Elektronisk Forpost Norge
Medlem av EDRi, European Digital Rights

Forsvarsdepartementet
Via departementets høringsportal

11. februar 2019

Høringssvar - Ny lov om Etterretningstjenesten

Elektronisk Forpost Norge (EFN) viser til Forsvarsdepartementets høring av 21. november 2018 med forslag til ny lov om Etterretningstjenesten.

Som følge av lovforslagets omfang og kompleksitet, og den relativt korte høringsfristen, er det begrenset hvilke temar vi har hatt mulighet til å gå inn i.

Deler av høringsutkastet er utarbeidet i samarbeid med Den norske dataforening - IT-politisk råd, som avgir egen høringsuttalelse.

Vedlagt er vår høringsuttalelse til forslag om ny lov om Etterretningstjenesten.

Med vennlig hilsen

Bjørn Remseth
nestleder EFN

Britt Lysaa
Høringsansvarlig

Elektronisk Forpost Norge
Pb 27 Vålerenga, 0626 OSLO E-Post: horing@efn.no Tlf. 996 24 544

Høringsuttalelse fra EFN - ny lov om Etterretningstjenesten

EFN har forståelse for av at det er behov for en oppdatert og mer informativ lov om Etterretningstjenesten. Gjennom Grunnloven § 102, det alminnelige legalitetsprinsippet og Den europeiske menneskerettskonvensjon artikkel 8 er Norge forpliktet til å ha klare, forutsigbare og tilgjengelige lovregler for myndighetenes inngrep i den enkeltes rett til privatliv.
Den gjeldende loven er svært overordnet, og bærer preg av å være en rammelovgivning. Deler av den eksisterende praksis som beskrives i høringsnotatet, og i EOS-utvalgets særskilte melding om rettsgrunnlaget for Etterretningstjenestens overvåkningsvirksomhet[1], slik vi ser det, tangerer grensen[2] av hva gjeldende lovgivning tillater. En slik utvikling er naturlig når loven over tid har blitt fritt tolket og praktisert i hemmelighet.

Ved ny lovgivning er det særdeles viktig at lovgiver har et bevisst forhold til konsekvensene av de fullmakter som gis til Etterretningstjenesten.
Uten klart definert formål, klart definerte formålsbegrensninger, entydige presiseringer i loven, kontroll av og innsyn i praktiseringen, som alle er betingelser for å kunne ha en åpen offentlig debatt - er det sannsynlig at også denne over tid vil bli tolket utvidende, og gjerne langt utover hva som var lovgivers intensjon.

Vi finner at lovforslaget bryter med menneskerettslige forpliktelser etter EMK og Grunnloven, og er imot teknologisk masseovervåking gjennom «tilrettelagt innhenting».

Innhold

1 https://eos-utvalget.no/norsk/saerskilte_meldinger/content_1/text_1401199513555/1474459575882/eos_s_rskilt_melding_norsk_web.pdf
2 https://www.dagbladet.no/nyheter/forsvarsministeren-skyver-oss-foran-seg-sier-eldbjorg-lower/69572325

Digitalt Grenseforsvar - Tilrettelagt Innhenting

Lyse II-utvalget beskrev «Digitalt Grenseforsvar» og innhenting av data i transitt over grensekryssende fiberkabler før kryptering på link-laget[3] foretas.
Lovforslaget omtaler et skille mellom kommunikasjon som krysser norske grenser, og kommunikasjon som fullt og helt foregår i Norge. En slik distinksjon er meningsløs når kommunikasjonen foregår over internett, siden selv alt fra hjemmelekser til kommunikasjon med forvaltningen i dag rutinemessig tar en sving innom minst ett datasenter eller ruter plassert utenfor landets grenser.
I realiteten vil bortimot all elektronisk kommunikasjon i dag passere landegrensen, enten på grunn av ruting, fordi en bruker en skytjeneste e.l., eller fordi programmene en bruker har interne moduler som lenker mot data utenfor landegrensen. Majoriteten av grensekryssende datastrømmer vil være initiert av personer i Norge som nytter internett til ordinære, daglige gjøremål.

Ikke-målrettet masseovervåking med data innhentet i bulk kommer også med en høy kostnad, noe vi vil kommentere videre i dette høringssvaret.

Tilrettelegging for aksess

I det foreliggende forslaget er tilretteleggingsplikten gjort helt generell og omfatter alle tilbydere av elektroniske kommunikasjonstjenester[4]. Fra å være begrenset til de fysiske kablene som krysser norske grenser beskriver man nå et "sugerør" inn i det norske kjernenettet og til potensielt alle tjenesteleverandører og deres kunder. Forslaget kan forstås som at Etterretningstjenesten skal gis tilnærmet fri tilgang til tilbydernes systemer. Dette forslaget fremstår derfor som vesentlig mer omfattende enn det som ble drøftet og anbefalt av Lysne II-utvalgets rapport. Forslaget strekker seg også mye lenger enn hva en finner i Sverige, hvor kun fiber*eiere* berøres av FRA-loven.

§ 7-2, d)

> **"***sørge for tilgang til kommunikasjon uten hinder av linkkryptering eller lignende kryptering som tilbyder kontrollerer***"**.

Dette er svært generalisert og omfatter alle tilbydere av elektroniske kommunikasjonstjenester og alle varianter av krypteringstjenester disse nytter eller tilbyr sine kunder.
L2 link-kryptering er et konkret begrep, uavhengig hvilke krypteringsalgoritmer som er nyttet så er dette begrenset til kryptering på L2 link-nivået.
Derimot «*lignende kryptering som tilbyder kontrollerer*" kan omfatte alle varianter av kryptering og på alle nivåer i nettverket, helt opp til sluttbruker av tjenester, og kalles generelt en «bakdør».

Mens Lysne-II foreslo tilretteleggingsplikt for eiere/tilbydere av fiberkabler som har direkte tilknytning til grensekryssende kabel, går høringsnotatet flere skritt videre, og gir Etterretningstjenesten tilnærmet fri tilgang til tilbyders systemer. Her åpnes for uante muligheter som vanskelig lar seg kontrollere.Forslaget strekker seg også mye lenger enn hva en finner i Sverige, hvor kun fiber*eiere* berøres av FRA-loven.

Dersom formålet er eksplisitt grensekryssende datastrømmer i transitt over fiberkabel forventes at kun de som eier fiberkabel pålegges en tilretteleggingsplikt. Om en har ment noe annet så må det spesifiseres slik at loven kan forstås.

3 L2-kryptering, lag 2 i OSI-modellen
4 høringsnotatet punkt 11.15.2 og 11.15.3

En lovtekst må være presis og entydig for det formålet den er ment å dekke, som eksempelvis

> "sørge for tilgang til kommunikasjon uten hinder av fibereierens L2 link-nivå kryptering for fiber som har direkte forbindelse mot grensekryssende kabel, uavhengig hvilke krypteringsalgoritmer fibereieren selv nytter for denne fiberen".

Alt annet enn slik entydig spesifisering vedrører bedrifters og kunders sikkerhet for ende-til-ende kommunikasjon - og vil også inkludere kabler internt i landet som ikke har direkte tilknytning til knutepunkter mot grensekryssende fiberkabler.

Det er vanskelig å se hva «tilpasset tilrettelegging» er ment å omfatte, utover å generere høystakker. Det er også vanskelig å se om eller hvordan kontroll og ettersyn er tenkt.

Om kryptering spesielt

Krypteringsdebatten fra 1990 tallet har kommet tilbake de siste årene. Politi, sikkerhets- og etterretningstjenester ønsker tilgang til krypteringsnøkler eller ukrypterte data. Samtidig er sterk kryptering vitalt avgjørende for sikkerheten og tilliten til internett som transportmedium for kommunikasjon. Det tok flere år å bygge opp denne tilliten via utvikling av gode produkter for kryptering som skal og *må* sikre den konfidensialitet som *må* være på plass for å nytte internett kommersielt. Temaet er komplekst men en bør ta lærdom fra historien[5]. Vi finner det oppsiktsvekkende at norske myndigheter etter et par siders drøfting i forslagets punkt 11.15 foreslår å gi tilbyderne av kommunikasjonstjenester en slik vidtgående tilretteleggingsplikt.
Ved å setter likhetstegn mellom L2 link-kryptering og *all annen kryptering som tilbyder kontrollerer,* skapes det en stor usikkerhet om hva som er ment. Om forslaget skulle passere i slik form vil det være et stort feilgrep.

Kryptering er viktig for web-basert handel eller informasjonstjenester, nettbasert betaling, virtuelle private nett og andre teknologier som har formål å sikre konfidensialitet og sikkerhet generelt, inkludert integritet for passord og andre autentifiseringsbevis som nyttes. En bakdør til kryptering vil medføre at den eller de krypteringsmetoder det gis bakdør til, vil ansees lite nyttige og i verste fall ubrukelige. Som eksempel kan nevnes at da det ble kjent at en spesiell krypteringsmodul (Dual_EC_DRBG[6]) hadde en bakdør, ble dette en kostbar affære for industri som nyttet dette i sine krypteringsprodukter. Tilsvarende for "ghosts", som er bakdør rett inn i en kommunikasjonstjeneste slik at tredjepart kan stilltiende "delta" i kommunikasjonen.

Generelle og vage definisjoner i lovteksten gir også usikkerhet om hvorvidt Etterretningstjenestenen kan få aksess til krypteringsnøkler (escrow key) for elektroniske identitetsløsninger fra tilbydere av sådanne løsninger. En nasjonal eID kan fort virke lite tiltrekkende, og i verste fall verdiløs om en vet eller mistenker at tredjepart kan bruke ens private krypteringsnøkkel og derved ens digitale identitet for dekryptering eller signering. Tilsvarende for digitale sertifikater som benyttes for kryptert aksess til web (https) eller mellom e-post servere. Eksemplene er mange, men samtlige varianter av bakdører svekker tillit til tjenestetilbyder og kan også svekke innovasjon og utvikling.
L2-link kryptering nyttes også innen eller mellom bedrifter for å utveksle spesielt sensitive data. Kryptering på L2-link nivå er mere egnet for effektiv og hurtig transport, mens kryptering på høyere nivå er mere ressurskrevende (båndbredde og CPU/datakraft).

5 Doomed to repeat history? Lessons from the Crypto Wars of the 1990s https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/Crypto%20Wars_ReDo.7cb491837ac541709797bdf868d37f52.pdf
6 Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generation) NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard https://www.scientificamerican.com/article/nsa-nist-encryption-scandal/

Tilrettelagte bakdører har også et juridisk aspekt.
Det juridiske ansvaret for datalekkasje, innbrudd, hacking eller lignende, som forårsakes av tilrettelegging eller behandling av innhentede data er ikke nevnt.
Hvem har ansvaret dersom et av grensesnittene mellom tilbyders og Etterretningstjenestens systemer skulle lekke informasjon til en tredjepart. Slike situasjoner er ikke helt ukjente, blant annet har det vært flere mediesaker om at lovlig avlyttingsutstyr plassert hos tilbyder har lekket informasjon til fremmed etterretning.
Ved å tilrettelegge for bakdør, åpner en også for de en ikke vil ha inn. Det må være klart forstått av lovgiver at alle varianter av bakdører forvitrer sikkerheten til den en er forpliktet å beskytte.

Automatiserte søk og behandling av data i bulk

Bearbeiding av slike datamengder som beskrives i forslaget kan ikke gjøres manuelt.
For å tilrettelegge for søk i slike ustrukturerte datamengder som bulkinnsamling gir, bruker man automatiserte teknikker, som kan være ulike former for maskinlæring, automatiserte analyser og mining av data. Med "tilrettelagt innhenting" vil det være tale om svært store datamengder om personers kommunikasjon, vaner, handlingsmønstre, preferanser, vennekrets, osv. Den teknologiske utviklingen for bearbeidelse av store datamengder går fort, og det er liten grunn til å tro at ikke Etterretningstjenesten vil nyttiggjøre seg av den til enhver tid tilgjengelige teknologi som foreligger.
Men dette reiser prinsipielle og etiske spørsmål, som ikke er belyst i høringsnotatet[7,8]. AI eller automatiserte algoritmestyrte beslutningsprosesser kan ha innbakte mangelfulle og udokumenterte prosesser, som kan gi utilsiktet skjevhet i resultatene ("bias"). Videre bearbeidelser kan gjerne forsterke innebakte stereotyper. Prediktive analyser er bare et (kontroversielt) eksempel på dette.

Fra et kontrollperspektiv vil en løsning basert på automatisering og maskinlæring skille seg vesentlig fra et regime hvor søk og analyse gjøres uten slike teknikker. Dette problematiseres ikke i høringsnotatet.
Det er vanskelig å kontrollere hva, hvordan og hvorfor, og på hvilket grunnlag dataene er blitt sortert, filtrert bort og/eller behandlet og "tagget", underveis i prosessen - eller hvorfra dataene faktisk har sin opprinnelse.
Det er heller ikke oppgitt om kildekoden er tilgjengelig for kontroll eller hvordan EOS-utvalget skal kunne kontrollere dette.

Korttidslageret

Innhenting av data i bulk vil gi store datamengder selv når det samles inn i korte tidsintervaller[9].
I realiteten kan enhver nettbruker få hele eller deler av sin daglige aktivitet fanget opp i løpet av et døgn. Dette vil være personlig, fortrolig, sensitiv og/eller konfidensiell informasjon som innhentes, og som maskinelt bearbeides og analyseres for videre lagring i et "metadatalager"[10].
Over en periode av to uker kan en teoretisk tilrettelegge for profiler/kategorisering av bortimot hele befolkningen via teknikker for indeksering og mining av data.

7 The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation
https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf
8 Automating Society - Taking Stock of Automated Decision-Making in the EU
https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf
9 Moderne kabler har høy kapasitet (160 Tbp, terabits per sekund og pr. kabel)
10 Eksempelvis må en e-post åpnes for å hente ut metadata fra brevets innhold.

Metadatalageret

Begrepet “metadata” i kontekst av data innhentet i bulk for videre bearbeidelse, kan kategoriseres som indeksering, fingerprinting og tagging av data avledet av innhold. Begrepet er teknologisk riktig, men representerer noe annet og mere omfattende enn når det samme begrepet har blitt brukt om for eksempel trafikkdata fra telekommunikasjon. Både mengden og typene metadata innhentet i bulk vil langt overgå hva det var tale om å pålegge lagret gjennom datalagringsdirektivet. Denne type metadata er ment for å kunne flette sammen biter av data med andre biter av data, for å kunne komplettere bildet av en person.

Et søk i dette lageret, er i realiteten et sett av bakgrunnsprosesser, som her kan hente ut 15 måneders livshistorie. Metadatalageret er langt mere dyptinngripende enn de aller fleste har begrep om eller kan forstå uten å få dette visualisert. Dette har aldri vært debattert i offentligheten. Det er uvisst hvordan domstol skal kunne få grunnlaget for å vurdere hvorvidt søk her er tilstrekkelig legitimt da det verken foreligger mistanke om kriminalitet eller lovbrudd.

Langtidslageret

Ved tilslag på et «målrettet søk», vil dataene tilknyttet personen (eller hendelsen) bli lagret i 15 år eller mere. Videre innhenting og akkumulering av data relatert til dette målobjektet vil bli komplettert med data fra alle tilgjengelige kilder, inkludert fremtidig datainnhenting i bulk og/eller datastrømmer dedikert objektet, inklusive innholdsdata som da vil langstidlagres.
For den som blir utsatt for dette, så intensiveres overvåking videre framover. I flg. Lysne II kan også data innhentet fra utplasserte sensorer i samfunnet, for å utfylle bildet.

Data kombineres med oppkjøpte dataprofiler eller data fra åpne kilder (sosiale media, blogger, oppkjøpte personprofiler, o.l.) og vil ha varierende og tilfeldig kvalitet. Datainnsamlingen kan utvides med søk fra (2 eller kanskje flere lag fra) den elektroniske vennekretsen – som medfører at søk relatert til en enkelt person fort ender med “målrettet søk” mot flere tusen personer[11].

Domstolen blir forelagt en enkel sak, uten viten om eller kontroll av de mange, kanskje tusentalls andre, som automatisk følger med i prosessen. Dette er detaljerte og sensitive opplysninger om et ukjent antall borgere. Uten av disse er mistenkt for noe eller har gjort annet enn å få sitt navn eksponert i en tilfeldig kontekst.

Kort oppsummert om datainnhenting i bulk

Datastrømmer innhentes i bulk, filtreres, sorteres og bearbeides for å oppnå detaljerte datasett for søk etter relevante mål/personer. Ved tilslag vil målsøk kunne utvides og vokse til store databaser med detaljerte opplysninger om hele befolkningen.

Under dette regimet som her foreslås, er ingen garantert beskyttelse mot statlig innsyn i privat elektroniske kommunikasjon. Dette er også etisk betenkelig.
Retten til privat og fortrolig kommunikasjon, uten statlig inngrep og avlytting er en betingelse for å sikre rettstaten, demokratiet og innbyggernes frihet. Dette regimet er særdeles intrusivt[12] og kan vanskelig sees som “nødvendig for nasjonens sikkerhet”, men er snarere et overgrep mot den

11 Datatilsynet var konservativ da de henviste til 25.000 – mange av oss finner høyere tall ved å gjennomgå utvidet “vennekrets”.
12 In Defense of Bulk Surveillance: It Works https://www.lawfareblog.com/defense-bulk-surveillance-it-works

friheten som staten skal sikre individet.

Lysne II viser også til hvordan data innhentet ved DFG/TI kan kompletteres med data innhentet fra utplasserte sensorer lokalt i nettverk og virksomheter. En lokal sensor vil, avhengig av plassering, få tilgang til intern trafikk i virksomheten og derfor mulighet til å inspisere enkelte typer kryptert kommunikasjon[13]. En slik sensor som sniffer nettet kan derfor potensielt kunne innhente ukryptert informasjon fra en bedrifts nettverk, som ellers ikke er tilgjengelig utenfor bedriftens nettverk.

Regimet DGF/TI representerer en ubegrenset blankofullmakt for ikke-målrettet teknologisk masseovervåking og lagring av befolkningens personlige kommunikasjon, med formål å bygge "en høystakk"[14] for utenlandsetterrettning.

Helhetsinntrykk og implikasjoner for personvernet

Konseptet som «tilrettelagt innhenting» utgjør, er bortimot et komplett overvåkningssystem, med *særdeles* dyp inngripen i personvernet og den private sfære. Høringsforslaget anerkjenner også at dette er problematisk, men argumenterer for at rikets sikkerhet potensielt vil trues av retten til å ha en privat sfære og fortrolig kommunikasjon uten statlig inntrengning.

Fra høringsdokumentet, 4.2.2.1 :

Nasjonalstatens mest grunnleggende oppgave er å ivareta statens suverenitet og innbyggernes sikkerhet. Grunnleggende verdier for vår stat og statsform – å sikre demokratiet, rettsstaten og menneskerettighetene – er nedfelt i Grunnloven § 2. Det overordnede formålet med Etterretningstjenestens virksomhet er å bidra til å verne om Norge som en fri og selvstendig stat, som nettopp er en forutsetning for at vi kan ha en fungerende rettsstat og et demokratisk styresett. Borgerne har således en berettiget forventning om at staten gjør det den kan for å ivareta både statens eksistens og handlefrihet og borgernes sikkerhet. Ivaretakelsen av disse forpliktelsene kan måtte balanseres mot andre rettigheter borgerne har.

Grunnloven § 2, som det vises til, sier følgende "*Verdigrunnlaget forblir vår kristne og humanistiske arv. Denne Grunnlov skal sikre demokratiet, rettsstaten og menneskerettighetene.*"

Den manglende proporsjonaliteten i bruk av militær teknologi mot det sivile samfunnet, kan ikke sies å trygge demokratiet, rettsstaten, menneskerettighetene eller borgernes friheter. En rettsstat skal trygge individet mot statlig makt, mens det som her beskrives, er en grov maktforskyvning. Det foreslåtte regimet for slik massiv overvåkning kan ikke forsvares som "strictly necessary for safeguarding democratic institutions".

Organisasjonen Freedomhouse[15] som overvåker demokrati og frihet verden over, utgir regelmessig rapporter fra sine funn. Rapporten for 2018 viser at myndigheter verden over iverksetter tiltak for å få kontroll over befolkningens data, med den følge at tilliten til internettet svekkes og tilsvarende svekkes demokratiets grunnlag.

Kildevern og yrkesgrupper med lovpålagte og/eller behov for spesielt vern

Dataene som flyter inn i dette regimet kommer fra samtaler mellom advokat og klient, lege og

13 webbasert (HTTPS) nevnes, men annet kan være relevant, avhengig av konfigurasjon og nettets topologi.
14 Departementet skriver "dersom Etterretningstjenesten skal kunne finne nålen, må den ha tilgang til høystakken."
15 https://freedomhouse.org/content/our-history

pasient, sensitive helsedata, intime kjærester, journalist og dennes kilde, familiemedlemmer, naboer, forskjellige parter innen en bedrift eller mellom bedrifter, barn og lærere, osv. Der er ingen grenser, da all elektronisk kommunikasjon omfattes.
Hvordan disse skal skilles fra hverandre, er ikke vektlagt. Vi leser vage hentydninger til at også disse som har lovpålagt taushetsplikt eller har garantert konfidensialitet kan være terrorister eller ha sådanne forbindelser. Teoretisk er dette selvsagt mulig, men det er totalt ute av proporsjoner å bruke millitær overvåkningsteknologi her.

Der er dessverre mange eksempler på overvåking av journalister i vestlige, demokratiske land. Et slikt overvåkingsregime truer samfunnsoppdraget journalister har, og truer derved også demokratiet. Deres oppdrag er blandt annet å avdekke maktmisbruk, som er viktig for avdekking av korrupsjon og kriminalitet i samfunnet.
Rollen til undersøkende journalister vanskeliggjøres eller forhindres via overvåkingsregimer. Pew Research[16] viser at 71% av amerikanske reportere som dekker nasjonal sikkerhet, mener deres data overvåkes, og GCHQ[17] har akkumulert e-poster til journalister i kjente media.
Vi trenger ikke se utenfor landet for å finne at en tidligere forsvarsminister beordret sikkerhetstjenesten til å spore kilden bak en avisartikkel som kritiserte forsvaret[18]. Riktignok håndterte den norske sikkerhetstjenesten dette på en etisk og ryddig måte, men problematikken er så alvorlig at den truer de grunnleggende verdier i det samfunnet som staten skal beskytte.
I dette regimet som her foreslås er kildevernet kraftig redusert.

Er tilrettelagt innhenting egnet til å skape en negativ nedkjølingseffekt?

Det korte svaret er Ja. I høy grad.
Et lengre svaret er Ja, og det er også egnet til å forvitre demokratiet og bryte ned den tilliten som vi alle setter svært høyt.

En vil gjøre andre valg når en er under konstant overvåking.
Der har vært mange rapporter om "chilling effect" de siste årene. Blandt annet kan nevnes *Internet surveillance, regulation, and chilling effects online: a comparative case study*, fra *Internet Policy Review* fra mai 2017[19] som viser til at statlig oversyn og overvåking har en nedkjølende effekt, med utslag i manglende samfunnsdeltakelse, endret oppførsel med selvsensur og høy grad av konformitet.
I rapportens sammendrag står det:

> *With internet regulation and censorship on the rise, states increasingly engaging in online surveillance, and state cyber-policing capabilities rapidly evolving globally, concerns about regulatory "chilling effects" online—the idea that laws, regulations, or state surveillance can deter people from exercising their freedoms or engaging in legal activities on the internet have taken on greater urgency and public importance. But just as notions of "chilling effects" are not new, neither is skepticism about their legal, theoretical, and empirical basis; in fact, the concept remains largely un-interrogated with significant gaps in understanding, particularly with respect to chilling effects online. This work helps fill this void with a first-of-its-kind online survey that examines multiple dimensions of chilling effects online by comparing and analyzing responses to hypothetical scenarios involving different kinds of regulatory actions—including an anti-cyberbullying law,*

16 Most of America's investigative journalists believe their gov. has spied on them, according to a Pew Research Centre study. http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/
17 GCHQ captured emails of journalists from top international media https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post
18https://www.vg.no/nyheter/innenriks/i/w7zj1/stroem-erichsen-faar-kritikk-etter-kildejakt
19 Internet surveillance, regulation, and chilling effects online: a comparative case study https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case

> *public/private sector surveillance, and an online regulatory scheme, based on the Digital Millennium Copyright Act (DMCA), enforced through personally received legal threats/notices. The results suggest not only the existence and significance of regulatory chilling effects online across these different scenarios but also evidence a differential impact—with personally received legal notices and* ***government surveillance online consistently having the greatest chilling effect on people's activities online****—and certain online activities like speech, search, and personal sharing also impacted differently.*

Under det foreslåtte regimet kan ingen lengre forutsette at deres kommunikasjon har den konfidensialitet personlig kommunikasjon rettmessig skal ha. Dette regimet griper dypt inn i individets integritet og den personlige sfære. Uavhengig av hva lovgiver ønsker å kalle regimet, så er dette teknisk tilrettelagt elektronisk overvåkning av befolkningens digitale aktiviteter, og hvor en bruker militær teknologi for å kunne trenge dypest mulig inn i individets private sfære.
En tilsvarende massiv overvåkning av befolkningens *fysiske* aktiviteter kunne ha visualisert et inntrykk av et autoritært regime.

Det er av absolutt nødvendighet at retten til privat sfære respekteres og vernes om for å kunne ivareta et robust demokrati. Individets frihet og retten til en privat sfære uten statlig inntrenging eller monitorering, er vitalt viktig og en nødvendighet for tillit mellom mennesker og tillit til statlige myndigheter.

En kan forvente at skepsis mot bruk av statlige elektroniske tjenester kan øke med bevisstheten om teknologisk overvåking. En trenger kun integrere elektronisk identitet med ansiktsbiometri og fingeravtrykk for å nærme seg Kina's «digitale agenda»[20]. Nedkjølingseffekten har nådd et slikt nivå i Kina at det er vanskelig å *ikke* se eller forstå hva maktovergripende overvåking gjør med et samfunn over litt tid. I kollegial samtale med en kineser detekterer en fort at dette er temaer en aldri snakker om. Statlig overvåking fungerer som sosial kontroll, og forvitrer de verdiene som staten skal verne om.
Som nevnt, ikke-målrettet masseovervåking med data innhentet i bulk kommer med en høy kostnad[21].

Lagring av IP adresse

Høringsdokumentet skriver det er igangsatt utredning av generell lagringsplikt for IP adresser som et virkemiddel mot kriminalitet og overgrep mot barn. Dette har liten sammenheng med militær etterretning[22,23], men viser også hvor overlappende og integrert DGF/TI-datalagringen er tiltenkt å omfatte.
Operatører nytter teknologi hvor en har utviklet nye metoder[24] for å utnytte IP(v4) adresse-feltet maksimalt. For å kunne lagre en nettbrukers IP adresse må derfor også denne brukers *detaljerte* aktiviteter lagres. Dette overgår langt hva som ble foreslått med Datalagringsdirektivet[25] og sorterer også under datalagring (versus etterretning mot utlandet).
Høringsdokumentet omtaler også IP-adresser som "ikke-personopplysning", men her vil EU-

20 Grenseløs – Digitalt diktatur https://tv.nrk.no/serie/grenseloes/2019/NNFA44000119
21 https://www.lawfareblog.com/defense-bulk-surveillance-it-works
22 Justisministeren vil lagre IP-adressen din i seks måneder https://www.vg.no/nyheter/innenriks/i/Wpk5G/justisministeren-vil-lagre-ip-adressen-din-i-seks-maaneder
23 Dark Room fikk ministeren til å gå for utvidet IP-lagring
https://www.nrk.no/hordaland/justisministeren-vil-innfore-utvidet-lagring-av-ip-adresser-etter-onske-fra-dark-room-1.13537868
24 Carrier Grade NAT (CGNAT) :
SSAC Advisory on the Changing Nature of IPv4 Address Semantics https://www.icann.org/en/system/files/files/sac-079-en.pdf
25 Digital Rights Ireland and Seitlinger and Others
https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

lovgivning si motsatt[26]. Dersom lagring av IP-adresser tenkes pakket inn under «tilretteleggingsplikt» så må dette gjøres kjent.

Formålsutglidning

I høringsdokumentet oppgis hovedhensynene bak lovrevisjonen å være kodifisering, rettslig forankring av Etterretningstjenestens allerede eksisterende, dvs. nåværende virksomhet og metodebruk, samt utvidelse av denne praksisen til å også omfatte aksess til datastrømmer i transitt over grensekryssende kabler fra nettilbydere og andre digitale tjenestetilbydere.

DGF/TI beskrives som Etterretningstjenestens verktøy mot utenlandske mål, men grensene mellom millitære og sivile oppgaver er vage.
Det er positivt at loven forbyr å nytte data fra DGF/TI i kriminell etterforskning, men lovforslagets unntak og henvisninger vanskeliggjør oversikt over hvordan disse data faktisk kan eller vil bli nyttet i fremtiden.

Utglidningspotensialet er overhengende høyt, og overskuddsinformasjon kan deles med andre offentlige myndigheter under visse vilkår.
En kan få forståelse av at formålsutglidningen allerede er påtenkt når en leser fra Lysne-II (side 77):

VDI-sensorene kommer til kort både hva angår utbredelse i antall og i forhold til bredden av virksomheter som er dekket. Det foreslås tiltak på området. I tillegg til dette fører bl.a. økt bruk av kryptering til et behov for å komme tettere inn på sluttbrukerne (virksomhetene) med de lokale sensorene.

Grunnet krypteringsutviklingen er det imidlertid grunn til å anta et denne typen analyse vil bli mer utfordrende å gjennomføre med DGF-data alene i fremtiden. Det er derfor viktig å fremheve at slik analyse vil måtte kompletteres med data fra E-tjenestens øvrige sensorer og kapabiliteter. I tillegg vil analysen kunne støttes med informasjon fra eventuelle lokale sensorer og samarbeid med berørte virksomheter for å kompensere for noe av krypteringsutfordringen. I den utstrekning DGF vil bli påvirket av krypterings-utfordringer i fremtiden, vil dette således i stor grad kunne kompenseres med samspill med tjenestens øvrige kapabiliteter og data fra lokale sensorer, samt samarbeid med NSM, PST og den aktuelle virksomheten.

E-tjenesten kan i dag ofte ikke dele graderte signaturer mottatt fra partnere. Egenutviklede signaturer kan i større grad deles nasjonalt. Dette vil igjen gi grunnlag for langt mer målrettet bruk av overvåkings- og deteksjons-ressursene i de nasjonale nettene.

Her må loven reflektere entydig at data som innhentes fra sensorer fra bedrifters interne nettverk eller fra offentlige internett, ikke skal deles med DGF/TI. Samfunnet må informeres om hvilken grad de er overvåket, hvilke data som lagres om dem, hvordan dataene brukes og hvordan de får innsyn i disse (egne) data. DGF/TI regimet, som akkumulerer data fra, til og om Norges befolkning, treffer midt i kjerneoppgavene til PST og Kripos. Lysne-II nevner en del om fordeler ved at Etterrettningstjenesten, PST og Kripos kan utfylle hverandre ved å dele hverandres data. Det er naturlig at disse har noen felles og overlappende interesser. Annonseringen av cybersikkerhetssenteret[27] viser også hvor nært tilknyttet og infiltrert disse gruppene er.

Mange scenarier er mulige, vi gir bare de mest opplagte fra de vi spør oss selv:

26 The GDPR states that IP addresses should be considered personal data as it enters the scope of ‘online identifiers’. Etter personopplysningsloven er IP-adresse å anse som en personopplysning.
http://heim.ifi.uio.no/gisle/local/law/gdpr_norsk.html#ftp030
27 Cybersikkerhetssenteret Kripos, PST, Etterretningstjenesten, m.fl. https://nsm.stat.no/blogg/ncss-lansering/

Er stortinget prinsippfast nok til å fortsette å si nei?
Hver gang?

Kripos, PST:

> "Hvorfor skal forsvarets E-tjeneste beskytte pedofile, voldtektsforbrytere, narkosmuglere og mordere?"

I nær fremtid:

> "Det er samfunnsnyttig og ytterst nødvendig at vi linker databasen for de nye, ansikt-/fingerprint biometriske, nasjonale eID-dataene mot DGF/TI. Vi må beskytte borgerne mot ID-tyveri."

Deretter:

> "DGF/TI har vært helt essensielt for vårt arbeid, men på grunn av utstrakt bruk av kryptografi hos våre motstandere må vi nå ha utvidede fullmakter til dataavlesning og regulering av kryptografi"

I bakgrunnen, på bakrommet:

> "For å sikre viktig infrastruktur må strømnetteiere få tilretteleggingsplikt for innhenting av data fra smarte strømmålere".

Deling av informasjon med fremmede stater

Det er fullt forståelig at Etterretningstjenesten må ha konfidensialitet vedrørende kjerneområdet sitt, etterretning mot utlandet.

Det vil være ønskelig om EOS-utvalget har innsyn i hvilke informasjon som deles, i hvilket omfang og hvordan disse dataene behandles.
Tilsvarende bør det være åpenhet om hvilke land en har utvekslingsavtaler med.

Vi er bekymret for faren gjensidig overvåkning av hverandres innbyggere utgjør. Med den grenseoverskridende kommunikasjon vi har i dag, står man i fare for å errodere en hver form for rett til privatliv, hvis man ikke legger inn beskyttelsesmekanismer mot dette.

Cyberspionasje

§ 4-3 (Forbud mot industrispionasje) indikerer at en er bevisst at det foreslåtte DGF/TI-regimet kan potensielt gjøre spionasje enklere.
Ethvert forsøk på å åpne bakdører til krypterte data vil lede til svekkelse av den sikkerhet bedrifter er nødt til å ha for å kunne gjøre forretninger over internett.
For bedrifter er datasikkerhet og ende-til-ende kryptering beskyttelse mot uønsket innsyn og spionasje. Bakdører for kryptering eller "ghost", sorte bokser, sniffere, o.l. er ikke tillitsvekkende.
En bør heller ikke fremstille DGF/TI som beskyttelse mot datainnbrudd eller hacking, for dette er uriktig og kan også lede enkelte bedrifter til å tro at implementering av faktisk datasikkerhet da blir mindre viktig. Det kan også lede politikere og andre beslutningstakere til ta feile avgjørelser vedrørende elektronisk sikkerhet.
I vår profesjon har vi sett både datainnbrudd, cyberspionasje og resultatene av disse. Metodene skal vi ikke gå inn på, men de er mangfoldige og ofte forårsaket fra hendelser eller uforsiktighet på innsiden av bedriften.

Den beste metoden for forebygging er å øke bevisstheten om sikkerhet og konsekvensene som følger av manglende sikkerhet implementert.

Om kontroll med Etterretningstjenestens metodebruk

Fra Lysne-II side 51*:*
E-tjenesten har intet ønske om å drive masseovervåkning. En må likevel legge til grunn at det utstyret som eventuelt vil brukes til DGF, vil ha teknologisk kapasitet til å gjøre nettopp dette. Videre vil det relativt enkelt kunne tilpasses til en slik oppgave. De tillitsskapende hindre som må legges i veien for masseovervåkning, vil derfor ikke kunne være av ren teknologisk art. De vil måtte bestå av teknologiske filtreringsmekanismer som er underlagt menneskebasert, uavhengig og effektiv kontroll.

Lysne II beskriver viktigheten av uavhengige organer for ettersyn av og kontroll med DGF/TI. Utvalget foreslo et kontrollregime langs tre akser, med domstolskontroll, et tilsyn for løpende kontroll med DGF/TI og etterfølgende kontroll fra EOS-utvalget og domstolskontroll som innehar "etterretningsfaglig kompetanse, teknisk og operativ innsikt i tjenestens virksomhet samt i overordnede myndigheters styrings- og prioriteringsvirksomhet".
Departementet foreslår at domstolskontrollen legges til de ordinære domstoler ved Oslo tingrett, og at det i stedet for et eget tilsyn pålegges EOS-utvalget å føre skjerpet kontroll med tilrettelagt innhenting. Departementet "vurderer at disse endringene styrker ordningen"[28].

Domstolskontroll

Domstolskontrollen i den foreslåtte form vil neppe innebære reell kontroll med Etterretningstjenestens bruk av data fra DGF/TI regimet. Dette fordi det vil være nødvendig med betydelig teknisk dybdekunnskap og innsikt for å gjøre en reell vurdering av om vilkårene i loven er oppfylt for søk i de lagrede metadata. Særlig gjelder dette for forholdsmessighetsvurderingen, hvor det er nødvendig å forstå teknikken for å kunne vurdere omfanget og hvor inngripende et gitt søk er.

Det er heller ikke lagt opp til at domstolen skal få tilgang til slik kompetanse fra andre enn Etterretningstjenesten selv. En ordning med offentlig oppnevnt advokat kan ikke reparere dette, da advokaten - som ikke kan konferere med noen - etter all sannsynlighet vil ha like dårlige forutsetninger for å utfordre Etterretningstjenesten på det tekniske området som domstolen selv. Domstolskontrollen trenger derfor å styrkes med tilgang til uavhengig teknisk kompetanse, for eksempel ved at det oppnevnes fagkyndige meddommere når begjæringen fra Etterretningstjenesten skal vurderes.

EOS-utvalgets kapasitet

Stortingets Evalueringsutvalg for EOS-tjenesten skriver i sin rapport[29], side 127

> *Det er imidlertid på det rene at utvalgsmodellen, og det faktum at utvalgsmedlemmene innehar verv som i utgangspunktet skal ivaretas ved siden av fulltids arbeid, begrenser EOS-utvalgets kapasitet og dermed omfanget av kontrollvirksomheten. Særlig for de av medlemmene som har fulltidsstillinger i tillegg til dette vervet, oppleves det som krevende å sette av tilstrekkelig tid.*

28 side 210 i høringsnotatet.
29 https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf

> *Utvalget har videre opplyst at det ofte opplever tidspress på inspeksjonene og i møtevirksomheten, og gjerne skulle hatt mer tid både til interne drøftelser og til å ta opp saker av eget tiltak.*

Samme rapport, side 162

> *Det er likevel viktig at både omverdenen og EOS-tjenestene kan stole på at det er EOS-utvalget som står for den reelle kontrollen av tjenestenes virksomhet, og ikke utvalgets sekretariat. En forutsetning om dette ligger til grunn for utvalgsmodellen som sådan, dets parlamentariske forankring og sammensetning. EOS-utvalgets eksistens hviler på en forutsetning om at utvalgets avgjørelser skal fattes av utvalgsmedlemmene i fellesskap, og være uavhengige og selvstendige resultater av en kritisk diskusjon av de funn utvalget og sekretariatet har gjort i undersøkelsen av en sak. Selv om sekretariatet besitter særlig faglig ekspertise og kontinuitet, har EOS-utvalgets medlemmer et særlig ansvar for å kontrollere at sakene er tilstrekkelig utredet. Det er utvalget som har det endelige ansvaret for avgjørelsenes innhold og eventuell kritikk som rettes mot EOS-tjenestene.*

Vi ser ikke at EOS-utvalget *som sådan* har kapasitet til å føre en skjerpet kontroll med tilrettelagt innhenting i tillegg til sine eksisterende oppgaver. Evalueringsutvalget foreslo blant annet, av kapasitetshensyn, at EOS-utvalget ikke lenger skulle føre kontroll med sikkerhetsklareringssaker. Dette forslaget ble ikke fulgt opp i Stortinget, slik at kapasitetsutfordringene må antas å være minst like store i dag som da rapporten ble utgitt og vil øke betraktelig med dette regimet.

Det vil være en teknisk krevende oppgave å ettergå alle faser i dette regimet. Den tekniske kompetansen dedikert EOS-utvalget må vurderes mot de faktiske oppgaver DGF/TI vil kreve, og være adekvat. Et løselig anslag med 4 nye årsverk virker som grov undervurdering av tilsynsrollens omfang og viktighet.

EOS-utvalgets arbeidsform og rapportering

Departementet er i høringsnotatet inne på at EOS-utvalgets organisering som et organ under Stortinget legger en del føringer for hvordan kontrollen kan gjennomføres. Vi er særlig opptatt av tidsaspektet og av utvalgets myndighet. Det er liten tvil om at EOS-utvalget har gjort grundig arbeid innenfor de gitte rammene. Men utvalgets konklusjon er prisgitt forvaltningen. Dersom forvaltningen er uenig i EOS-utvalgets konklusjoner, er prosessen før en endelig avklaring i Stortinget potensielt svært tidkrevende. Dette kan være akseptabelt for områder som EOS-utvalget fører kontroll med i dag, men vil ikke være akseptabelt for et tiltak hvor feil og ulovligheter kan ha så store konsekvenser som ved tilrettelagt innhenting.
EOS-utvalget har heller ikke aksess til det som er definert som «ulovfestede metoder». Dette skriver de selv i tilsvar til Forsvarsministerens utsagn om at "Utvalget har innsyn i alle deler av virksomheten til alle våre hemmelige tjenester"[30] , og henviser til sin årsmelding[31].

En slik prosess kan vanskelig forsvares for et slik vidtrekkende overvåkingsregime som DGF/TI er. Vi viser derfor til EU *Agency for Fundamental Rights*[32] som anbefaler at et uavhengig kontrollutvalg må være robust, fritt uavhengig og ha adekvat makt og kapasitet relativt den makt og kapasitet en Etterrettning har. Organets myndighet må være klart lovfestet og ha tilstrekkelig ressurser, budsjetter, adekvat ansatte og høy teknisk kompetanse, kunne igangsette etterforskning selv, ha komplett og permanent aksess til det de skal overse, og organets avgjørelser bør være bindende.
EOS-utvalget bør rapportere regelmessig, offentlig publiserte rapporter med detaljerte statistikker

30 Vi skal beskytte norske borgere https://www.dagbladet.no/kultur/vi-skal-beskytte-norske-borgere/70735726
31 Side 55, EOS-UTVALGET Årsmelding 2017 https://eos-utvalget.no/norsk/content/text_ed78f726-e398-40b4-8926-5e169ba74a64/1523359815630/_2017_eos_a_rsmelding_nett.pdf
32 EU Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union – Volume II

og dokumentasjon over sine funn. Her kan en se til kommersielle tjenester, hvordan disse gjør dette.

Kontroll med valget av aksesser

Tilretteleggingsplikten i forslaget er utformet generelt, og vil i prinsippet være gjeldende til enhver tid, jf § 7-2. Dette er til forskjell fra situasjonen i en rekke andre land som har innført bulkaksess, hvor det kreves en beslutning fra politisk hold hver gang det skal etableres en ny aksess. I angloamerikanske land omtales dette gjerne som en "warrant" fra ansvarlig statsråd. Vi finner det underlig at man i forslaget legger opp til at Etterretningstjenesten fritt kan velge aksesser, uten at for eksempel Forsvarsdepartementet fatter en beslutning i hvert enkelt tilfelle. Slik forslaget er utformet kan man som tilbyder risikere å få e-tjenesten "på døren", og plikter da å yte omfattende tilrettelegging uten at dette er omfattet av noen forhåndskontroll. Slik vi ser det vil det være påkrevet at man i det endelige forslaget omarbeider § 7-2 slik at tilretteleggingsplikten er avhengig av en beslutning rettet mot den aktuelle kabeleier. En slik beslutning bør fattes minst ett nivå over Etterretningstjenesten, slik det gjøres i de land det er naturlig å sammenligne seg med.

Rettssikkerhet, kontroll og klagerett

Som tidligere nevnt må EOS-utvalget rapportere transparent om sine funn regelmessig.

Det foreligger ingen klageorgan for individer, den eller de personer som mistenker eller erfarer misbruk/feilbruk av egne data eller opplever uheldige eller urettferdige konsekvenser ved et slikt overvåkingsregime.
En person det rettes søk mot, må ha rett til å informeres om dette. Det bør gis melding til den eller de som har blitt utsatt for overvåkning eller som blir flettet inn i «målrettede søk».

Departementet mener det er "*mindre stigmatiserende å havne i søkelyset til en etterretningstjeneste sammenlignet med å havne i søkelyset til politiet*".
Dette er grov ignoranse overfor individets rettigheter og er et eksempel på at forsvarets ønsker settes over individets og sivilsamfunnets rettigheter.
Den som havner i politiets søkelys har både rett til å forsvare seg og rett til informasjon om hva saken gjelder - og vil fritas fra enhver mistanke om uberettiget anklaget.
Når en person befinner seg innenfor søkelyset av Etterrettningstjenesten, enten denne ansees som målrettet eller ikke, kan dette få uheldige konsekvenser for personen. Eksempelvis så kan automatiserte beslutningsprosesser forårsake at en person finner sin identitet på en "no-fly-liste", ikke få nødvendig visa for en reise eller mister andre rettigheter. Rettigheter inskrenkes eller mistes uten at personen mistenkes for å ha gjort noe som tilsier at rettigheter bør innskrenkes.
Automatiserte beslutningsprosesser, data som inngår i analyser, data som innhentes fra andre kilder, åpne data, dataprofiler innkjøpt kommersielt, data fra andre lands eller leverandørers overvåkingsmaskinerier må problematiseres og diskuteres.
Agoritmestyrte prosesser, med alle de feil, stereotyper og "bias" som følger med og hvor beslutningene bak vurderinger ikke kan dokumenteres og ansvar pulveriseres, kan ha fatale konsekvenser, også for samfunnet i sin helhet. Dette er overholde ikke diskutert.

Et ombud for henvendelser og/eller klagesaker bør diskuteres.

Andre områder - diverse

Regimet DGF/TI har ingen dokumentert arkitektur. Det diskuteres kun funksjonalitet og det er derfor umulig å vurdere hvilken sikkerhet de lagrede data faktisk vil ha. Det er uvisst hva og hvordan alt kobles sammen innbyrdes og også tilknyttinger mot eksterne kilder. Brudd på datasikkerhet kommer like gjerne (oftere) innenfra som utenfra.

Overvåking eller fordekt innhenting mot norske borgere på norsk jord er ikke lov pr i dag. Departementet stadfester også at denne loven videreføres (§ 4-1) .
Likevel vil enhver bruker av elektroniske tjenester og kommunikasjon bli fanget i dette overvåkingsregimet som beskrives.

Forslaget foreslår at overvåking ikke er overvåking før i det øyeblikket data benyttes. Omdefinering av begreper dekker ikke over at dette er teknologisk masseovervåking ved bruk av militær teknologi.

Høringsdokumentet er vagt og flytende på områder som vil berøre datasikkerhet generelt - det er vanskelig å se hvilke datatekniske sikkerhetsutfordringer dette kan få for bedrifter, ikke minst små og mellomstore bedrifter som ikke har egne IT-ressurser.

Det kan bli vanskelig å ha tilstrekkelig tillit til tjenestetilbyder dersom denne blir pålagt tilrettelegging av bakdører.

Det er vanskelig å se at staten vil kunne ivareta troverdig garanti for fortrolig kommunikasjon mellom individ og forvaltning.

Det er vanskelig å forstå hvilke personvernregler som gjelder, eller hvorvidt der overhode er noen, da Etterretningstjenesten opererer med sine egne lover, eventuelt er unntatt fra lover, mens nettbrukeren tror GDPR persondatabeskyttelse er gjeldende.

Høringsforslaget kan så tvil om hvorvidt systemer for «key escrow» er sikret mot «innhenting».

Endepunktinnhenting (§ 6-8) omtales som operasjon rettet mot utlandet, mens lovteksten er generell og tillater tilsynelatende også endepunktinnhenting fra systemer i Norge.

Vi har utelatt å kommentere cyberoperasjoner, offensive eller defensive cybertiltak, men det er uklart hvordan data akkumulert under DGF/TI regimet inngår her.

Vi mener det foreslåtte regimet DGF/TI er så omfattende og så dypt inngripende i den private sfære at det fremstår som et høyrisikabelt sosialt eksperiment.

Konklusjon

EFN finner at høringsforslaget er vidfattende, vagt og mangelfull på flere områder, samtidig som vigtige temaer ikke dekkes eller ikke belyses tilstrekkelig. Lovbegrunnelsen virker lite reflektert og vil være vanskelig å forstå om dette forslaget vedtas i Stortinget.

Formålet virker mangfoldig og tvetydig, uten klare, entydige formålsavgrensninger, og fremstår svært generell og lite målrettet. Potensialet for formålsutglidning virker faretruende høyt. Formålet beskrives nærmest som at alle borgeres digitale aktiviteter må tagges, indekseres, digitalt fingerprintes og metadatalagres for å maksimere størrelsen på en høystakk, slik at nåla kan søkes.

EFN kan ikke se at teknologisk masseovervåking av borgernes fortrolige elektroniske kommunikasjon er en nødvendighet for å ivareta nasjonens sikkerhet. Maktforskyvning i størrelsesorden som her foreslås, forvitrer også de demokratiske verdier og menneskerettslige friheter staten skal beskytte. