IT-Politisk Forening
www.itpol.dk

10. oktober 2011

Til medlemmerne af
Folketingets retsudvalg

Vedr.: Notat om udvidelse af internetlogning (skrevet af IT-Politisk Forening)

IT-Politisk Forening har skrevet et notat om udvidelse af internetudbydernes logningsforpligtelse, som vi gerne vil sende til medlemmerne af Folketingets retsudvalg.

Baggrunden for vores notat er en rapport fra en arbejdsgruppe under Justitsministeriet, som anbefaler en udvidelse af internetudbydernes logningsforpligtelse, herunder brugerregistrering på internetcafeer, offentlige hotspots og internetadgang på biblioteker.

Rapporten/notatet fra Justitsministeriet (Politikontoret) har sagsnr. 2009-945-1473, dokument nr. JJA40456, og er dateret 17. juni 2011. Vi har fået adgang til notatet via aktindsigt hos Justitsministeriet. Notatet fra Justitsministeriet er ikke offentliggjort, men det har fået en del medieomtale, dels i juni måned, dels under den netop overståede valgkamp.

Såfremt det har Retsudvalgets interesse, vil IT-Politisk Forening gerne uddybe vores synspunkter over for medlemmerne af Retsudvalget. Foreningens bestyrelse kan nemmest kontaktes på email: bestyrelsen@itpol.dk

Med venlig hilsen

Jesper Lund
Bestyrelsesmedlem, IT-Politisk Forening

Privatadresse: Carl Bernhards Vej 15, 2.tv, 1817 Frederiksberg C
Telefon: 2972 7719, Email: itpol@jesperlund.com

Vedlagt: notat om udvidelse af internetlogning (8 sider, PDF fil)

IT-Politisk Forening

Notat om udvidelse af internetlogning

Executive summary

- Notat fra justitsministeriet foreslår en kraftig udvidelse af internetovervågningen i Danmark
- Borgerne får forbud mod at have åbne trådløse netværk og mod at "udlåne" deres internetadgang til fremmede personer
- Formålet er at lukke huller i den eksisterende logningsbekendtgørelse så alle forbindelser logges, men der efterlades blot nye huller da man med VPN og TOR stadig kan få anonym adgang til internettet
- IT-Politisk Forening har tidligere advaret mod at internetovervågning er en farlig glidebane, og de nye forslag fra Justitsministeriet bekræfter vores værste formodninger
- Forslagene fra Justitsministeriet medfører desuden ganske betydelige praktiske og økonomiske byrder for specielt privatpersoner, foreninger og mindre virksomheder som cafeer, hoteller og campingpladser
- Ulemperne ved øget internetovervågning er mange og konkrete, mens fordelene er få og teoretiske
- IT-Politisk Forening foreslår at man helt afskaffer internetovervågningen eller i det mindste den del som vedrører offentlige hotspots, hvor Justitsministeriet indirekte indrømmer at den nuværende logning er værdiløs for politiet

Analyse og kritik

I slutningen af juni omtalte medierne et notat fra Justitsministeriet om revision af logningsbekendtgørelsen. Notatet gav anledning til en del kritik da der lægges op til en kraftig udvidelse af internetovervågningen, for eksempel krav om personregistrering for brugere af offentlige hotspots og internetadgang på biblioteker.

Forslagene blev kraftigt kritiseret af blandt andre Jacob Mchangama, som kaldte det "et frontalangreb på det frie og åbne internet" http://mchangama.blogs.berlingske.dk/2011/06/23/et-frontalangreb-pa-det-frie-og-...

Notatet er ikke offentligt tilgængeligt på Justitsminisieriets hjemmeside, men vi har fået notatet ved henvendelse til Justitsministeriet. I den forbindelse har Justitsministeriet gjort os opmærksom på at der er tale om en foreløbig

udgave af en rapport som senere skal sendes til det politiske system. Arbejdsgruppen bag notatet har bedt om kommentarer fra blandt andet teleselskaberne og Horesta, men ikke fra den almindelige befolkning som også vil blive direkte berørt af forslagene.

