

2 <http://www.demos.co.uk/catalogue/thefutureofprivacyvolume1>.

3 <http://www.epic.org/reports/dmfprivacy.html>.

4 Common Criteria er en ISO-standard ved navn: ISO/IEC 15408:2005, og den kan i sin fulde længde findes på <http://www.commoncriteriaportal.org>. Privacy-kravene fremføres i standardens 2. del: "Security functional requirements", <http://www.commoncriteriaportal.org/public/files/ccpart2v2.3.pdf>.

Hvilken beskyttelse giver loven?

Borgernes rettigheder efter persondataloven er beskrevet her:

<http://www.it-borger.dk/lov-og-ret/kedebreve/dine-rettigheder-ifm-registrering-af-oplysninger>

Hvad gør jeg ved brud på min privacy?

Der findes en vejledning til at foretage en anmeldelse af mistanken om et lovbrud her:

<http://www.datatilsynet.dk/anmeld/index.html>

Hvornår krænkes privacy?

Der er to forskellige niveauer i forhold til en eventuel krænkelse af privacy:

- Den ene type mulig krænkelse vedrører, om man frivilligt eller ufrivilligt bliver bedt om at afgive data. I en række tilfælde har man ikke noget imod at aflevere data. I andre tilfælde føler man måske, at nogen har overskredet den individuelle tærskel for, hvad man godt ville bevare som en hemmelighed. Der er altså tale om frivillighed versus ufrivillighed.
- Den anden type mulig krænkelse vedrører om afgivelsen af data er lovlig eller ulovlig i betydning i strid med Lov om behandling af personoplysninger.

Der bliver dermed fire scenarier for mulige krænkelse:

	Frivillig	Ufrivillig
Lovlig	I dette scenarium er der ikke tale om en krænkelse	I dette scenarium, er der tale om en indsamling af data, som man føler overskrider personlige grænser, men der er ikke tale om en decideret lovovertrædelse.
Ulovlig	I dette scenarium er der tale om en ulovlig indsamling af data, som den data vedrører, ikke selv føler nogle problemer ved at afgive. Typisk er lovninngen sat for at beskytte folk - uanset om de føler et behov herfor eller ej.	I dette scenarium er indsamlingen af data ulovlig og samtidig vil den data vedrører føle sig krænket ved at skulle afgive dem.

Under alle omstændigheder er det væsentlige, at man vurderer, hvilken risiko der er for, at den man afgiver oplysningerne til, misbruger dem f.eks. til et andet formål end de er afgivet eller til at eksponere dem for offentligheden. Den risiko, man vurderer at udsætte sig selv for, vil typisk hænge sammen med ens følelser for graden af fortrolighed, der ligger i de data man bliver bedt om at afgive.

I en række tilfælde kan man være nødt til at afgive data, man betragter som fortrolige til et system, hvis dette er indrettet på en sådan måde, at det kun virker, hvis data afgives. En række systemer kan også være indrettet til automatisk at kræve dit

samtykke til at data må bruges til en række forskellige ting. Dette samtykke kan eventuelt være ulovligt.

Hvis man mener, at der er tale om en lovovertrædelse, kan man anmelde sagen til Datatilsynet, som beskrevet ovenfor. Datatilsynet vil så vurdere, om der er tale om en overtrædelse af loven.

Tidshorisonten kan også spille en rolle. Der er typisk tale om forskellige holdninger til data før de afgives, mens de afgives og efter de afgives. Samtidig kan der også være forskellige krav til f.eks. indsamling og lagring af data.

Casesamling

CASE: Videoovervågning

Kameraer har en masse positive brugsmuligheder, herunder ønsker vi alle at gemme gode oplevelser. Men samtidig kan kameraer bruges til at overvåge og kontrollere mennesker.

Videoovervågning som teknologi bliver både nemmere, billigere og stadigt mere fintfølede. At koble et webcam til et TCP/IP netværk er i dag noget, enhver kan gøre.

Samtidig ser vi den traditionelle analoge optagelse kombineret med både automatisk ansigtsgenkendelse og kobling i netværk, så det ikke længere blot er midlertidige billeder (som oftest slettes uden at blive gennemset), men nu er realtidsovervågning der samtidig automatiseres og kobles med databasesystemer. I UK har man i dag overvågningskameraer med tilkøbt højttaler, som giver mennesker besked på at samle affald op.

I medierne hører man ofte udtalelser som at ”jeg har ikke noget at skjule” eller ”overvågning giver tryghed”. I praksis er sammenhængene mere nuancerede og dækker over et utal af voksende problemer. F.eks. er det slående, at i verdens mest tv-overvågede land, UK, er mødrene så bange for at lade deres børn lege ude, at de i praksis ikke får lejlighed til at lege frit. Virkeligheden er altså snarere, at borgerne skræmmes til at acceptere overvågningskameraer, men at de i praksis ikke giver tryghed.

Hvad er problemet

Der er en lang række problemer med videoovervågning og generelt alle former for biometrisk identificerende overvågning.

Umyndiggørelse – Problemet med overvågning er altid, at den overvågede umyndiggøres og udsættes for risici uden for vedkommende kontrol. Problemet er endnu værre, hvis overvågning kobles med biometri (se Biometri). Skiltning med overvågning er ikke tilstrækkeligt, hvis ofret ikke kan værgе sig. Det giver ikke ofret tryghed, at kunne se med på overvågningskameraet i ofrets soveværelse – det synliggør blot ofrets afmægtighed og magtudøvelsen.

Targeting – Overvågning opsamler viden som før eller siden vil blive brugt mod de overvågede – kriminelt, kommercielt, planøkonomisk eller politisk (Big Brother). Det kan ske i realtid via direkte kobling med ansigtsgenkendelse til bagvedliggende it-

systemer. Det kan ske forsinket som når søgedatabaser begynder at bruge ansigtsgenkendelse, så billeder på nettet pludselig ikke bare er billeder, men faktisk bliver til en del af en database.

Adfærd – Menneskers adfærd påvirkes i form af selvcensur på samme måde, som hvis en pistol var rettet mod dem. Men værre fordi pistolen er latent og virker med tilbagevirkende kraft. Opsamlede film, tale og handling kan blive misbrugt uden for kontekst og skaber dermed frygt fordi mennesker involveret ikke kan estimere truslen. Nogen vil overvurdere truslen med en stærkt hæmmende virkning, andre vil undervurdere truslen med efterfølgende misbrug som konsekvens.

Falsk sikkerhed – Overvågning etablerer en falsk sikkerhed for mennesker, fordi det ikke fører til undsætning. Som eksemplet fra UK dokumenterer fører overvågning ikke til en opfattelse af tryghed.

Terrorisme – Hvis mennesker misinformeres til at man kan have tillid til en model, de ikke kan kontrollere, så vil og kan det let misbruges. Det mest oplagte eksempel er et overvågningskamera på et offentligt sted koblet med en bombe som detoneres via ansigtsgenkendelse. Ofret virker selv om detonator og narres af at bomben maskeres som noget myndighederne påstår troværdigt uden det kan sikres.

Hvad kan vi gøre

Håbet om den præventive effekt mod kriminelle handlinger kan ikke overføres til egen tryghed, hvorfor man bør adskille hensynet til at forebygge mod kriminel adfærd (ansvarliggørelse) og ofres sikkerhed (forebyggelse og kontrol primært i form af tilbageførbarhed). Overvågning af uskyldige med henblik på at forebygge kriminalitet bør undgås og erstattes af ikke-invaderende og mere nuancerede midler.

Forbyde Overvågning – Eksisterende lovgivning omkring overvågning skal ikke slækkes, men bør strammes fordi truslen om magtmisbrug vokser med den teknologiske udvikling. Se om Biometri fordi biometrisk overvågning rummer helt specielle problemer.

