IT-Politisk Forening
Formand Jesper Lund
2972 7719
jesper@itpol.dk

4. marts 2016

Notat om ”ny” og ”gammel” sessionslogning

Dette notat har fokus på forskellene mellem den gamle sessionslogning, som eksisterede mellem 2007 og 2014, og det nye forslag fra Rigspolitiet og Justitsministeriet.

For så vidt angår den nye sessionslogning, er notatet er baseret på en analyse af følgende materiale:

- Materiale fra Justitsministeriet, som blev præsenteret på et møde den 29. januar 2016 for en række organisationer og teleindustrien. Materialet kan ses her.
- En 7-siders notits dateret 30. januar 2016 (dok.nr. 1861555) udarbejdet af Justitsministeriet om revision af logningsreglerne, som ifølge oplysninger i medierne er distribueret til nogle partier (formentlig retsordførerne).
- Plancher udarbejdet af Rigspolitiet om sessionslogning (dateret 22. februar 2016), som er tilgængelig på Politiets hjemmeside her.

Problemer med den gamle sessionslogning

I logningsbekendtgørelsen fra 2006 kan sessionslogning udføres på to måder: enten ved registrering af sessioner[1] efter § 5, stk. 1, eller ved at registrere oplysninger om hver 500. pakke (§ 5, stk. 4). I begge tilfælde skal registreringen ske på kanten af udbyderens net (§ 5, stk. 5). Disse bestemmelser blev mellem 2004 og 2006 forhandlet mellem Justitsministeriet og teleselskaberne, bl.a. for at holde udgifterne til sessionslogning på et acceptabelt niveau (modsat den milliard-regning som der er udsigt til med det nye forslag om sessionslogning). De store teleselskaber valgte typisk hver 500. pakke af praktiske og økonomiske hensyn, mens der blandt nogle (især mindre) internetudbydere blev registreret sessioner.

Rigspolitiet har efter logningsbekendtgørelsens ikrafttræden kritiseret denne implementering af sessionslogning. Det synes at være Rigspolitiets opfattelse, at det var implementeringen af sessionslogningen, som var årsag til, at den var totalt ubrugelig for politiet i perioden 2007-2014.

Registrering af hver 500. pakke i stedet for sessioner
I medierne er registrering af hver 500. pakke blevet betegnet som stikprøver, og flere artikler skriver at kun en del af internettrafikken er blevet registreret (underforstået at de kriminelle nærmest skulle være ”uheldige”, hvis deres trafik til en bestemt server blev registreret).

Denne beskrivelse er stærkt misvisende. I realiteten er stort set enhver form for internettrafik, bortset fra meget korte dataoverførsler, blevet registreret. Ingen kriminel ville forlade sig på, at det

1 En internetsession er (lettere forenklet) den periode hvor der overføres data i en bestemt datakanal. Det forklares nærmere senere i notatet. Den officielle vejledning til logningsbekendtgørelsen af 2006 giver i øvrigt ikke en entydig definition på en ”internetsession”, og i praksis vil registreringen af sessioner være afhængig af det tekniske udstyr, som internetudbyderen anvender.

er tilfældigt om der sker registrering, specielt ikke når der eksisterer simple og effektive metoder til at undgå registrering, hvis man ønsker dette. For eksempel ved at bruge VPN eller Tor.[2]

Når der overføres data på internettet åbnes der en datakanal mellem afsender og modtager. Denne datakanal er defineret ved IP-adresser og porte for afsender og modtager, hvilket er de oplysninger som indgår i sessionslogningen. Når der overføres data sker det i små pakker af maksimalt 1500 bytes, som transporteres i denne datakanal. Det betyder at der er en masse pakker med identisk sessionslogningsinformation (samme IP-adresser og portnumre), og der skal ikke overføres ret meget information for at en af disse pakker med meget stor sandsynlighed bliver registreret (som 1:500 pakker). Og blot én registrering er nødvendig for at politiet kan se, at personen har haft kontakt til en bestemt server. Ti identiske registreringer i sessionslogningen (samme IP-adresser og portnumre) er ikke mere informative end en registrering.

Et besøg på forsiden af DRs hjemmeside (www.dr.dk) henter således omkring 1500 pakker fra DRs servere, og sandsynligheden for at en af dem bliver registreret er 95%. Efter at have læst et par artikler på www.dr.dk, er der overført endnu flere pakker, og sandsynligheden for at en af dem bliver registreret, er for alle praktiske formål 100%.

Opsummering: det kan ikke have været en reel begrænsning i den gamle sessionslogning, at der kun blev registreret information om hver 500. pakke. Ingen internettrafik af væsentlig betydning undgår registrering, fordi antallet af pakker er meget stort.

