

Har vi intet at skjule? *eller* En brugervejledning til digitalt selvforsvar

Af David Walther Birk

Den 15. september 2007 trådte bekendtgørelsen om logning af tele- og internettrafik i kraft. Danmark tog dermed et vidtgående skridt i overvågningen af civile borgere. Hvad kan du selv gøre for at undgå at blive digitalt overvåget?

Argumentet

Den 15. september 2007 trådte bekendtgørelsen om logning af tele- og internettrafik i kraft. Danmark tog dermed et vidtgående skridt i overvågningen af civile borgere: konsekvent systemiseret registrering af al digital kommunikation. Med andre ord bliver telefonsamtaler, sms'er, email og internet-aktivitet registreret og gemt i op til et år. Dette med henblik på terror-beskyttelse og forebyggelse af kriminalitet.

I juridiske termer hedder det sig, at muligheden for indgreb i meddelelshemmeligheden altid skal være der. Det er som det lyder: privat kommunikation er reelt holdt op med at eksistere, og den 15. september 2007 var dermed dagen hvor Danmark, uden nogen lagde mærke til det, blev et samfund med elementer som Orwell og Kafka fiktioniserede i deres vildeste paranoia.

Formålet med denne artikel er at informere om, hvordan vi som privatpersoner kan forsvare os mod denne registrering, og ikke mindst hvorfor vi overhovedet skulle være interesserede i at forsvare os. Det sidste er måske det vigtigste, da indførelsen af denne vidtgående overvågning blev begået af en majoritet af folkevalgte politikere uden større ståhej. Og efterfølgende reaktioner (eller manglen derpå) tyder på, at det ikke just er et emne, folk bekymrer sig videre om. Så vi starter med, hvorfor vi overhovedet skal tage os af det.

I stort set alle sammenhænge, hvor overvågning bliver diskuteret, kan man høre et eller flere varianter af et specifikt argument til forsvar for overvågning: "Hvorfor

skulle jeg bekymre mig om at blive overvåget, hvis jeg ikke har noget at skjule?” Hvilket vil sige, hvorfor skulle lovlige borgere være bekymret for deres privatlivs fred? Og dermed underforstået, folk der bekymrer sig om overvågning, må have kriminelle hensigter.

I dets simple form kan det afvises med ligeså simple (retoriske) argumenter såsom:

- ▶ Har du gardiner? Må jeg se dine kreditkort-regninger fra sidste år?
- ▶ Jeg er ikke tvunget til at retfærdiggøre beskyttelse af mit privatliv. Du er tvunget til at retfærdiggøre, hvorfor jeg skal overvåges. Kom tilbage med en dommerkendelse.
- ▶ Jeg har intet at skjule, men jeg har heller ikke noget, jeg har lyst til at vise dig.
- ▶ Hvis du intet har at skjule, har du ikke noget liv.
- ▶ Det handler ikke om at have noget at skjule, det handler om at mit privatliv ikke rager nogen.
- ▶ Stalin ville have elsket det.
- ▶ Sender du også alle dine breve som postkort?

I ”intet at skjule”-argumentets mere avancerede form hæves argumentet fra et personligt niveau op til et spørgsmål om samfundsmæssig nytteværdi: Hvad har mest værdi for samfundet? At ingen ved, du har ringet til din mor og dit lokale pizzeria eller at vi fanger potentielle terrorister. Ifølge dette eksempels logik er det kun terrorister, der bør være bekymrede.

Selv hvis man havde noget at skjule, for eksempel at man hver dag ringede til sine 5 bollevenner og 20 sex-linier fra jobbet, så er det jo ikke din mand/kone eller din chef, der har adgang til informationerne. Det har kun folk der jagter terrorister og andre kriminelle. I denne form er ”intet at skjule”-argumentet svært at afvise med en smart replik.