Social forhandling – Mange nye former for kilder til skjult overvågning fordrer behov for udvikling af bevidst forhandling. F.eks. ved at mobiltelefoner med diktation eller kamera ikke KAN optage uden at alle andre tilstedeværende f.eks. via deres mobiltelefon accepterer at blive gjort til genstand for overvågning. En lidt mildere model er at al social optagelse SKAL kobles med et trådløst signal herom, så ofre selv kan træffe deres forholdsregler.

Sidste udvej – Ved at etablere et FYSISK SYNLIGT skjold foran overvågningskameraet, kan man med ikke-invasive midler (såsom varmesensorer) detektere personer som nærmer sig de aktiver, man ønsker at sikre. Hvis borgeren har digitale værktøjer til at autentikere, så kan overvågningskameraet slås til kun for personer, der nægter at autentikere og dermed udgør en ukendt trussel.

Koble med person aktivering – Ofret (f.eks. en gammel dame) kan udstyres med en trådløs overfaldsalarm som samtidig med at det fysiske skjold glider væk og en vis præventiv effekt aktiveres, så kan det fungere som alarm, der påkalder opmærksomhed og muliggør undsætning. En sådan funktion vil virke selvregulerende, f.eks.

i toge, fordi alarmering uden grund vil henlede opmærksomheden på kilder til utryghed samtidig med at ofrene for unødvendig overvågning gøres opmærksomme og kan tage behørig forbehold i situationen.

CASE: Logning af internetanvendelse

Spor på internettet (Hvornår krænkes privacy?)

Når man er på internettet eller sender mails efterlader man sig en masse elektroniske spor. Det kan f.eks. være informationer om hvilken browser du bruger, hvilket styresystem du bruger, hvilket sprogområde du foretrækker og hvilke filtyper din computer kan anvende. Disse spor kan opsamles i en log over, hvad du foretager dig på nettet.

Et af de mere alvorlige spor du efterlader dig er din computers IP-adresse. IP-adressen er den adresse, som din computer har fået tildelt af din internetudbyder. Den svarer til din fysiske adresse. Hvis du ikke havde en fysisk adresse kunne postbuddet ikke levere post til dig. Og hvis du ikke har en IP-adresse ville f.eks. en webserver ikke vide, hvor den skulle levere en hjemmeside, som du havde bedt om at se. Alle computere på internettet har en IP-adresse, der identificerer dem.

IP-adressen er unik for den computer du sidder ved. Hvis du flytter dig til en anden computer får du en anden IP-adresse. Netop fordi adressen er unik, kan man bruge den til at spore den computer, du sidder ved. Og når du sidder derhjemme, kan man spore adressen til dig og din familie. Derfor siger Datatilsynet, at IP-adressen er personhenførbart.

Dine handlinger (Hvad gør jeg selv galt?)

Når du er på nettet viser du automatisk og som standard din IP-adresse. IP-adressen kan som nævnt bruges til det formål at finde ud af, hvor informationer skal sendes hen. Men IP-adressen kan også bruges til det formål at finde ud af, hvem der foretager sig hvad på nettet.

Ifølge en bekendtgørelse fra 2007 (logningsbekendtgørelsen) skal din internetudbyder lave et register over, hvem der besøger hvilke hjemmesider, og hvem der sender mails til hinanden. Oplysningerne skal efter en domstols afprøvelse stilles til rådighed for politiet. Det vil sige, at alt, hvad du foretager dig på nettet, kan politiet få adgang til, hvis de har mistanke om, at der foregår noget kriminelt fra din computer.

Registrering af din IP-adresse kan også finde sted, hvis forskellige virksomheder, du besøger på nettet, har en kommerciel interesse heri. Dette er ulovligt i Danmark (med mindre der eksplicit er et formål med det), men det finder helt sikkert sted alligevel.

Logning kan i en række sammenhænge have yderst saglige formål. Vigtigst er det, at man kan bruge logning til at få overblik over, hvem der gør hvad. Dette kan være relevant, fordi man på den måde kan undgå angreb på sine it-systemer. Man kan også drage folk til ansvar for deres handlinger.

Hvordan beskytter jeg mig selv?

Hvis du vil undgå, at der er nogen, som systematisk kan følge med i, hvad du foretager dig på nettet, er det nødvendigt at skjule din IP-adresse. Du kan imidlertid ikke skjule den for alle, da den som nævnt skal bruges til at modtage informationer. Hvad du kan gøre, er at sikre dig, at man ikke kan se, hvem du reelt kommunikerer med.

Det kan gøres ved at du kobler din computer, med din egen IP-adresse op til en anden computer, med en anden IP-adresse og beder denne anden computer om at kontakte den tredje computer, som du i virkeligheden gerne vil kommunikere med. På den måde kan man kun se, at du kommunikerer med den anden computer, men ikke at du reelt kommunikerer med den tredje computer.

I praksis kan dette gøres på flere måder: ved at bruge en åben proxy, ved at bruge en anonymiseringstjeneste eller ved at bruge TOR-netværket. TOR-netværket er det, der er lettest at bruge, så det er den anbefaling, vi vil give her.

I praksis skal du gøre følgende:

- hente og installere den nyeste version af programmet TOR fra <http://tor.eff.org/>.
- programmet bruges ved at der kommer en knap i din browser, så du kan slå anonym surfen til og fra.
- du skal være opmærksom på at du kun beskytter oplysningerne om din IP-adresse ved samtidig at være varsom med hvad du ellers foretager dig på nettet - f.eks. bør du ikke have nogle plugins.
- i praksis kan det anbefales at have to browsere, en, som bruges til almindelig lyd, hvor man har behov for at se billeder, film, osv, og så en, hvor man kan have al multimediefunktionalitet slået fra og TOR-netværket slået til.

I øvrigt henvises der til særskilt vejledning om internetanvendelse.

CASE: Biometri

Biometri dækker over teknologier, som inddrager elementer af fysisk individuelle forskelle såsom fingeraftryk, iris, stemmer, DNA og mere adfærdsbaserede aspekter såsom gang og sprogbrug etc.

Biometri bruges naturligt af mennesker, når vi genkender hinanden. Tilsvarende har biometri i mange år været brugt til f.eks. at fange kriminelle på basis af biometriske spor efterladt på gerningssteder og at vedlægge f.eks. id papirer billede eller lignende.

Problemet med biometri?

Biometri er karakteriseret ved, at man kun har et sæt af biometriske "nøgler" som er fysisk data, der ikke kan ændres. Samtidig kan de ikke holdes hemmelige eller på anden måde beskyttes mod spoofing, dvs. identitetstyveri baseret på at forfalske en anden persons biometri.

Konsekvensen er en meget farlig kombination af mange forskellige trusler på samme tid. Borgeren kan ikke opretholde sikkerhed, fordi han altid tvinges til at identificere sig med det samme sæt nøgler (de biometriske karakteristika). Borgeren kan ikke få nye nøgler i tilfælde af at nogen med succes har stjålet og forfalsket hans biometriske nøgler. Og borgeren risikerer, at skulle bevise sin uskyld præsenteret for et "be-

vis” på misbrug og kriminalitet, hvor en anden har forfalsket borgerens digitale biometriske nøgler

Tendens

Hvordan sikrer vi mod denne teknologi?

Grundlæggende skal der skelnes mellem 2 former for biometri. Den ene er overvågning som f.eks. overvågningskameraer, der kan sikres ved FYSISK at blokere selve kameraet indtil indirekte ikke-invasive såsom infrarøde eller akustisk baserede sensorer har detekteret en sikkerhedstrussel som ikke reagerer på digitale anmodninger om at ”logge ind”, dvs. bevise en retmæssig adgang.

Den anden form er brug af biometri til egentlig identitet. Her er det kritisk at man aldrig opsamler eller indretter systemer til at KUNNE opsamle biometriske data.

Man kan arbejde med 2 grundlæggende principper. – den ene baseres på såkaldt biometrisk kryptering, hvor biometriske data indgår sammen med en nøgle som kun borgeren kender i en matematisk kryptografisk funktion, så man kan generere et resultat, der kan sammenholdes med et forventet resultat. Troværdigheden af denne type teknologi mangler stadig at blive bevist.