Version2 har den 7. september offentliggjort notatet i forbindelse med en artikel
http://www.version2.dk/artikel/her-er-notatet-fra-justitsministeriet-om-person-l...

Selv om der ikke er tale om den endelige rapport med anbefalinger til revision af logningsbekendtgørelsen, har IT-Politisk Forening valgt at skrive denne analyse og kritik af rapporten (notatet). For det første fordi vi gerne vil være i god tid hvis et lovforslag pludseligt bliver hastet i gennem, som det desværre ofte er set på overvågningsfronten. For andet fordi vi primært forventer tekniske ændringer i f.eks. den måde som personregistreringen skal foretages på, og medmindre den endelige udgave af rapporten bliver skrevet fuldstændigt om, vil der være nogle fundamentale principper som vi finder stærkt foruroligende. Når den endelige udgave af rapporten foreligger, vil vi naturligvis opdatere vores kommentarer hvis der er anledning til det.

Huller i de nuværende logningsregler

Baggrunden for notatet er et ønske om at lukke "huller" i den nuværende logningsbekendtgørelsen. Arbejdsgruppen blev i 2009 anmodet om at overveje hvordan brugere af internetcafeer, hotspots og internetadgang på biblioteker kan registreres. Notatet fra juni 2011 er imidlertid noget mere vidtgående end det, hvilket vil fremgå af vores analyse og kritik i det følgende.

I dag stiller logningsbekendtgørelsen krav om at internetudbyderne registrerer brugernes trafik, typisk i form af afsender og modtager IP adresse for hver 500. pakke. Derudover skal afsender og modtager for alle emails registreres særskilt. Der er imidlertid to væsentligt begrænsninger i denne registrering i forhold til et ønske om en komplet registrering af internettrafikken.

For det første er det kun internetudbydere i "telelovens forstand" som skal foretage logning. Det betyder groft sagt at der skal være tale om en kommerciel aktivitet hvor internetadgang stilles til rådighed for en modydelse, enten penge for et internetabonnement eller salg af andre produkter, for eksempel en cafe som tilbyder kunderne internetadgang via hotspot. En offentlig uddannelsesinstitution eller et offentligt bibliotek er undtaget fordi der ikke er et kommercielt grundlag. En virksomhed regnes heller ikke for at være en internetudbyder, selvom virksomheden giver medarbejderne adgang til internettet.

Den anden begrænsning er at internetudbydere kun skal registre de oplysninger som i forvejes behandles om brugerne. Den bestemmelse har stor betydning for om brugerne i praksis kan identificeres hvis politiet senere får adgang til de trafikdata som er logget. Ved en traditionel kablet internetforbindelse er brugerens identitet registreret og valideret fordi internetadgangen skal leveres på en bestemt adresse. Det samme vil normalt gælde ved mobilt bredbånd med løbende abonnementsforhold og mulig bindingsperode. Internetudbyderen vil være sikker på at kunden ikke løber fra regningen, og brugervalideringen sker således af økonomiske årsager.

Men der eksisterer også situationer hvor internetudbyderen ikke har nogen interesse i at registrere eller kontrollere brugerens identitet. Det gælder for eksempel forudbetalt mobilt bredbånd, hvor et SIM kort kun er gældende for en bestemt periode eller indtil en bestemt trafikmængde er opbrugt. En cafe med internetadgang vil højst være interesseret i at begrænse adgangen til de betalende kunder, hvilket kan gøres med en fælles adgangskode som står på kvitteringen eller menukortet. Vi er også bekendt med cafeer som har et helt åbent trådløst netværk fordi det giver en god og billig reklame, og personalet skal ikke bruge tid på IT-support til kunder som måske har tastet adgangskoden forkert ind. Det er vigtigt at understrege af cafeen stadig er omfattet af logningsbekendtgørelsen som udbyder fordi internetadgangen regnes for en kommerciel aktivitet, men udbyder er alene forpligtet til at registrere de brugeridentiteter som det trådløse access point tildeler brugerne, hvilket som regel vil være MAC adressen på brugerens trådløse netkort. En MAC adresse kan ikke direkte henføres til en specifik navngivet person, og derudover er det meget nemt at ændre (spoofe) udstyrets MAC adresse.