I stedet kan man pege på en hel række fundamentale problemer med argumentet: Argumentet sidestiller retten til privatliv med retten til at skjule kriminelle aktiviteter. Det opfatter dermed beskyttelsen af individets privatliv som værende grundlæggende imod samfundets generelle interesse. Dette er en grundlæggende fejltagelse. Man kan argumentere, at mange elementer i beskyttelsen af et individs privatliv er i samfundets interesse, hvis vi fastholder, at samfundets interesse er at bevare demokrati og individuel frihed. Simplificeret kan man sige at samfundet består af individer, og jo bedre individerne har det, jo bedre har samfundet det. Så hvis vi betragter individuel frihed som en værdi, må det også betragtes som en værdi for samfundet. Og beskyttelse af individets privatliv, og følelsen individet har af at have et privatliv kan betragtes som en essentiel del af individuel frihed. Det kan formuleres som det, at jeg føler mig fri til at gøre som jeg vil inden for hjemmets fire vægge uden andres kontrol, fri til at sige hvad jeg vil uden bekymring for at nogen vil bruge det imod mig (ytringsfrihed), fri til at stemme på hvem jeg vil uden at blive sat i bås, og så videre.

De fleste følgevirkninger af overtrædelser af privatlivets grænser er desuden noget, der må betragtes som uønskeligt i et retssamfund. Af sådanne følgevirkninger kan nævnes afhøring, identifikation med dette og hint, usikkerhed, eksklusion, tillidsbrud, afpresning, personlig forfølgelse og lignende. Hvis ophævelsen af borgernes sikkerhed og tillid til systemet er prisen vi må betale for måske at forhindre terror, så kan man

diskutere om det er det hele værd. Og man kan argumentere at løsningen er værre end problemet. Et slags defensivt selvmord.

Et andet element er, at selv om vi måske ikke har noget imod, at staten ved man har ringet til mormor, så giver det kun mening at samle sådanne informationer, hvis man samler store mængder af dem og forbinder dem til det enkelte individ. Så ikke bare mormor, men alle du ringer til, hvornår og hvor du var da du gjorde det (via triangulering af mobilmaster), alle du skriver til og hvornår, alle websider du besøger, hvornår og hvad du gør på dem, alle du er i kontakt med over nettet og så videre ud af en tangent, der kun er begrænset af graden af ens paranoia (og alene situationen nu er grundlag for en ret høj grad af berettiget paranoia). Alle disse informationer bliver ikke brugt til at konstatere, om du har gjort noget ulovligt eller ej, de bliver brugt til at kigge efter mønstre og profiler af, hvad der bliver opfattet som potentielle terrorister og potentielle kriminelle. Det handler slet ikke om overvågning af kriminalitet, det handler om forsøg på at kigge ind i fremtiden og forudsige, hvem der måske vil begå terror og kriminalitet.

”Videnskaben” bag udarbejdelsen sådanne specifikke mønstre og profiler er selvsagt meget hypotetisk, i den forstand at den i høj grad er frakoblet virkeligheden, og snarere har med fordomme at gøre. Man kan forestille sig en slags tip en 13er med spørgsmål som: Er personen muslim, er personen fra fattige kår, er personen af anden etnisk herkomst, stemmer personen på dette eller hint parti og lignende. Hvis vores hypotetiske person så opnår for eksempel 5 point kan han/hun betragtes som potentiel udøver af tankekriminalitet. Og ikke bare denne han/hun, men ligeledes alle som har kontakt med vedkommende. Hvis der så er flere potentielle tankekriminelle i kontakt med hinanden, bliver det endnu mere interessant. Og så videre og videre. Det er en skrue uden ende, hvor store dele af den danske befolkning risikerer i stigende grad at blive mistænkeliggjort og overvåget, baseret på helt tilfældige og stærkt usikre faktorer, som ingen har adgang til. Dette er det kafkaske element.

En relateret konsekvens er, at hvis vi forstår information som magt, så får institutionelle organer umiddelbart isoleret fra politisk kontrol, for eksempel PET, meget stor magt over private individer i det danske samfund. Igen kan man spørge (stærkt retorisk), om det er noget, vi er interesseret i som demokrati og retsstat.