Den anden type er baseret på såkaldt on-card match, hvor de biometriske nøgler gemmes og aldrig forlader tokens, som borgerne selv har kontrol over. Biometri virker her som password til at etablere adgang til borgerens digitale nøgler.

Hvis du vil vide mere

Recommendations – Advisory Board of EU's ICT Security & Dependability Taskforce
http://www.securitytaskforce.eu/dmdocuments/securist_ab_recommendations_issue_v3_0.pdf

Cavoukian & Stoianov

http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

EPICs svar omkring bl.a. RFID og biometri til FTC workshop om ID

http://www.epic.org/privacy/id_cards/epic_ftc_032307.pdf

Royal Academy of engineering - Dilemmas of Privacy & Surveillance

http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

Biometrics and National Id 2.0 – talk at SRC’07

http://www.src07.de/PDF/ParalleleSitzung1/Engberg_PL1.pdf

CASE: TV-kanalovervågning (Kabeltv/TV over IP)

Med bredbånd kommer signalerne ikke længere som broadcast, men sendes individuelt. Det rummer en masse nye muligheder for On Demand TV, to-vejs services, søgninger, digital mediesupport etc.

Men samtidig skaber det også grundet manglende sikkerhed i infrastrukturen en omfattende overvågning hjemme i den enkelte husstand.

Hver gang man skifter kanal på ens tv, så registreres det af en central server i en profil. Profilen kan analyseres med henblik på at fremsende individualiserede reklamer og andre formål. Adgangen til disse profiler sælges på auktion og kan ikke antages at være gemt i databaser indenfor landets grænser. Almindelige forventninger om lovgivningsmæssig beskyttelse er allerede en illusion på samme måde som visse TV-stationer omgår medielovgivningen ved at sende over landets grænser.

Tendens

Gradvis kobles hele den konvergente medieverden sammen så borgerne vil snart blive udsat for individuelt målrettet reklame og sandsynligvis også egentlig individualiseret reklame baseret på disse stadigt mere dybdepsykologiske profiler. Adgangen til den enkelte borger sælges på auktioner for højeste bud.

Man kan diskutere om disse information udgør et problem, men her sætter kun kreativiteten grænsen, fordi disse data dækker over politisk medieforbrug, voksenkanaler og hele sriben af holdningsmæssig og kulturel profilering, som kan danne grundlag for arbejdsmæssige, kriminelle, kommercielle og politiske indgreb og overgreb.

Hvordan sikrer vi dette område?

Den enkelte borger kan intet gøre, så det er grundlæggende en statslig opgave at kræve sikkerhed for borgerne. Som alle andre områder gælder det om grundlæggende at umuliggøre opsamling af data udenfor borgerens kontrol. F.eks. via såkaldt mixing kan man "blande" husstande i dynamiske skiftende grupper, hvor den enkelte transmission ikke kan spores til en bestemt modtager og dermed indgå i en akkumuleret profil.

Borgeren kan altid frivilligt afgive nøgleinformation til at sammenstille profiler – enten fordi man ønsker en given service eller af andre årsager. Men det kritiske er, at borgeren skal kunne SKIFTE profil og helt nedlægge en gammel profil uden at have afgivet kontrollen over henførbareheden.

Hvis du vil vide mere

<http://www.seroundtable.com/archives/012985.html>

CASE: Google det store dyr i åbenbaringen eller "Big Brother"?

Google Desktop er et meget anvendt værktøj. Ved hjælp af Google er det mulig at foretage søgning baseret på et enkelt nøgleord. Umiddelbart betragtet udgør programmerne ikke nogen større trussel mod beskyttelse af individet, men en række forhold giver anledning til væsentlig bekymring. Som udgangspunkt er det vanskeligt for den gennemsnitlige bruger at foretage en balanceret installation af programmet og sikre at man har fuldstændig kontrol over hvilke data der afgives og hvordan Google fungerer. Følgende områder må man forholde sig endog overordentlig kritisk til:

1. Ved installation af Google Desktop medfølger andet ikke relateret programmel – i professionelle kredse kendt som foistware, dvs. ikke ønsket software. Når først man har accepteret installation af Google kan man ikke forhindre installation af de øvrige softwarepakker – eksempelvis en suite af Adobes

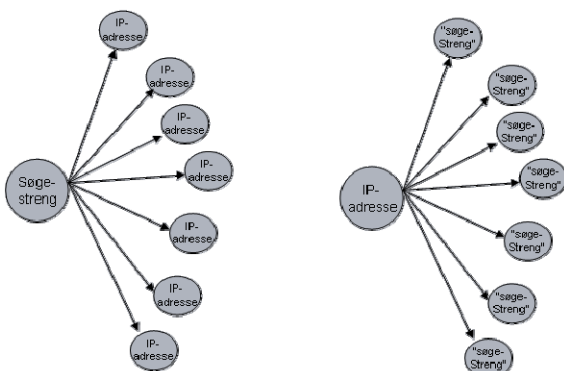
produkter. Forsøger man at fjerne disse programmer fungerer de øvrige ikke længere.

2. Ved anvendelse af funktionen ”brug fra flere computere” vil Google kopiere filer/indeks (eks. WORD, PDF, EXCEL m.v.) fra respektive computere til Googles egen/egne servere, hvor brugeren så kan hente information via en tilfældig web-browser. I udgangspunktet siger Google at informationen ikke er tilgængelig for andre end informationsejeren, men denne garanti rækker kun så langt som sikkerheden i Googles Access Management. Desuden er information formentlig ikke beskyttet mod udlevering i forbindelse med en retslig kendelse.
3. Sidst men ikke mindst er det betænkeligt at Google ikke har fraskrevet sig retten til at scanne information med henblik på målrettet markedsføring. Den systematiske indeksering af information på brugerens harddisk er et oplagt mål for målrettet bombardering med markedsføringsmateriale. De nødvendige forudsætninger herfor er allerede tilstede, idet Google under installation af softwaren også installerer en cookie der kan opsamle nødvendige oplysninger om din adfærd (jeg slettede lige den samling af indekserede søgninger som Google have registreret på min pc – 357 i alt inden for ca. 14 dage. Brug f-eks. Search files and folder med søgekriteriet ”google”).
4. Google Calendar giver brugeren mulighed for at lagre en mængde privat information. Ved installation er værktøjet som standard sat til ”privat”, men brugeren har mulighed for at slå en delingsfunktion til, således at alle kan søge i den private kalender (og det er da smart!) og det betyder virkelig alle. Vi kender danske eksempler på dette, hvor en endog meget stor koncern kunne konstatere at virksomhedsintern information var tilgængelig i det åbne rum. Eventuelle konfigurationsfejl fra brugerens side er naturligvis uden ansvar for Google.

Google er en kommerciel virksomhed og det skal man ikke glemme. Google tjener penge på markedsføring og jo mere information der kan hentes om den enkelte brugers anvendelse af Internet jo flere penge tjener Google fordi denne information er mange penge værd hvis den kan omsættes til personrettet markedsføring.

Hvilke oplysninger gemmer Google?

Dette spørgsmål kan ikke besvares helt entydigt, men ved at gennemlæse deres egen FAQ kan følgende i hvert fald konstateres:



Dette indebærer at Google indekserer alle søgestrengene og relaterer dem til en specific ip-adresse og kan ved at se på en specifik ip-adresse se hvad brugeren har søgt på. Ifølge Google relaterer man ikke personlige data som brugernavn o.l. ***med mindre brugeren er registreret Google bruger***”.

Hvem der har adgang til denne information er usikkert. Iflg. Google bruger man kun data kommercielt, men de svarer også direkte adspurgt om hvorvidt man vil udleverer til myndigheder, at man følger gældende lovgivning. Heraf kan man faktisk slutte, at man ikke er sikret mod misbrug af persondata så længe det sker fra et land der har en anden lovgivning end den europæiske. Dette har bl.a. resulteret i at EU Artikel 29-gruppen er i oprør.