Kravet om logning på cafeer og andre offentlige hotspots er ofte blevet kritiseret fordi de indsamlede brugeroplysninger alene er MAC adresser, og da MAC adresser normalt ikke peger på personer, er det meget usandsynligt at de vil kunne bruges til noget i en politimæssig efterforskning. Vi finder det særdeles interessant at Justitsministeriet selv fremhæver denne begrænsning på side 5 i notatet. Vi er klar over at Justitsministeriet gør dette for at begrunde de efterfølgende forslag om obligatorisk personregistrering på hotspots, men vi betragter det samtidig som en indirekte anerkendelse af at dele af den nuværende logning er overflødig (uanset hvad man mener om logningsbekendtgørelsen, giver det ingen mening at logge trafikdata som aldrig vil kunne bruges).

Der vil også være tilfælde hvor en abonnent er registreret, men hvor internetadgangen bruges af flere personer. Et eksempel er en boligforening som køber en internetforbindelse og deler denne mellem de enkelte lejemål. Hvis der er færre end 100 lejligheder, er boligforeningen i dag ikke omfattet af logningsbekendtgørelsen.

En ny model for internetlogning i Danmark?

Alt i alt er der altså en række "huller" i logningsbekendtgørelsen, og notatet beskriver forskellige metoder til at lukke disse huller. Overvejelserne er ikke begrænset til personregistrering på offentlige hotspots. Hele logningsbekendtgørelsen er faktisk i spil i notatet, og slutresultatet er en model hvor al internettrafik i Danmark enten kan henføres til en bestemt person, hvis identitet er valideret af internetudbyderen, eller til en kontaktperson (kunde hos internetudbyderen) som præcist skal kunne gøre rede for hvem der har brugt internetforbindelsen. Det er en meget vidtgående ændring af logningsbekendtgørelsen, hvor internetadgang nærmest administreres efter de samme principper som våbentilladelse. Forslagene betyder også at den almindelige dansker vil blive direkte reguleret af logningsbekendtgørelsen, enten med forbud mod at lade andre bruge internetforbindelsen eller med krav om logning hvis dette ikke overholdes.

Forslagene i notatet kan opdeles i to hoveddele: udvidelse af kredsen af pligtsubjekter (hvem skal foretage logning) og krav om valideret personregistrering.

Alle skal være omfattet af logningsbekendtgørelsen

For så vidt angår kredsen af pligtsubjekter kommer notatet med et temmelig vidtgående forslag: i stedet for telelovens udbyderbegreb og dets kommercielle grundlag, skal ALLE være omfattet af de samme regler. Hvis der er mere end en person som bruger en given internetforbindelse, vil der være tale om at give andre adgang til internettet ("internetudbyder"). Det gælder også en almindelig husstand hvor en familie deler en internetforbindelse (f.eks. en ADSL forbindelse).

Det er dog ikke meningen at der nødvendigvis skal foretages logning på alle niveauer, blot fordi nogen får adgang til andres internetforbindelse. Kriteriet for krav om logning på personniveau skal baseres på en skelnen mellem disse to tilfælde

1. Internetforbindelsen bruges af en afgrænset og kendt kreds af personer (eksempel: en husstand eller en virksomhed)
2. Brugerne af internetforbindelsen kan ikke på forhånd afgrænses (eksempel: en cafe hvor gæsterne får internetadgang)

Notatet foreslår at der skal ske logning på personniveau i tilfælde 2), mens det i tilfælde 1) vil være tilstrækkeligt at en afgrænset og identificeret kreds af personer kan henføres til en konkret internetforbindelse. I tilfælde 1) vil der altid ske logning af trafikken på et højere niveau, typisk hos en kommerciel internetudbyder. Når politiet får adgang til trafikdata, vil disse data kunne henføres til enten en bestemt person eller til en afgrænset kreds af personer. Det er langt mere vidtgående end den nuværende logning, hvor dele af trafikken helt er undtaget og hvor trafikdata måske kun kan henføres til en MAC adresse.