Registrering på kanten af udbyderens net

Under den gamle sessionslogning skal registrering ske ved overgangen mellem udbyderens eget net og andre net (”på kanten”). Det betyder at intern trafik, for eksempel mellem to TDC-kunder ikke bliver registreret. Det vil kun sjældent være en reel begrænsning, fordi TDC-kunder primært kommunikerer med servere uden for TDCs net.

Der er dog en bestemt situation, hvor registrering på kanten af nettet giver nogle væsentlige ulemper for den gamle sessionslogning. Det er den situation, hvor kunderne deler offentlig IP-adresse via noget der hedder NAT (network address translation). Det bruges typisk til mobilt internet, fordi der ikke er IPv4 adresser nok til alle kunder.

På kanten af udbyderens net kan internetudbyderen ikke altid skelne mellem de enkelte kunder, og hvis en sessionslogning er en sammenblanding af et par hundrede kunder, er den selvsagt ikke brugbar for politiet.

Dette problem har uden tvivl begrænset brugbarheden af den gamle sessionslogning i perioden 2007-2014, men det er samtidigt væsentligt at være opmærksom på, at dette problem kun har ramt en del af kunderne. Det skyldes to forhold:

1. Det er langt fra alle kunder, som har internetadgang med NAT og deling af IP-adresser. Hos de store teleselskaber vil kunder med faste forbindelser (som ADSL eller kabel-TV internet) typisk have deres egen IP-adresse. Her vil sessionslogningen have virket 100% efter hensigten i 2007-2014, altså uden utilsigtet sammenblanding af flere kunder.

2 I forhold til sessionslogning vil brugen af VPN (virtual private network) eller anonymiseringsnetværket Tor betyde, at den reelle destination for internettraffiken skjules. I stedet registreres trafik til en VPN server eller et Tor adgangspunkt (en såkaldt ”entry node”), hvilket politiet ikke kan bruge til noget. Det kan alene fortælle politiet, at personen bruger VPN eller Tor, men altså ikke hvad personen reelt har lavet på internettet.

2. Mindst en mobiludbyder (TDC) har implementeret en yderligere logning i den såkaldte NAT-gateway for at kunne skelne mellem de enkelte kunder i den sessionslogning, som foretages på kanten af nettet. I en notat fra Rigspolitiet af 26. marts 2014 (se her side 9) står der således

> *For så vidt angår mobillogning har TDC implementeret en logningsmodel, der identificerer den enkelte brugers mobile internetkommunikation og kæder denne information sammen med geografiske data i en såkaldt 'datastreng', der både kan anvendes til at stedfæste en persons færden alene ud fra automatiske internet-sessioner og til at identificere, hvilke andre IP-adresser personen har oprettet forbindelse til via det mobile internet. Denne mobillogningsløsning har vist sig at være et brugbart efterforskningsredskab.*

Objektivt set løser "TDC modellen" problemet med at der ikke kan skelnes mellem de enkelte kunder, når der bruges NAT (deling af IP-adresser). TDCs sessionslogning af mobil internettrafik har desuden registreret sessioner (og ikke hver 500. pakke) siden i hvert fald 2012.

Udsagnet "et brugbart efterforskningsredskab" skal nok tages med et gran salt i forhold til sessionslogning, da det er fra perioden 2007-2014, hvor Rigspolitiet som bekendt ikke kan anvise et eneste eksempel, hvor sessionslogning har givet et væsentligt bidrag til at opklare forbrydelser. Det førte til at Justitsministeren ophævede kravene om sessionslogning den 2. juni 2014.

Den nye sessionslogning, som Rigspolitiet ønsker sig, er imidlertid baseret på "TDC modellen" for den mobile internetkommunikation. Dermed er den nye sessionslogning baseret på metoder, som har været prøvet tidligere under den gamle sessionslogning.

Opsummering: registrering på kanten af udbyderens net har givet nogle begrænsninger, men det er langt fra alle kunder, som har været "ramt" af disse begrænsninger. Hvis sessionslogning virkelig var et "brugbart efterforskningsredskab" for politiet, burde der være eksempler på dette i perioden 2007-2014, enten fra kunder som har egen IP-adresse (uden deling), eller fra de mobilkunder hvor der er implementeret yderligere logning som "TDC modellen" for at løse det konkrete problem med at skelne mellem kunderne. Men som bekendt er det ikke tilfældet. Politiet har ikke kunnet bruge sessionslogningen, heller ikke i de situationer hvor sessionslogningen rent faktisk fungerede efter hensigten.