Hvilke oplysninger modtager Google?

Hvis du anvender Google Desktop og vælger at aktivere de avancerede funktioner, vil Google Desktop sende information om de netsider du besøger, for at forbedre funktionerne i Google Desktop, f.eks. personalisering af nyheder, der vises i sidepanelet. Hvis du aktiverer de avancerede funktioner, kan Google Desktop også indsamle en begrænset mængde upersonlige oplysninger fra din computer og sende dem til Google. Dette omfatter bl.a. oversigtsoplysninger som f.eks. hvor mange søgninger, du har foretaget, og hvor længe det har taget at få resultaterne (interessant for en arbejdsgiver eller andre at følge med i hvor meget tid du bruger på internettet). Ifølge Google anvendes disse oplysninger til at gøre programmet bedre. Du vælger at aktivere de avancerede funktioner under installationen, og du kan altid skifte mening ved at ændre dine skrivebordsindstillinger, ***men du har ingen mulighed for at fjerne de oplysninger Google allerede har registreret.***

Oplysninger, der kan identificere dig personligt – f.eks. dit navn og din adresse – vil ikke blive sendt til Google uden din udtrykkelige tilladelse, men det er en sandhed med modifikationer idet det ud fra sammenhængen i mange situationer vil være muligt at følge det elektroniske spor direkte tilbage til kilden.

Sådan bruger Google de unikke applikationsnumre, cookies og dermed forbundne oplysninger

Din udgave af Google Desktop omfatter et unikt applikationsnummer. Når du installerer Google Desktop, vil dette nummer samt en besked om, hvorvidt installationen lykkedes, blive sendt tilbage til Google. Når Google Desktop automatisk kontrollerer, om en ny version er tilgængelig, vil det nuværende versionsnummer samt det unikke applikationsnummer blive sendt til Google. Hvis du aktiverer de avancerede funktioner, er det unikke applikationsnummer med i den information, der sendes til Google. Det unikke applikationsnummer er nødvendigt, for at Google Desktop kan arbejde, og *det kan ikke deaktiveres.*

Google Desktop bruger den samme cookie som Google.com og andre Google-tjenester. Hvis du aktiverer de avancerede funktioner, vil Google-cookien være med i den information, der sendes til Google.

Hvordan får jeg Google Desktop til at lade være med at registrere eller vise visse filer?

Hvis der er filer eller andre data, du ikke ønsker registreret af Google Desktop, er der iflg. Google selv flere måder, du kan undgå at få disse data vist, kopieret og registreret, ligesom det er muligt at fjerne dem fra registeret, efter de er blevet registre-

ret. Sidstnævnte udsagn er imidlertid tvivlsomt hvis først information er registreret i Google, for i anden sammenhæng en talsmand for Google sagt, at man ikke har intentioner om at fremstille et program, der gør det mulig for en bruger at fjerne alle registrerede oplysninger.

Hvordan fjerner jeg Google Desktop fra min computer?

Du kan til enhver tid afslutte din brug af Google Desktop ved at afinstallere Google Desktop programmet gennem funktionen ”Tilføj eller fjern programmer” i kontrolpanelet. Når du afinstallerer programmet, vil Google Desktop registeret og alle kopier i det blive slettet. De originale filer og applikationer ændres ikke.

Hvis du sletter din Google-konto eller afinstallerer Google Desktop, vil de indekse-ede filer i funktionen Søg på andre computere ikke længere være tilgængelige med Google Desktop, og de kan forblive på Googles servere i op til 30 dage, før de vil blive slettet iflg. FAQ, men igen er denne information inkonsistent med information givet andetsteds og det er sandsynligt at data kan gemmes op til flere år. I øvrigt henviser Google nu til dansk terrorlovgivning der efter deres opfattelse kræver at data gemmes i op til to år.

Hvilken beskyttelse har bruger mod at information anvendes af nationale eller andre myndigheder?

I virkeligheden ingen, idet Google blot siger, at man overholder gyldige og legale regler såsom dommerkendelser og undersøgelsesbegæring der vedrører personlig information. Dette er i virkeligheden det springende punkt, fordi det i sidste ende er spørgsmål om hvor Google lagrer sin information. Da det er en amerikansk virksomhed og al data- og systemkontrol udgår herfra er de som udgangspunkt underlagt amerikansk lovgivning, der ikke har særlige regler for beskyttelse af persondata. EU's ekspertgruppe for persondata, den såkaldte artikel 29 gruppe, har imidlertid i maj 2007 skrevet til Google, at deres indsamling af personoplysninger er i strid med EU's regler for beskyttelse af persondata, og henstillet at Google ændrer praksis. I brevet understreges det, at selvom Google er en amerikansk virksomhed er de forpligtet til at efterleve EUs lovgivning, når de driver virksomhed rettet mod det europæiske marked og -forbrugere. Der er i skrivende stund tegn på at Google vil imødekomme denne henvendelse.

Kan vi forvente endnu flere udfordringer med Google? Ja, antagelig. Den nylige erhvervelse af DoubleClick Inc. vil resultere i at Google kan registrere endnu mere information. DoubleClick anvender avanceret teknologi for at følge den enkeltes færden på nettet (intelligente cookies). Deres teknologi har hidtil primært fokuseret på at følge vores indkøbsvaner på nettet, men teknikken er universel og kan anvendes til at følge hvad som helst, f.eks. vores politiske og religiøse adfærd, søgninger på sex, drugs og meget mere.

Kan vi overhovedet beskytte os?

Ja og nej. Følgende regler kan anvendes:

1. Vil du være sikker på at helt undgå Googles opmærksom så lad være med at bruge Google overhovedet. Det er ingen garanti for at de ikke alligevel er på banen, men mængden at data er reduceret.

2. Lad være med at installere tilbudte tjenester fra Google med mindre du er særdeles avanceret og kan begrænse skaderne. Det kræver minutiøs konfiguration at foretage en begrænsning.
3. Du kan anvende en "anonymizer" der anonymiserer din ip-adresse, men det kan være i strid med lovgivningen i visse lande

Det er relativt sikkert at en virkelig dybgående gennemgang af Google vil bringe endnu flere ubehageligheder frem i lyset og det vil være nødvendig at der øves at massivt pres mod Google fra alle tænkelige kanaler med henblik på at begrænse deres stort set uindskrænkede informationsindsamling.

CASE: E-handel (Netbutikker bryder loven)

I dag findes mellem 4.000 – 5.000 on-line butikker i Danmark og tallet er stigende. Omkring 400 netbutikker har i dag e-mærket og dermed har forbrugeren garanti for at netbutikkerne lever op til gældende lov samt e-mærkets særlige krav.

E-handelsfonden, som står bag e-mærket, har i år offentliggjort en undersøgelse som viser, hvor gode de danske netbutikker er til at overholde markedsføringsloven, persondataloven, forbrugeraftaleloven og naturligvis e-handelsloven på e-handelsområdet. Undersøgelsen viser desværre vist, at de danske netbutikker fortsat har problemer med at efterleve e-handelslovgivningen på centrale områder.

De e-mærkede netbutikker får endnu engang topkarakterer. Det skyldes, at de i forbindelse med selve certificeringen har været igennem en proces, der sikrer, at netbutikken lever op til gældende lov samt e-mærkets særlige krav. Først da må netbutikken benytte e-mærket.

Undersøgelsen, der bygger på 181 tilfældigt udvalgte netbutikker, bygger på, hvorvidt netbutikken oplyser om persondatapolitikken (hvilke data der indsamles, Persondatalovens § 28) samt om CVR-nummeret er tilgængeligt på hjemmesiden (E-handelsloven § 7 stk. 1 nr. 4).