Et tredje element er faren for sekundært brug. Som loven er nu, er det op til teleselskaberne og internetudbydere selv, at opbevare informationerne (for slet ikke at tale om hotellerne/kroerne/internetcaféerne). Det vil sige private virksomheder af varierende størrelse (og varierende ansvar over for det danske samfund). Værdien af store mængder følsomme personoplysninger inden for markedsføring er meget stor. Tag Google som eksempel: et af verdens rigeste firmaer tjener penge udelukkende på at placere reklamer de rigtige steder. I den mere lyssky afdeling finder vi junk-mail industrien, der vurderes til at omsætte for 282 millioner dollars, eller 1.3 milliarder danske kroner årligt. Faren for at nogen bliver fristet til at stjæle informationer om foreksempel alle TDC's kunder, er ganske reel – udelukkende på baggrund af disse informations enorme økonomiske værdi.

I en hel anden boldgade er udenlandske efterretningstjenesters formodentlige adgang til oplysningerne (CIA har allerede adgang til alle dine bankoplysninger, dette var et af de nye elementer da alle danske bank-aftaler blev opdateret for nylig, igen et resultat

af terrorkpakken). En ting er PET, der nok er hemmelige og skæg-og-blå-briller-agtige, men de synes dog stadig først og fremmest lidt latterlige og forholdsvis udskadelige som de går rundt og tilbyder hash til gengæld for information. Men hvad med CIA? Hvad med alle andre vestlige efterretningstjenester? Hvad med vores nye samarbejde med efterretningstjenester, der systematisk benytter tortur? Det er jo ikke nogen hemmelighed, at folk udvist fra Danmark til deres ophavsland er blevet tortureret udelukkende på baggrund af det faktum, at de er blevet udvist. Hvad er så situationen når militærregimer og politistater får adgang til enorme mængder information om hvilken som helst person?

Dette er på nuværende tidspunkt relativt hypotetisk. Men hypotetisk paranoia er desværre også nødvendigt at tage med i overvejelserne. For én ting er, at situationen som den er nu, kan være nok så bekymrende, en anden ting er hvad fremtiden potentielt måtte bringe. For det er et helt central element, at når først ændringer i infrastrukturen er gennemført (i dette tilfælde registrering og logning af al digital kommunikation), er de meget svære at slippe af med. Dertil kommer, at den politiske virkelighed kan ændre sig fra dag til dag.

Én virkelighed er, at det rare velfærdsdanmark går og overvåger os for at fange nogle slemme terrorister (og deler informationerne med knap så rare CIA), en helt anden virkelighed er hvor mægtigt et våben total overvågning af al digital kommunikation kan være i de forkerte hænder. Forestil jer STASI med denne teknologi og infrastruktur. De var uhyggelige nok i forvejen, men armeret med nutidens redskaber – systematisk overvågning af alle borgere, ville DDR have været et overvågningssamfund af helt sindssyge proportioner. Den eneste reelle forskel på det danske samfund i dag og vores værste politistats-mareridt, er at den politiske virkelighed er relativt velmenende. Det ændrer imidlertid ikke på den formelle infrastruktur, som udfoldes i skrivende stund, samt på det faktum, at demokratier historisk set har forholdsvis let ved at tippe over i fascisme.

Så er vi solgt til stanglakrids? Ikke helt, for vi må ikke glemme at de grundlæggende forhold der gør total overvågning mulig også muliggør forsvar mod overvågning. Overvågning af al digital kommunikation kan lade sig gøre, fordi al vores digitale kommunikation passerer igennem centrale enheder – men vi har selv fuld kontrol over hvad, der passerer igennem disse centrale enheder, eller nærmere i hvilken form. I det følgende vil jeg redegøre for hvordan vi kan skjule indholdet af forskellige former for digital kommunikation. Deres logning bliver ligegyldig, hvis det de logger er uforståeligt.