Den nye sessionslogning som Justitsministeriet vil foreslå

Med forbehold for at vi endnu ikke har set et konkret forslag fra Justitsministeriet, er det IT-Politisk Forenings forståelse at den nye sessionslogning vil være baseret på disse elementer:

1. Der skal registreres oplysninger om internetsessioner med start- og sluttidspunkt svarende til § 5, stk. 1 i den gamle logningsbekendtgørelse. Der bliver ikke mulighed for alternativt at registrere hver 500. pakke. En internetsession er (lettere forenklet) den periode hvor der overføres data i en bestemt datakanal (samme portnumre og IP-adresser).

2. Derudover skal der registreres oplysninger om antal bytes overført i hver session, og hvis der er tale om mobil internetkommunikation, skal der også registreres masteoplysninger for sessionens start- og sluttidspunkt.[3]

3 Der er angiveligt flere forskellige modeller i spil for masteoplysninger i forbindelse med internettrafik, så på dette punkt er det meget usikkert hvad Justitsministeren konkret vil foreslå i det kommende lovforslag.

3. Registreringen skal ske ”tæt på kunden”. Det betyder at intern trafik mellem f.eks. TDC-kunder skal registreres, og at sessionslogningen ikke må være en sammenblanding af flere kunder som deler IP-adresse. For mobil internetkommunikation bliver det i praksis noget, som er meget tæt på ”TDC modellen” beskrevet ovenfor.

Grundlæggende set er der efter IT-Politisk Forenings vurdering ingen substantiel forskel mellem den nye og den gamle sessionslogning.

Registrering tæt på kunden gør sessionslogning lige anvendelig for alle kunder, mens der under den gamle ordning var begrænsninger for visse kunder. Eller også skal man sige lige uanvendelig, fordi politiet ikke kunne bruge den gamle sessionslogning selv i de situationer, hvor den rent faktisk fungerede efter hensigten. Populært sagt får vi mere af det, som ikke virkede under den gamle sessionslogning.

Forskellen mellem sessioner og registrering af hver 500. pakke kan ikke betragtes som en væsentlig forskel, jf. den første afsnit i dette notat. Sessionslogning kan i begge tilfælde fortælle, om en person har haft kontakt med bestemte servere. Ikke mere end det (uddybes nedenfor i næste afsnit).

En internetsession er primært et teknisk begreb, som generelt ikke vil være sammenfaldende med f.eks. længden af en Skype samtale, eller den tid en person bruger på en hjemmeside. Internettet fungerer fundamentalt anderledes end et telefonsystem, hvor man nemt kan registrere længden af en samtale (en ”session” i telefonsystemet).

Det er heller ikke muligt ud af sessionslogning at se, om der er tale om hjemmesider eller servere, som personen aktivt har besøgt, eller om det er baggrundstrafik fra programmer/apps eller såkaldte 3. parts elementer på hjemmesider, som downloades passivt i baggrunden. Det samme gælder antal bytes overført. Omvendt er telefonopkald noget, som man aktivt foretager.

Masteoplysninger har som sådan ikke noget med sessionslogning at gøre. De kan fortælle hvor personen er henne (hvilken mobilmast der er kontakt med), men sammenkædningen med internetsessioner bidrager næppe med nogen selvstændig værdi, blandt andet fordi sessionslogning ikke er så informativ som Rigspolitiet giver indtryk af, jf. det næste afsnit om hvad man realistisk set kan uddrage af en sessionslogning.

Hvad kan man (ikke) se ud af sessionslogningen?

Rigspolitiet har givetvis ret i, at kriminelle i stigende grad bruger internettet i stedet telefonopkald og SMS beskeder. Med opkaldslister fra teleselskabet har politiet nemt kunne afdække hvem der kommunikerede med hvem.

Men når kommunikationstjenester som Skype erstatter telefonopkald, kan internetudbyderen ikke registrere hvem der kommunikerer med hvem, fordi brug af Skype blot genererer internettrafik, der ikke umiddelbart kan udskilles fra kundens øvrige internettrafik. Til gengæld registrerer udbyderen af Skype-tjenesten (Microsoft) hvem der kommunikerer med hvem, men Skype er selvfølgelig ikke underlagt dansk lov. I mange tilfælde vil dansk politi utvivlsomt kunne få adgang til disse oplysninger hos Skype/Microsoft.

Spørgsmålet er nu om sessionslogning kan levere information, som svarer til opkaldslister for almindelig telefoni? Altså hvem kommunikerer med hvem? Justitsministeriet og Rigspolitiet har i

2016 produceret notater, som prøver at give indtryk af, at dette er muligt.