Netbutikkerne bryder loven

Mange danske netbutikker efterlever ikke lovgivningen på områder som aftaleindgåelse, persondatapolitikken og fortrydelsesretten. Det er tre centrale områder, som svækker forbrugernes tillid til e-handel, fordi forbrugerne ikke får de oplysninger (fortrydelsesret m.m.), de er berettiget til ifølge gældende lov.

Privacy-perspektiver – Dankort-svindler

Forbrugerne er bange for at miste eller få misbrugt personlige oplysninger, når de handler på Internettet. Der skal fx oplyses navn, adresse, e-mail og et telefonnummer, bankkontonummer, kreditkortnummer m.m., så bliver de usikre og afbryder i værste fald handlen.

Finansrådet varetager de klagesager, hvor netbutikker har svindlet med forbrugernes dankort. Denne ordning kaldes for indsigelsesordningen eller charge back, og den giver forbrugeren ret til at få tilbagebetalt pengene, hvis netbutikken har svindlet med prisen eller varen.

Forbrugeren har ret til få tilbagebetalt pengene, hvis:

- Kunden ikke har modtaget varen
- Kunden har været udsat for et misbrug af sine kortoplysninger
- Kunden har fortrudt købet inden han har modtaget varen ved fx at nægte at modtage den eller undlade at afhente den på posthuset
- Der er trukket et højere beløb end forbrugeren havde godkendt ved bestillingen

CASE: Man kan ikke trække sine tidligere udtalelser på internettet tilbage

Når man lægger oplysninger ud på internettet, er det vigtigt at være opmærksom på, at man mister kontrollen med oplysningerne, og at de kan misbruges. Situationen kan f.eks. opstå ved at informationerne tages ud af en sammenhæng og bruges til andre formål, end man selv havde placeret dem i. Det kan også være at de tilgås af personer, som man ikke havde tænkt på, havde interesse heri. Problematikken er helt grundlæggende at selv oplysninger, som man har offentliggjort for år tilbage, pludselig vil kunne komme negativt tilbage til en selv.

Skal man have revet for længst glemte parkeringsbøder i næsen 20 år efter sagen er afgjort? Fartbøder, spritkørselsbøder, overtrædelse af politivedtægten, osv. Hvis alt hvad man gør i det offentlige rum (fysisk såvel som virtuelt) registreres og gemmes, skal det så på et senere tidspunkt kunne hentes frem?

Hvornår krænkes privacy

Privacy krænkes, når oplysninger, som kan henføres til mig, og som jeg vil opfatte som ikke-offentlige - altså som tilhørende privatlivets fred - indsamles og anvendes uden min eksplicitte viden.

Hvad gør jeg selv galt

Jeg kan f.eks. skrive eller kopiere oplysninger til et forum, chat-room, på en internetside eller giver andre personer tilsvarende oplysninger, som de gør offentligt tilgængeligt. Situationen kan typisk accelereres ved, at man fremsætter (især negative) udsagn med oplysninger af personhenførbart art om andre personer.

Hvordan beskytter jeg mig

Man kan beskytte sig selv ved ikke selv at skrive - og ikke give andre mulighed for at skrive - oplysninger om en selv, som man mener tilhører privatlivets fred. Ens egen privacy bliver ikke respekteret mere end den respekt man selv udviser for andres privacy.

Konkrete eksempler

1) I forbindelse med sagsbehandlingen laver en kommune et regneark over modtagere af offentlige ydelser for at give det politiske udvalg i kommunen en baggrund for at forstå omkostningerne til denne type ydelser og statistiske oplysninger herom. De personhenførbare oplysninger i bagvedliggende regneark kommer derved med i en fil, som lægges på kommunens politikernet. Samtidig åbnes af hensyn til demokratisk kontrol og åbenhed i beslutningsprocessen for at alle på internettet får adgang til kommunens politikernet.

2) I en periode lider jeg af en sygdom, som jeg finder råd og trøst ved at diskutere i et patient-chatroom dedikeret til den pågældende sygdom. Herved kan alle, som kan

genkende mig bag ved det valgte brugernavn, blive klar over hvad jeg har fejlet og hvordan jeg har haft det i en periode af mit liv, som jeg på et senere tidspunkt vil være meget ked af at få revet i næsen.

3) I et anfald af ungdommelig kådhed tager jeg sammen med nogle venner nogle ret kompromitterende billeder, som vi deler via en af nettets foto-delings tjenester uden at begrænse delingen til de involverede. Sammen med den tilhørende tekst kopieres og indekseres billederne af søgemaskiner og andre søgerobotter på nettet, hvorved de efterfølgende vil være tilgængelige, når jeg bliver udnævnt til et offentlig embede, som ikke harmonerer med de kompromitterende billeder.

CASE: Usikker IT-sikkerhed (Eksempler på hvordan ”privatlivets fred” kan krænkes via internettet.)

Adgangskoder

Simple adgangskoder er nemme at gætte, især for målrettede ordbogsangreb, programmer eller hvis brugeren bliver udsat for social engineering. Derfor er det vigtigt for brugere at vælge deres adgangskoder på mindst 8 tegn og benytte store og små bogstaver, tal, tegn og adgangskodesætninger. Generelt må det anbefales at man anvender flere forskellige faktorer til at få adgang - f.eks. biometrisk fingeraftryk kombineret med en pinkode eller et kort.

Genbrug ikke oplysninger

Ved at benytte samme navn, brugernavn, email, certifikat eller andre følsomme oplysninger på flere forskellige websider kan disse let sammenholde alle øvrige oplysninger, der er afgivet på de pågældende websteder. Det bliver herved umuligt at opretholde adskilte personae for forskellige sammenhænge som arbejde, privatliv, foreningsaktiv m.m. Dette bør ikke ske.

Identitetstyveri

E-mails og websider kan nemt forfalskes og er en brugt metode til at lokke følsom information ud af internettets brugere. Denne information kan værste tilfælde bruges til at få adgang til brugeres bankkonti. Metoden kaldes for phishing, spear phishing eller pharming og de forfalskede e-mails og websider er nemme at blive narret af som almindelig internetbruger.

Handelsvilkår på websider

Når internebrugere indkøber varer via internettet fremgår sælgerens handelsvilkår som regel i forbindelse med handlen. Hvis brugeren accepterer sådanne handelsvilkår på websider uden at læse disse først, risikerer brugeren at acceptere handelsvilkår som ikke er hensigtsmæssige for denne, fx fraskrivelse af ansvar og sælgerens ret til brug af afgivne informationer.

Cookie

En cookie kan indeholde følsomme informationer, f.eks. brugernavn og password, præferencer o.l. Praksis med at gemme brugernavn og password i en cookie er ved at forsvinde, da risikoen er kendt, men det forekommer stadig. Cookies anvendes også i forbindelse med automatisk login på websider. Selvom en cookie ikke selv indeholder følsomme informationer, kan den åbne for adgang til disse. For at stjæle en cookie skal der udnyttes en sårbarhed på systemet. Brugere kan jævnligt slette cookies, hi-

størrelse over besøgte websider og midlertidige filer via funktioner i browseren. Hvis man gør dette sletter man også f.eks. autosignon til sin netbavnk.

Browser-cache

Når en webside bliver vist, med f.eks. personfølsomme oplysninger, bliver den ofte gemt i browserens cache (kopilager). For at få adgang til browserens cache skal der udnyttes en sårbarhed på systemet. Brugere kan slette browserens cache-information via funktioner i browseren.

Browser-passwordliste

Mange browsere tilbyder at huske brugeren logininformationer for diverse websider. Sikkerheden er blevet strammet, men bare det at man benytter det, udgør en risiko. For at stjæle fra browserens passwordliste skal der igen udnyttes en sårbarhed på systemet, men det er rystende enkelt hvis der er fysisk adgang til computeren.