Umiddelbart kan dette måske lyde som en relativt uskyldig ændring, men det er på ingen måde tilfældet. Udover det rent principielle i at foretage endnu mere masseovervågning af personer som ikke er mistænkt for en forbrydelse, indebærer notatets forslag at den enkelte danske familie får konkrete forpligtelser og restriktioner efter logningsforpligtelsen. Betingelsen for at husstanden ikke selv skal foretage logning på personniveau er at internetadgangen effektivt begrænses til husstandens medlemmer eller gæster som man efterfølgende kan navngive overfor politiet. Hvis man giver en ukendt kreds af personer adgang til internetforbindelsen via et åbent trådløst netværk, bliver man selv omfattet af logningskravene. Reelt er dette et forbud mod åbne trådløse netværk fordi kravene til foretage logning i sig selv er ganske betydelige (f.eks. en PET-godkendt kontaktperson der står til rådighed 24 timer i døgnet, samt de nye foreslåede krav om personvalidering). Det åbne trådløse access point nævnes direkte i notatet, men der er andre grænsetilfælde som ikke diskuteres. Skal familien ligefrem notere navnene på børnenes måske ofte skiftende venner i teenageårene, hvis familien giver børnenes venner adgang til deres internetforbindelse?

En virksomhed vil kun falde ind under tilfælde 1) hvis internetadgangen begrænses (og afskærmes) til virksomhedens medarbejdere. Virksomheden må ikke give gæster adgang til internettet, medmindre der oprettes et separat gæstenetværk hvor der er krav om logning på personniveau. En boligforening som har fælles internetadgang for foreningens lejemål skal indskærpe overfor medlemmerne at de ikke må lade andre (herunder gæster i hjemmet) få adgang til internetforbindelsen. Hvordan dette skal kontrolleres i praksis fremgår dog ikke af notatet.

I enkelte situationer kan der blive tale om en begrænsning af logningen sammenlignet med de nuværende regler. Det gælder kommercielle internetudbydere hvor brugerkredsen er afgrænset og kendt. Notatet nævner fitnesscentre, private uddannelsesinstitutioner og hoteller som mulige eksempler. For hotellernes vedkommende forudsætter det dog at hotellet nøje kontrollerer identiteten på hver eneste gæst samt indskærper overfor gæsterne at de ikke må lade besøgende på værelset bruge internetadgangen. Den slags formaninger og identitetskontrol vil næppe være gavnlige for et serviceerhverv, så at der skulle være tale om en regelforenkling for hotellerne er nok mere teori end praksis.

Valideret personregistrering for alle forbindelser

Den andel hoveddel af notatets forslag handler om valideret brugerregistrering. Hvis der er krav om logning efter principperne ovenfor, skal det samtidigt være et krav at denne logning kan henføres til en person hvis identitet er kontrolleret inden der gives adgang til internettet. For kablede internetforbindelser og mobilt bredbånd med løbende abonnement sker dette allerede i dag, men for forudbetalt mobilt bredbånd, offentlige hotspots, internetadgang på biblioteker og anden kortvarig internetadgang skal der indføres nye regler som sikrer at brugerens personoplysninger altid registreres og kontrolleres/valideres. Uden en valideret personregistrering må internetudbyderen simpelthen ikke give brugeren adgang til internettet.

Arbejdsgruppen gennemgår en række metoder til at sikre dette. Konkret diskuteres fordele og ulemper ved automatiseret validering baseret på CPR nummer, adgangskoder sendt per SMS til en mobiltelefon, kreditkortnummer samt naturligvis NemID (de fleste metoder anvendes allerede i dag i begrænset omfang forskellige steder i landet). Notatet er ekstremt grundig med hensyn til at sikre at man rent faktisk identificerer en person, hvilket giver problemer for både SMS koder og kreditkort.

Brugen af SMS koder vil kun være acceptabel for Justitsministeriet hvis man samtidig forbyder anonyme taletidskort i Danmark, og metoden kun kan anvendes på danske mobilnumre da man af gode grunde ikke kan forbyde udenlandske taletidskort der kan roame i Danmark (ligesom andre udenlandske SIM kort). Arbejdsgruppen har også fundet frem til at man i udlandet kan købe forudbetalte Visa og Mastercard, som ikke nødvendigvis kan spores til en bestemt person fordi de kan købes mod kontant betaling (for 1000 kroner plus gebyrer køber man et kreditkort hvor der maksimalt kan bruges 1000 kroner inden kortet spærres). Arbejdsgruppen har været i kontakt med Nets (PBS) og sammen har de fundet en løsning: der eksisterer tabeller med nummerserier som bruges til forudbetalte kreditkort, så man skal blot udelukke disse kort (tabellerne skal løbende opdateres).

Disse begrænsninger er måske "nødvendige" for at kunne sikre personidentifikation, men de betyder samtidig at en række personer vil blive udelukket fra at bruge offentlige hotspots eller internetadgang på biblioteker. Personer under 15-18 år og udenlandske turister vil være overrepræsenteret i denne gruppe, og i sidste ende kan disse restriktioner have økonomiske konsekvenser for turisterhvervet i Danmark. Som fallback mulighed for de automatiske brugervalideringer nævner arbejdsgruppen ganske vist manuel kontrol af billed-ID, men udenlandske turister vil formentlig undre sig over at Danmark forlanger fremvisning af pas for noget så trivielt som kortvarig adgang til internettet. I den forbindelse skal det bemærkes at arbejdsgruppen har undersøgt udenlandske erfaringer med

personregistrering på hotspots, men man har ikke været i stand til at finde nogle.

Alt i alt er der tale om en kraftig udvidelse af internetovervågningen i Danmark, og reglerne kommer til at berøre den enkelte dansker temmelig direkte. Dels på grund af forbuddet mod at give andre adgang til internetforbindelsen (og forbuddet mod åbne trådløse netværk), dels på grund af de nye identifikationskrav ved offentlige hotspots og internetadgang på biblioteker. Det bliver mere besværligt for den danske befolkning at få adgang til internettet, og udbredelsen af offentlige hotspots vil utvivlsomt blive påvirket i negativ retning. Hvis fantasien får frit spil, er der mange kommercielle aktiviteter hvor det ud fra en økonomisk synsvinkel kan betale sig at give offentligheden adgang til internettet, for eksempel denne artikel hvor et forlag overvejer at lave et gratis hotspot i Kongens Have i håb om at sælge flere e-bøger
http://politiken.dk/kultur/tvogradio/ECE1366400/traadloest-internet-i-kongens-ha...

Hvis der er krav om ikke bare logning men også valideret personregistrering, vil den slags aktiviteter blive væsentligt dyrere, og internetudbyderen vil få en masse ballade med at forklare brugerne hvorfor deres identitet skal registres og kontrolleres. Reklameværdien ved at forære internetadgang væk vil hurtigt blive overskygget af det negative image ved at man skal agere kontrollant på statens vegne i en privatiseret masseovervågning af internettet.

Der vil stadig være store huller i logningen

Der er et andet aspekt ved arbejdsgruppens notat som vi i IT-Politisk Forening finder stærkt foruroligende, og det er argumentationen for at indføre mere overvågning. Flere steder er der en argumentation ala følgende: hvis man ikke lukker de huller som der er i den nuværende trafikregistrering (logning), og hvis der er mulighed for at "snyde" sig uden om logningen, vil udgifterne ikke stå i et rimeligt forhold til værdien af logningen. Et andet sted i notatet (side 44) argumenteres der for at det er urimeligt at overvåge lovlydige borgeres kommunikation, hvis de kriminelle nemt kan snyde sig uden om, og det vil arbejdsgruppen altså ændre på ved at overvåge al internetkommunikation.

IT-Politisk Forening er meget uenig i disse udsagn. Vi er selvfølgelig enige i at det er urimeligt at overvåge lovlydige borgeres kommunikation, men vi kan altså ikke se at det gør nogen forskel om de kriminelles kommunikation (måske) også overvåges. De kriminelle udgør en meget lille del af befolkningen, ikke mindst fordi trafikdata kun må anvendes på alvorlige lovovertrædelser, så uanset hvor grundigt man laver logningen, vil næsten alle registreringer vedrøre lovlydige borgere. Det er i øvrigt også de lovlydige borgere som betaler for denne overvågning via forhøjede priser for internetadgang. Flere steder i notatet står der godt nok at "udgifterne står i et rimeligt forhold til gevinsten for politiet", men den slags udsagn er letkøbte når man bruger andres penge.

Derudover vil de meget vidtgående forslag faktisk ikke forhindre anonym adgang til internettet når det kommer til stykket. Det hjælper ikke noget at man registrerer at den måske terroristmistænkte NN har adgang til internettet hvis man ikke kan registrere de IP adresser som NN reelt har kontakt til. Hvis NN bruger en udenlandsk VPN forbindelse der ikke logger

udgående trafik, eller bruger et anonymiserende netværk som TOR, vil politiet alene kunne se at NN bruger internettet ligesom alle andre borgere i Danmark, men hvad NN laver på internettet kan politiet ikke se. Der er i sig selv ikke noget som helst mistænkeligt ved at bruge VPN forbindelser eller TOR. Udover statens overvågning er internetbrugere udsat for en omfattende kommerciel profilering fra virksomheder som Google og Facebook, og IP-anonymisering er et af midlerne til at beskytte sig mod den slags. I Frankrig har man desuden set en øget interesse for udenlandske VPN forbindelser efter Hadopi loven med three-strikes, altså afbrydelse af internetadgangen efter tre påståede ophavsretslige krænkelser. I Danmark forventes det at en lignende ordning snart vil blive foreslået (den såkaldte "brevordning" under Kulturministeriet). Det er nemt for en eventuel terrorist at skjule sig i den store mængde af borgere som, af den ene eller den anden grund, bruger anonymisering på internettet for at beskytte deres privatliv.

Logningspakke 2 (Justitsministeriets notat) vil altså have præcist samme problem som logningspakke 1 (de nuværende regler). Der vil [stadig] være gabende huller i overvågningen, som folk kan udnytte til at skaffe sig anonym adgang til internettet. Over for det står et justitsministerium som argumenterer for at hvis vi ikke lukker de nye huller, vil udgifterne og besværet ved de eksisterende initiativer være spildte. Næste logiske skridt kan derfor være indgreb overfor brugen af udenlandske VPN forbindelser, TOR netværket og lignende mindre kendte netværk som Freenet.

Logningspakke 2 er altså næppe den sidste i rækken. Men efter vores opfattelse er det teknisk umuligt at forhindre anonym kommunikation på internettet, og forsøg på at gøre det fra statens side vil uundgåeligt medføre en indskrækning af vores frihedsrettigheder og en krænkelse af vores ret til privatliv.

IT-Politisk Forening's anbefalinger til politikerne

IT-Politisk Forening vil kraftigt advare mod samtlige forslag i Justitsministeriets notat om revision af logningsbekendtgørelsen. Der er ingen grund til at tro at de vil virke efter hensigten, og Justitsministeriet er i øvrigt ikke i stand til at fremlægge en bare marginalt overbevisende argumentation for at forslagene er "nødvendige". Det nærmeste vi kommer er løse udsagn fra PET om at målpersoner i stigende grad prøver at sløre deres kommunikation (side 11), samt de tidligere nævnte nærmest cirkulære argumenter om at udgifterne til overvågningen (som betales af borgerne, ikke af politiets budgetter) ikke står i et rimeligt forhold til udbyttet hvis der er for mange huller. Ingen ønsker terror i Danmark, men terrorproblemet kan ikke løses ved at jagte et uopnåeligt mål om at forhindre anonym kommunikation på internettet. Nogle gange får man det indtryk fra terrordebatten (eller frygten?), at hvis en gruppe af personer kan kommunikere anonymt, kan de også sprænge Nørreport Station i luften. Men det er altså ikke tilfældet. Det er nemt at kommunikere anonymt hvis man ønsker dette, men som Bruce Schneier argumenter for i denne artikel ("hvor er alle terroristerne henne?"), er det faktisk svært (heldigvis!) at gennemføre en terroraktion
http://www.schneier.com/essay-314.html

Den kraftige udvidelse af udbyderbegrebet (pligtsubjekter) medfører konkret en række praktiske og økonomiske byrder for specielt privatpersoner,

foreninger og mindre virksomheder med hotspots. Privatpersoner får forbud mod at have åbne trådløse netværk, og de forpligtes til at holde styr på hvem der bruger deres internetforbindelse (hvis gæster får adgang). Foreninger som idrætsforeninger, spejdere, ungdomsklubber, hackerspaces m.v. kommer også ind under logningsbekendtgørelsen, hvilket ikke er tilfældet i dag (qua det manglende kommercielle grundlag). Hvis disse foreninger har en kendt medlemskreds, skal de efter notatets forslag ikke selv foretage logning, men der skabes alligevel to væsentlige byrder. For det første er der en række krav til at sikre en "kendt medlemskreds" som går langt udover hvad en foreningskasserer normalt laver. For det andet skal foreningen effektivt afskærme deres trådløse netværk så kun de registrerede medlemmer kan bruge det. Mange foreninger med lukkede trådløse netværk skriver i dag adgangskoden på en seddel i foreningens lokaler, men denne metode kan ikke længere bruges hvis foreningen har gæster. Alle kan se koden og bruge netværket, inklusive gæsterne, og den går ikke. Virksomheder med hotspots (som cafeer, hoteller og campingspladser) er allerede i dag forpligtet til at foretage logning fordi de er udbydere med kommercielt grundlag, men udgifterne til denne logning til stige hvis der kommer krav om valideret personregistrering. Der er oprettelsesudgifter, løbende abonnement til det firma som skal foretage valideringen, samt transaktionsgebyrer til Nets/DanID for at bruge kreditkort og NemID.

IT-Politisk Forening har hele tiden været modstander af internetlogningen, og vi anbefaler fortsat at den bliver afskaffet så hurtigt som det er muligt. Hvis der ikke er politisk tilslutning til en fuldstændig afskaffelse af internetregistreringen på nuværende tidspunkt, bør det politiske system i det mindste overveje at afskaffe den del af overvågningen hvor der ikke eksisterer et løbende abonnementsforhold mellem internetudbyderen og brugeren, og hvor registreringen derfor ikke peger på en person men for eksempel alene på en MAC adresse. Vi har i notatet Justitsministeriets (indirekte) udsagn om at denne del af internetregistreringen reelt er værdiløs for politiet fordi den ikke peger på en person. Formentlig vil det være en meget lille del af den samlede internetregistrering som dermed ophæves, men det vil være en betydelig administrativ lempelse for eksempelvis små cafeer som tilbyder internetadgang til deres kunder.