Sessionslogning indeholder information om kommunikation med IP-adresser. En IP-adresse er ikke det samme som et telefonnummer, der normalt kan henføres til en person. Kun i meget specielle situationer vil internetkommunikation ske som såkaldt peer-to-peer kommunikation, dvs. direkte mellem to personers IP adresser. Ofte går kommunikationen via en central server, som måske registrerer hvem der kommunikerer med hvem (men langt fra altid).

Det er heller ikke al peer-to-peer kommunikation, som i praksis kan identificeres ud fra en sessionslog. Det skyldes at en sessionslog indeholder et meget stort antal registreringer om internettrafik fra mange forskellige programmer eller apps, og politiet vil altid lede efter den berømte nål i høstakken.

Opsummering: sessionslogning kan vise hvilke servere, som en person har kontakt med, for eksempel om personen bruger Skype. Men det vil generelt ikke være muligt ud fra sessionslogning at se hvem der har kommunikeret med hvem. Sessionslogning er generelt person-til-server, ikke person-til-person som opkaldslister for telefoni.

Dette uddybes i den resterende del af dette notat med bemærkninger til Justitsministeriets (hemmelige) 7-siders notits om nye logningsregler og Rigspolitiets plancher om sessionslogning, der er offentligt tilgængelige på internettet.

Justitsministeriets notits om revision af logningsreglerne

Justitsministeriets 7-siders notits indeholder nogle formuleringer, som er egnet til at give læseren det indtryk at sessionslogning svarer til opkaldslister for telefoni. Notitsen bruger efterforskningseksempler med telefonlogning (eksempelvis dobbeltdrabet i Tusindårsskoven), og giver derefter læseren det indtryk, at den samme type nyttige information kan opnås for internetbaseret kommunikation med sessionslogning.

På side 4 i notisen i afsnittet ”Rigspolitiets anbefalinger” beskrives det hvordan sessionslogning registrerer kontakt med IP-adresser for den enkelte slutbruger:

> *Rigspolitiet foreslår, at udbyderne fremover for hver slutbruger skal foretage logning af oplysninger om internettrafik, så det bliver muligt at fastslå, hvilke IP-adresser der er i kontakt med hinanden og omfanget af den enkelte datasession (antal bytes overført).*

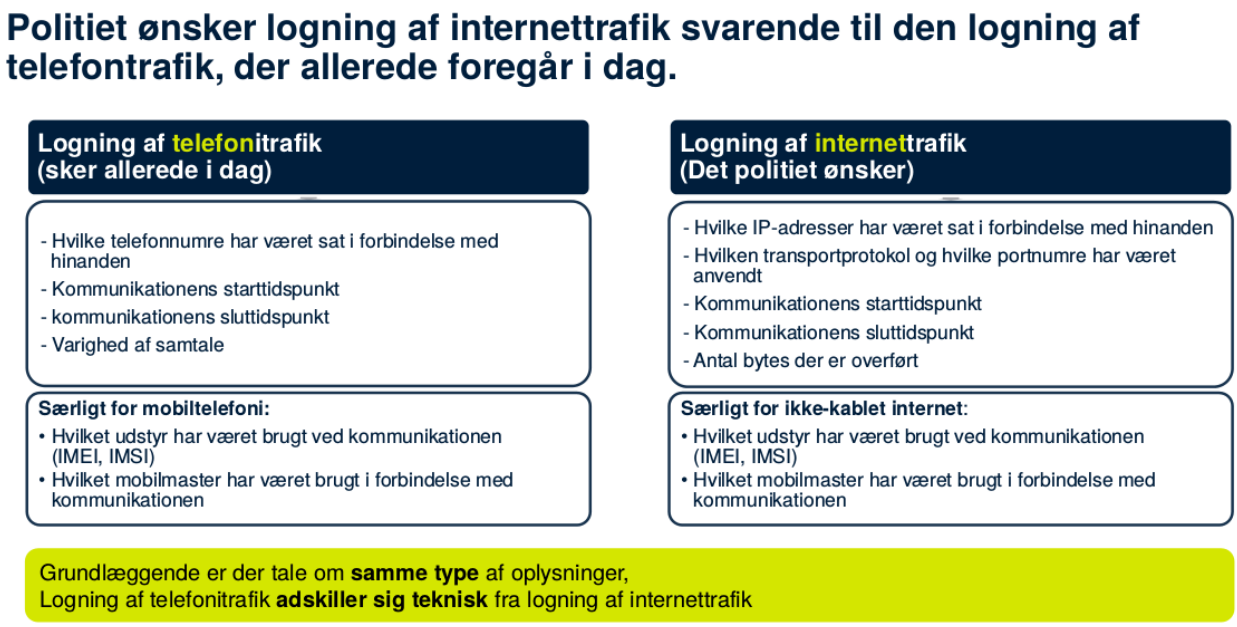
Det er en korrekt beskrivelse af sessionslogning (hvilke IP-adresser er i kontakt med hvilke IP-adresser). Men så kommer følgende påstand nederst på side 4:

> *Hermed vil pligten til at logge data om internetkommunikation – som på nuværende tidspunkt kun i meget begrænset omfang omfatter oplysninger om, hvem der har kommunikeret med hvem, i hvilket tidsrum, og hvor de var på det pågældende tidspunkt – komme til at svare til den gældende pligt til at logge data om almindelig telekommunikation.*

Det er stærkt misvisende at sige ”svare til” og sammenligne med den almindelige telelogning. Bortset fra helt specielle situationer, der i praksis vil være sjældent forekommende, er det ikke muligt ud fra sessionslogning at se hvem der kommunikerer med hvem (person-til-person).

Rigspolitiets plancher til offentligheden

Rigspolitiet har lavet et notat (plancher) med tre eksempler på brug af sessionslogning. På side 4, gengivet nedenfor, påstås det at logning af teletrafik (opkaldslister) grundlæggende er den samme type oplysninger som sessionslogning.



Som tidligere nævnt er det stærkt misvisende. Logning af teletrafik er person-til-person med et begrænset antal registreringer (opkald). Sessionslogning er for det første person-til-server bortset fra meget specielle situationer, og for det andet er det altid "nålen i høstakken", fordi sessionslogning indeholder et meget stort antal registreringer fra alle mulige typer internettrafik. Et forsigtigt skøn er at der for en almindelig bruger af en smartphone bliver registreret 10.000 sessioner per dag.[4]

Derefter følger på side 7-9 i planchesættet tre eksempler på brugen af sessionslogning. I virkelighedens verden er brug af sessionslogning at lede efter nålen i høstakken, men i eksemplerne er høstakken fjernet, og så er det nemt at se nålen. Sagt på en anden måde: sessionerne vil aldrig optræde på den simple måde, som de tre eksempler giver indtryk af.

Eksemplet på side 8 ("Eksempel 2") skal vise hvordan sessionslogning kan afsløre hvem der har kommunikeret med hvem over Skype. Det forudsætter at selve Skype samtalen sker direkte mellem de to personers IP-adresser, hvilket langt fra altid er tilfældet, og derudover forudsætter det, at man rent faktisk kan finde de Skype-relaterede sessioner i den høstak, som sessionslogningen udgør. Det vil efter IT-Politisk Forenings vurdering kun være muligt i ganske få tilfælde. Internetsessioner fra et Skype opkald vil aldrig optræde på den simple måde, som eksemplet giver udtryk for.

4 Websider består i dag generelt af mange forskellige elementer, som hentes i separate datakanaler, og ofte med flere datakanaler til samme server (IP adresse) for at optimere overførslen (dvs. forskellige source porte, og dermed forskellige sessioner). Det øger antallet af sessioner ganske kraftigt. På en computer vil læsning af en artikel på www.jp.dk generere omkring 200 sessioner. Hver gang der klikkes på et nyt artikel-link, genereres der omkring 200 nye sessioner. Hvis UDP sessioner til DNS opslag også skal logges (i dag er det typisk intern trafik, så det kommer ikke med når logning sker på kanten), vil antallet af registreringer blive endnu højere. Selv om alle DNS opslag normalt sker til samme server (destination IP-adresse), vil det ikke være samme UDP session, fordi der bruges forskellige source porte.

Derudover vil Skype/Microsoft under alle omstændigheder have registreret mere nyttige informationer om Skype opkald end hvad sessionslogningen kan fortælle, selv i den teoretiske situation som eksemplet på side 8 repræsenterer.

Sidst, men ikke mindst: hvis politiet virkelig var i stand til at bruge sessionslogning til at se hvem der kommunikerer med hvem via Skype, burde dette også have været muligt med 2007-2014 sessionslogningen. Men her mangler vi som bekendt fuldstændigt eksempler på at politiet kunne bruge sessionslogning til noget i deres efterforskning.

Opsummering om de to notater fra Justitsministeriet og Rigspolitiet

Ingen af de to notater kommer med reelle forklaringer på, hvorfor den nye sessionslogning skulle fungere bedre end den gamle sessionslogning fra 2007-2014. Reelt præsenteres vi alene for de samme begrundelser for sessionslogning, som blev brugt til at indføre den gamle sessionslogning for 10 år siden. Den sessionslogning som ikke virkede, og som derfor blev afskaffet af Justitsministeren i 2014.