Keystroke-logger

Det vi skriver på tastaturet kan forholdsvis nemt kopieres og lagres i en fil etc. Den slags 'aflytning' kan ske både software- og hardwaremæssigt. Programmer der udfører 'aflytning' vil som regel blive opdaget af anti-virus software. Programmerne kan blive installeret (automatisk) ved besøg på hjemmesider, via en sårbarhed i browseren, ved at hente og installere programmer fra tvivlsomme websteder eller ved at åbne vedhæftede filer i email.

Bagdøre (trojansk hest)

Et program, der giver, som regel uindskrænket, adgang til vores system uden vi ved det. Sådanne programmer havner på computeren på samme måder som keystroke loggeren. Der kan også være tale om enten utilsigtede eller forsætlige sikkerhedshuller i programmer, der downloades med et umiddelbart legitimt formål, f.eks. i forbindelse med installation eller brug af digital signatur.

Google-hack

Ved hjælp af særligt udformede søgninger på Google er det muligt at finde f.eks. webkameraer og forbinde sig til dem. Når man installerer f.eks. et webcam eller en mikrofon er det vigtigt at læse dokumentationen og sikre sig at apparatet ikke bliver brugt, uden man er klar over det.

Digitale billeder

Billeder taget med et digitalkamera kan indeholde flere informationer end man skulle tro - og har de været redigeret på en computer kan der være føjet mere til. Når billederne sendes ud på nettet - for at blive til papirbilleder eller pryde en hjemmeside - kan der være afsløret meget mere end man havde tænkt sig.

Eksterne servere

Kompromittering af f.eks. mailserver eller proxyserver. Hvis det er muligt at skabe en forbindelse til administrationsdelen på en server, vil der være adgang til at læse al information der passerer den. De fleste privatpersoner anvender en mail- eller proxyserver hos deres internetudbyder og må derfor bero på dennes sikkerhed. IT administratorer i virksomheder kan have adgang til al kommunikation – også selvom der benyttes SSL kommunikation mellem en medarbejder og en ekstern webside.

I mange sammenhænge bruger vi andre servere og der kan være behov for viden om graden af sikkerhed.

Trådløse netværk

Kan sikres med kryptering og kodeord, men er det som udgangspunkt ikke. Herved kan fremmede få direkte adgang til et lokalnetværk eller en privat internetforbindelse udenom eventuelle firewalls i det faste netværk

Botnets

Når computere ikke står beskyttet på internettet eller ikke er opdateret med programrettelser, risikerer computerne at blive overtaget af hackere og optaget i botnets. Botnets er netværk af overtagede computere, som hackere kan anvende til at udføre it-kriminalitet uden internetbrugeres viden.

CASE: Demokratiske elektroniske valg

I et repræsentativt demokrati er Demokratiske valg det mest kritiske element, fordi det kontrollerer magtfordeling og påberåber legitimering af monopolisering af vold i hænderne på en stat.

Den fysiske valghandling er gennem lang tid optimeret til at forebygge de mange og konstante forsøg på at snyde i forbindelse med denne magtfordeling. Motiver spænder lige fra at øge egen magtandel til at lokalisere minoriteter og forhindre dem i at få andel i magten.

Specielt minoritetsbeskyttelsen er meget kritisk, fordi alle magtkonstruktioner har en latent tendens til at ønske at sikre og opretholde egen magt, hvorved oppositionen udgør en trussel og dermed ofte forfulgte. Det er således absolut kritisk for enhver valghandlings legitimitet at mindretal kan stemme UDEN man er i stand til at lokalisere HVEM der stemmer på minoritetspartier.

Kravene til en valghandling er nogen af de stærkeste, vi finder. Eksempelvis er kravet om, at man skal være alene i afstemningsboksen både for at sikre fortrolighed, men samtidig også for at beskytte mod tvang i forbindelse med afstemning. Selv hvis en borger udsættes for pres, skal vedkommende kunne stemme i henhold til egen overbevisning, uden at pressionskilden kan verificere, hvad vedkommende har stemt.

Legitimeringen af en valghandling er dermed en delikat balance mellem de forhold:

- at den enkelte borger har tillid til fortrolighed
- at vedkommende stemme tæller med ved valget
- at borgeren ikke kan dokumentere, hvad han har stemt og dermed ikke kan gøres til genstand for tvang.

Hvad er problemet

Myndighedernes ønske om at øge påstanden om legitimitet via stemmeprocenten eller mindske omkostningerne fører til forsøg på at svække valghandlingens reelle og opfattede legitimitet, samt åbner for muligheder for svindel.

Eksempelvis må det seneste Estiske valg formentlig afvises som demokratisk legitimt, fordi samarbejde mellem 2-3 instanser let kan afsløre hvad hver enkelt borger

har stemt - dermed er der ingen reel minoritetsbeskyttelse. Der er ingen beskyttelse mod tvang.

Der ligger en mulig signalværdi i ikke at møde op til en valghandling, som indikerer en opfattelse af ligegyldighed eller endda mistillid til hele valgprocessen. Valget at afgive en blank stemme er også et signal, idet det aktivt udtrykker mistillid i form af et signal om manglende opfattelse af repræsentation, opfattelse af mistillid til den demokratiske proces eller på anden måde en protest.

Hvordan sikrer vi dette område?

Vi har i dag ikke kendskab til teknologiske løsninger, der kan forsvare at man tager selve valghandlingen ud af en fysisk stemmeboks.

Man kan understøtte valghandlingen ved at digitalisere valghandlingen før, under og efter. Men yderst varsom – kravene er meget svære.

CASE: Offentlig forvaltning

Den offentlige forvaltnings håndtering af oplysninger om borgerne.

Fordelingen af rettigheder og pligter mellem den offentlige forvaltning og borgerne bygger på retsgrundsætninger, der består uanset den teknologiske udvikling.

Officialprincippet går ud på, at den offentlige forvaltning i samarbejde med borgeren har ret til at anskaffe sig de informationer, der er nødvendige for afgørelsen af en konkret sag.

Ophobning af informationer om borgeren til forvaltningens frie afbenyttelse strider som udgangspunkt imod dette princip. Hvis en given forvaltning til brug for den fortsatte behandling opbevarer oplysninger om borgeren, gælder der en række bestemmelser om vedligeholdelse, ligesom det lejlighedsvis skal overvejes, om det er relevant fortsat at beholde dem.

Officialprincippet slår igennem forskellige steder i Persondataloven.

Det er vigtigt, at borgerne kender til officialprincippet, idet krænkelser i forbindelse med påtænkte registersammenkøringer bør påtales.

Legalitetsprincippet vedrører proportionalitet mellem forvaltningens indgreb i bredeste forstand overfor borgeren og formålet dermed. Indsamling af følsomme og eller fortrolige oplysninger samt kortlægning af borgerens liv udgør et sådant indgreb. En gennemgribende kortlægning af alle borgernes liv og/eller en samkøring af alle tilgængelige informationer om borgerne, stillet til rådighed for dele af den offentlige forvaltning vil som udgangspunkt stride ikke bare mod Persondatadirektivet og Persondataloven, men også imod legalitetsprincippet. Legalitetsprincippet er hjemlet i Grundlovens bestemmelse om ejendomsrettens ukrænkelighed.

Både hvad angår officialprincippet og legalitetsprincippet er der tale om retsgrundsætninger, der står over den konkrete lovgivning. Krænkelser af disse vil kunne medføre, at konkret lovgivning – for slet ikke at tale om ulovnormerede ændringer i forvaltningens beføjelser – kan underkendes ved domstolene.

I forbindelse med E-government eller digital forvaltning er dele af embedsværket inde på tanken om, at nytten af at effektivisere den offentlige forvaltning skulle berettigede indgreb, der flytter på den hidtidige balance i kontrakten mellem borgerne på den ene side og forvaltningen på den anden, idet der i strid med den hidtidige forståelse af henholdsvis officialprincippet og legalitetsprincippet opbevares og genbruges indsamlede oplysninger om borgerne i langt større udstrækning end hidtil.

Der kan være tvivl om, hvornår grænserne overskrides. Som udgangspunkt er nytteværdien af en påtænkt effektivisering ikke tilstrækkelig som forudsætning for at gennemføre et generelt udsalg af borgerrettigheder. Det er navnlig betænkeligt, hvis man begiver sig ind på et ulovnormeret skråplan, der fører til risiko for reel eavesdropping (forhåndsindsamling af oplysninger uden formål, blot for nytteværdiens skyld og siden vilkårlig udnyttelse af dem til senere formål).

Før sådanne initiativer iværksættes, bør der

- indhentes udtalelser fra den forvaltningsretlige sagkundskab
- føres en principiel debat i form af en eller flere konferencer, ligesom folketingets retspolitiske udvalg bør involvers i sagen.

Politiets adgang til persondata falder i vid udstrækning indenfor en undtagelsesbestemmelse i Persondatalovens § 30, stk. 2, hvorefter hensynet til statens sikkerhed og politimæssig efterforskning går forud for lovens behandlingsbestemmelser.

Praksis er her uklar, idet opbevaring af oplysninger til senere brug strider imod loven i det omfang, en mistanke rettet imod en person viser sig ubegrundet.

CASES vedr. offentlig forvaltning: Quick skranken

Flere og flere kommuner indfører kvik-skranker, hvor borgerne i princippet kun behøver at henvende sig et sted for at få offentlig service, ændret deres bolig-, social- eller skatteoplysninger eller andet.

Problemer med privacy?

Problemet med kvik-skranken er, at der fra et sted gives adgang til en masse fortrolige oplysninger. Medarbejderen kan godt have et personligt log-in, men i en hektisk dagligdag kan det ske, at man 'låner' hinandens PC'ere, og dermed er det uklart, hvem det reelt er, der henter oplysninger om borgeren. Der kan også være ansat vikarer, som man tildeler et midlertidig password, der kan skiftes. Ligeledes er situationen den, at i en del kommuner landet over fungerer kvik-skranken således, at den er bemandet med personale, der i en turnusordning er én uge i kvik-skranken efterfulgt af en uge i deres fagstilling i en forvaltning, derefter én uge i kvik-skranken igen osv. Dette skaber en rettighedsproblematik – for hvis borgernes privacy skal sikres, bør personalet tildeles forskellige rettigheder alt afhængig af, om de befinder sig i kvik-skranken, eller de befinder sig ude i deres fagstilling i forvaltningen.

Kvik-skranken repræsenterer i virkeligheden en mulighed for medarbejdere for at hente mange oplysninger om borgerne på tværs af registre – også ud fra andre hensyn end dem borgerne har, måske nysgerrighed om naboen. Dermed kan der ske et brud på den privacy, som borgerne bør have krav på. Der kan også tegne sig nogle

andre mønstre, hvis der er mulighed for at ”samkøre” mange registre på tværs af forvaltningerne – oplysninger som borgerne (måske) gerne vil holde for sig selv, og som kan skade dem, hvis de bliver kendt i en større kreds - på deres arbejdsplads eller lign.

Da det f.eks. kom frem, at den daværende konservative formand Peer Stig Møller havde kørt spritkørsel som ganske ung måtte han gå af som formand. Det var ikke efterfølgende muligt at finde frem til, hvilken betjent der havde hentet oplysninger - der var flere - og dermed finde frem til den der havde fortalt det til bl.a. pressen.

Tendens

Det er vores oplevelse, efter at have talt med forskellige kommunale IT-chefer og medarbejdere, at der findes vidt forskellige måder at tildele rettigheder til medarbejderne i kvik-skranken. I nogle kommuner har kvik-skranke personalet stort set adgang til alle systemer, og i andre kommuner har de kun begrænset adgang og skal således gå tilbage i de enkelte forvaltninger for at søge dybere ned i borgerens data. Det er også vores oplevelse, at kommunerne ikke har gjort sig overvejelser omkring forskellige rettighedstildelinger, såfremt de bemander deres kvik-skranke efter en turnusordning. Der er dog udsendt en vejledning til kommunerne fra KL i samarbejde med Indenrigs- og Sundhedsministeriet og Datatilsynet i september 2006 – men noget kunne tyde på, at denne ikke er informeret godt nok ud i kommunerne.

Hvordan sikrer vi dette område?

Den enkelte borger kan intet gøre for at forhindre, at data bliver uretmæssigt anvendt – det er op til den enkelte kommune at sikre, at medarbejderen kun får adgang til de data, der er nødvendige for at vedkommende kan udføre sit arbejde. Ligeledes hviler ansvaret for rettighedstildeling, instruktion, overvågning og sanktionering på den enkelte kommune. Kommunerne bør, hvis de ikke allerede arbejder efter vejledningen: ”Datasikkerhed i borgerservicecentre”, straks begynde at arbejde efter denne vejledning. Desuden bør de få iværksat konkrete uddannelsesaktiviteter blandt kvik-skranke medarbejderne - f.eks. som Datatilsynet i vejledningen foreslår: et ”datasikkerhedskørekort”, som alle medarbejdere skal tage, inden de starter i kvik-skranken. Det kan f.eks. være en test med et antal spørgsmål, som forudsætter den fornødne viden om kommunens uddybende sikkerhedsregler og øvrige datasikkerhedsinstrukser, før medarbejderen vil kunne besvare den korrekt.

Referencer

Vejledningen; ”Datasikkerhed i borgerservicecentre”:

http://www.kl.dk/_bin/a1aac476-802a-41ca-b14a-82ea539966e1.pdf

CASES vedr. offentlig forvaltning: Bibliotekslån

Fortæl mig, hvad du læser, så skal jeg fortælle dig, hvem du er. Kommunerne har i og for sig i sine baser adgang til at læse, hvad der interesserer borgerne, efterhånden som de låner bøger, musikcd'er og videoer.

Der er tale om en klassisk problemstilling. Allerede, da den første registerlov blev vedtaget i Danmark, anlagde man ”the puzzle point of view”. Oplysning om det enkelte udlån behøver ikke være særlig følsomt, men får man samlet informationer om den enkelte borgers samlede lån over en årrække, er det samlede billede ikke bare retvisende, men også af en helt anden følsomhed end hver oplysning for sig.

Bruce Schneier, amerikansk ekspert på området, refererer ofte til fænomenet ”eavesdropping”, når han omtaler opsamling af enkelt informationer om det enkelte borger. Billedet svarer til, at man opsamler regndråber til et bassin. Symbolsk er et bassin noget andet end den enkelte vanddråbe. Og bassinet bliver også brugt til noget andet. Meningen med at opsamle information om den enkelte borgers lån er at styre tilbageleveringen af udlånet. Derimod er viden om den enkelte borger uvedkommende for biblioteket.

CASES vedr. offentlig forvaltning: Elektronisk Patientjournal

EPJ er på mange måder et centralt område for det digitale samfund.

For det første repræsenterer det en meget stor og voksende andel af samfundets resourceforbrug. Presset på at få kvalitet for pengene er voldsomt og voksende. Samtidig er interesserne i at sætte sig på dele af systemet mindst lige så stort, så der er meget stærke interesser på spil. Langt hovedparten af disse interesser og funktioner er dog sekundære i forhold til den primære sygdomsbehandling.

For det andet fordi EPJ arbejder med nogle af de skrappeste krav. Svinger systemet – teknologi, mennesker og processer - så dør mennesker eller deres livskvalitet forringes kraftigt. Når en akut situation opstår skal man hurtigt kunne få adgang til opdateret og korrekt information for at kunne hjælpe. Og når diagnoser og behandlinger skal planlægges og gennemføres kræver det adgang til detaljeret information i præcis den rigtige form for at understøtte en stadigt mere kompleks og nuanceret proces.

For det tredje fordi sundhed repræsenterer et voldsomt komplekst system med mange specialeområder og funktioner, der skal arbejde sammen og koordineres i et komplekst samspil. Det kræver adgang til den rigtige information – i den rigtige form, på det rigtige tidspunkt. En kompleksitet der hastigt vokser til andre områder af det offentlige system, ud over landegrænser og på tværs af offentlige/private skel. Systemparadigmet skal kunne vokse med denne kompleksitet.

For det fjerde, fordi området er et af de allermest følsomme. Folks dårligdomme og data herom har endog meget store misbrugsmuligheder og repræsenterer meget store værdier i de forkerte hænder. Kommercielle, teknokratiske, kriminelle og sågar sociale interesser

For det femte er brugervenlighed ekstremt vigtigt. Lige fra at nogle patienter ikke selv kan håndtere egen information i den ene ende over de meget dynamiske og til tider kaotiske forhold på et hospital til at datagenbrug stiller endog meget store krav til den semantiske standardisering på tværs af systemer og formål. En diagnose om overfølsomhed i går, kan i dag være kritisk i en akutsituation og i morgen være en væsentlig parameter for kostsammensætning.

Folketinget har netop truffet beslutning i L50B om at vende samtykkeretten omkring EPJ samtidig med at man begrænser sikkerhedsspørgsmålet til at logge adgange og etablere såkaldt rollebaseret adgangskontrol. Grundprincippet omkring EPJ er dermed en rent regel-baseret adgangsbegrænsning til afdelingen. Bortset derfra er EPJ en database uden særlige sikkerhedsmekanismer med administrative

adgangskontroller håndteret på afdelingsgruppe-niveau kombineret med logning af enkelttransaktioner.

Det har været på tale at etablere et central samtykke register – i praksis først og fremmest for at håndtere såkaldte negativ samtykker, dvs. hvor borgeren siger at netop denne person (f.eks. en nabo) ikke må få adgang til data.

Endelig bør det bemærkes at denne model allerede synes at danne rollemodel for andre områder, herunder specielt servicecentre i kommunerne.

Hvad er problemet?

De fysiske patientjournaler var ikke godt sikrede, men med digitaliseringen sker et meget væsentligt skift, idet massebrug (mange), målrettede søgninger (f.eks. VIP) og triggers baseret på bestemte sammenhænge (f.eks. aborter) etc., nu gøres meget nemmere, billigere og samtidig kan ske på afstand, så gerningsmanden ikke kan spores. Samtidig muliggøres en voldsomt stigning i sekundærbrugen af borgerens data.

Hovedproblemet er, at der ikke er en holdbar sikkerhedsmodel og ikke engang synes at være forsøg på at skabe en sådan.

Logning er et glimrende element til mange ting, men som sikkerhedsværktøj for data er det ikke meget bevidt. Når så mange i henhold til L50B har adgang til EPJ er det alt for nemt at bruge andres adgange, det er nemt at have en plausibel forklaring mens data bruges til helt andre formål og endelig er der masser af adgang som sker bagom og udenom systemet f.eks. i forbindelse med større kørsler.

Rollebaseret adgangskontrol tager udgangspunkt i en model, hvor der ikke er nogen fundamental sikkerhed i EPJ samtidig med at adgange dels etableres på alt for højt niveau (for mange) og dels ikke er forfinet nok til at begrænse i forhold til formålet. Adgangsbegrænsningen er ikke direkte koblet til det og relationer, men baseres på overordnede forhold som let kan omgås.

Det er formentlig i borgerens interesse og nødvendigt at etablere en særskilt adgang som understøtter de dynamiske processer på et hospital mens indlæggelse foregår. Men denne model kan på ingen måde beskytte data generelt eller danne grundlag for den samlede sikkerhedsmodel for EPJ.

Hvad værre er, så er modellen slet ikke tilpasset eller forberedt for at EPJ-udviklingen kan sikres i takt med de stadigt stigende behov og krav om adgang fra stadigt flere sider. Et centralt samtykke-register koblet til en generel adgangskontrol vil være administrativt uhåndterbart, let at omgå og samtidig etablere nye risici. Hovedproblemet er at det i praksis vil være stort set umuligt at udtrykke samtykke i en tilstrækkeligt nuanceret form til at et regel-baseret system kan håndtere det uden det bliver til en ren pseudo-foranstaltning som ikke fører i praksis forbedrer sikkerhed eller retssikkerhed. Delegering til en portal kan selvfølgelig ikke komme på tale, hvis man ønsker blot et minimum af sikkerhed, fordi en sådan portal vil blive en såkaldt single-point-of-trust-failure.

Man har kort sagt skabt en konstruktion som drastisk forværrer sikkerheden omkring EPJ samtidig med at man har fjernet samtykkeretten og overset de stigende behov for en sikkerhedsmodel, der kan følge med.

Hvordan sikrer vi dette område?

Først og fremmest skal man på trods af den skarpe kritik af den nuværende tilgang passe alvorligt på med at tro at EPJ er et simpelt spørgsmål. Det rummer mange af verdens mest komplekse sammenhænge og modstridende interesser. Der vil uanset hvordan området angribes skulle ske en gradvis modning og action learning. Det vigtige er at kun det offentlige kan sikre at denne proces finder sted – det sker ikke hvis løsninger ikke kræves og efterspørges både politisk og af det administrative system.

Der er 3 helt centrale problemstillinger, som skal tilgodeses.

1) Problemstillingen omkring akut hjælp, hvor datasikkerhed og beskyttelse mod de mange forskellige former for kriminalitet ikke må slå folk ihjel. Modellen for akut hjælp sætter reelt overliggeren for sikkerhed.

2) Problemstillingen omkring en aktiv behandlingsproces under indlæggelse, hvor en væsentlig del af styring i sagens natur må overgå til de professionelle hjælpere, og så den generelle sikkerhedsmodel hvor borgeren som udgangspunkt er meget mere aktivt styrende. Under indlæggelse er det meget tænkeligt at man må etablere en midlertidig udvidet adgang som kan være rollestyret og f.eks. koblet til vagtplaner etc.

3) Men grundlæggende er der behov for en radikal forandring i holdningen til patienter og borgernes sundhedsdata, så data sikres på forhånd og al tilgang antages at være sekundær uden personhenførbare medmindre det eksplicit er del af en af patient etableret behandlingsadgang. Patienter betragtes i dag i al for høj grad som maskiner, der skal repareres – ikke som kompetente borgere med individuel suverænitæt og den bedste til selv at vurdere kvalitet. Man må som et demokrati tage udgangspunkt i antagelse af at borgeren er kompetent og skal have kontrol. Hvor det ikke er tilfældet (borgeren kan eller vil ikke) skal man kunne delegerere kontrollen, i første omgang til pårørende og først som sidste udvej til en læge etc.

Man kan tænke sig forskellige modeller til håndtering af ovenstående og man bør sikre support for både uafhængig opgradering og at kunne håndtere flere forskellige modeller i parallel, dels fordi områder har forskellige behov og fordi danske systemer vil skulle fungere i en stadig mere international og heterogen sammenhæng. Danske patienter indlægges i udlandet, på private hospitaler og sundhedsdata indgår i stigende grad i helt andre sammenhænge end det traditionelle behandlesystem (f.eks. omkring ernæring og livsforsikringer).

Men der foreligger konkrete bud på alle disse områder så i henhold til persondatadirektivets kriterium om maksimal sikring af borgeren givet teknologiens stade er man lovpligtig til at tage spørgsmålene alvorligt.

Omkring 1) annoncerede danske Priway ApS i efteråret 2006 en løsning til hvordan patienter kan have en engangsadgang som kan aktiveres i nødsituationer.

Omkring 3) har Canadiske Credentica annonceret en model baseret på såkaldte credentials. Teknologirådet beskrev i Fra Råd til Tinge Nr. 186 om "IT Privacy skal forbedres" en samlet model for EPJ baseret på at man vender kontrolmodellen.

Omkring 2) er der tale om en kombination af 3) og forskellige former for mere lokale modeller, der f.eks. kan være baseret på rolle-baseret adgangskontrol.