En brugervejledning til digitalt selvforsvar

Internet

Internetaktivitet kan identificeres med dig som person eller husstand, fordi alle forbindelser til internettet har et unikt nummer, et såkaldt IP-nummer. Dette nummer bliver tildelt os af internetudbyderen. Hvis man går ind på eksempelvis whatismyipaddress.com, kan denne helt tilfældige webside fortælle dig dit IP-nummer og placere dig geografisk i verden. Dog ikke helt præcist – det websiden kan se er placeringen af din internetudbyder, hvilket dog stadig giver muligheder for at vise dig

for eksempel danske webreklamer, selv om du er på en international side. I gamle dage kunne man føle sig relativt beskyttet fra overvågning og registrering, da det kun var din internetudbyder, der blev registreret – ligesom det kun var din internetudbyder, der kendte din egentlige identitet, og ikke loggede dine aktiviteter (eller det burde og skulle de ikke). Som nævnt er situationen en anden i dag, og al webaktivitet bliver forbundet til den private person, der står som ejer af den benyttede internetforbindelse og registreret til statens brug.

Det man kan gøre for at skjule ens internetaktivitet, er at benytte en såkaldt proxy-server. Det vil sige at man forbinder sig til et IP-nummer på nettet, der så sender dig de informationer og sider du nu besøger. Det eneste din internetudbyder så kan se, er IP-nummeret på proxy-serveren. Det siger ikke noget som helst om, hvilke sites du rent faktisk har besøgt på nettet. Du springer ganske enkelt det centrale registreringssted over. Der findes en del offentlige proxy-servere alle kan benytte (se for eksempel www.publicproxyservers.com), en del af dem er sågar anonyme. Det vil sige, at selv hvis en dygtig tekniker/hacker satte sig ned og brugte mange timer på at spore din aktivitet tilbage til dig, ville vedkommende bare møde en ubrydelig kryptering (men dette er ofte slet ikke nødvendigt, i og med de overvåger os alle, er der også en vis mængde anonymitet i masserne).

Hvis det skal gøres endnu smartere kan man bruge Tor: Anonymity Online (torproject.org). Det er et system af en hel masse forbundne proxy-servere, så hvis nogen prøvede at spore dig ville de blive mødt af et verdenskort fyldt med linjer, der suser på kryds og tværs af kontinenterne (nøjagtigt som i utallige Hollywood-film). Man kan endda få et plugin til Firefox-browseren, så man bare skal trykke på en lille knap i hjørnet, for at sprøjte blæk bag sin færden på nettet (se addons.mozilla.org/en-US/firefox/addon/2275). Det er en stor tilfredsstillelse at vende tilbage til whatismyipaddress.com og se dig placeret et sted i det centrale Kina. Eneste bagdel ved Tor er, at det endnu er ret langsomt. Men det kan bruges selektivt.

En helt anden mulighed er at bruge frit tilgængelige trådløse netværk. Der kan være visse moralske skrump, hvis det er naboens. Der er dog juridisk potentiale i at have åbne private trådløse netværk, hvordan kan man gøres ansvarlig for handlinger som alle i nærheden med trådløs internetkompatibilitet kunne have udført (så vidt jeg ved er det ikke afprøvet i det danske retssystem, men det har virket i USA).

Email

Med ovennævnte metode kan man forhindre, at ens email (hvis man bruger webmail) bliver identificeret med ens person. Men da det kan være besværligt altid at surfe bag en proxy-server, må vi bruge andre metoder til at beskytte os. Løsningen er simpel nok: kryptering af mailens indhold. En analogi til dette er, at putte sine breve i en kuvert, uden kryptering er dine korrespondancer frit tilgængelige for myndighederne som var de skrevet på postkort (hvis PostDanmark tog billeder af alle dine postkort).

Det fantastiske er, at kryptering af den type nationale forsvar bruger er frit tilgængelig for alle. Det vil sige at myndighederne sagtens kan se de krypterede beskeder, men de ville aldrig nogensinde kunne finde ud af, hvad krypteringen gemte.

Det mest almindelige system er PGP, det står for Pretty Good Privacy (se philzimmermann.com/EN/background/index.html for PGP's historie). Det er gratis og

som sagt ubrydeligt (med mindre de stjæler din digitale nøgle og kender dit password). Det fungerer på den måde, at hver enkelt person har en private key og en public key. Den private nøgle holder du for dig selv, den offentlige giver du til modtageren, alle dine venner eller hvem som helst. En analogi til systemet kunne være at du har én privat nøgle og en masse ulåste hængelåse (public key), som denne private nøgle låser op. Du giver så den åbne hængelås til en ven, han putter sin besked i en kasse og låser den med hængelåsen. Nu er den låst, og det er kun dig der har nøglen (og nøglen virker kun med den samtidige indtastning af dit password).

Der findes et simpelt PGP-krypterings-program til Windows, der hedder Windows Privacy Tray (winpt.sourceforge.net/en). Det kan bruges til mail, instant messaging (MSN), Facebook eller bare generel udveksling af information per tekst. Man kan også få et Firefox-addon, der integrerer PGP-kryptering direkte i gmail (se getfirepgp.org).

De rigtige paranoia-feinschmeckere vil selvfølgelig straks se fælden: Man kan forestille sig at en krypteret mail ville gøre én langt mere mistænkelig i myndighedernes øjne end en normal mail. For at vænne tilbage til postkort-analogien: når alle sender postkort er kuverten mistænkelig. Det er en del af problemet fremført ovenfor, mistænkeliggørelsen af forsvaret/bevarelsen af essentielle borgerrettigheder. Derfor, jo flere krypterede mails jo bedre. Det kan bruges som en simpel form for protest, harmløse eller endda meningsløse mails sendt udelukkende for at spille overvågerens tid og ressourcer.

Telefoner/sms'er

Telefoner er straks værre, da det er et lukket system, vi ikke har samme kontrol over som vores computere. En ekstra dimension er, at mobiltelefoners lokation kan spores via sendemaster, ned til omtrent 10 meters radius i byer. I retssagen imod Fighters & Lovers blev dét, at flere af medlemmerne var sporet i samme 2 kilometers radius inden for de samme 2 timer, brugt som inkriminerende argument (de var det samme sted, de forsamlede sig, de konspirerede).

Løsningen er simpel og utilfredsstillende: Sluk telefonen, eller bedre endnu - lad være at tage den med (en slukket telefon ude i byen afslører stadig hvor du var, da du slukkede den, og kan dermed ligesom den krypterede email virke ekstra mistænksom). Hvis vi skal helt ud på paranoiaens overdrev, bør man også tage simkortet ud, ansatte i FET (Forsvarets Efterretningstjeneste) skal når de møder på arbejde ikke bare slukke mobilen, men også fjerne simkortet. Dette understøtter teorien om, at selv slukkede telefoner udsender et signal).

En anden løsning er at købe forudbetalte simkort i løshandel. Opkald og sms'er vil stadig blive registreret men de vil umiddelbart ikke være direkte forbundne med et individ.

Alternativet kan være at bruge ip-telefoni, her er vi tilbage på computeren og dermed tilbage ved styrepinden. Skype benytter kryptering, dog er der en reel chance for at myndighederne har en bagindgang – altså din hackerfjende kan ikke umiddelbart lytte med, men myndighederne har en universal nøgle (i Tyskland er det officielt sådan). Et bedre alternativ er at benytte Zfone (zfoneproject.com), dette er en krypterings-

protokol udviklet af manden bag PGP. Zfone kan integreres med de fleste ip-telefoni-programmer, dog ikke Skype.

Afslutning

Der er utallige muligheder for at udveksle informationer diskret, som ikke er nævnt her (nogle mere snedige end tekniske, for eksempel at benytte sub-sub-fora på obskure curling-holds fansider). Men ovenstående må være dækkende for nu.

Metoderne beskrevet ovenfor kan syntes som et mægtigt besvær bare for at skjule aktiviteter der nok er private, men i det store perspektiv syntes lige gyldige. Men alle er de gode muligheder for at beskytte vores borgerrettigheder og ikke mindst at yde modstand imod politiske tiltag der langsomt men sikkert skubber vores civilisation tættere og tættere på afgrunden.

Til sidst bør det nævnes, at det måske største problem er, at så få syntes at bekymre sig om tilsidesættelsen af vores essentielle borgerrettigheder i lognings-bekendtgørelsen. Så hermed en opfordring til at sprede ordet med alle midler (massefinansierede landsdækkende trådløse pirat-netværk, mail-kun-krypteret-uge, officielle wikier, der planlægger terrorangreb for hypotesens skyld et cetera).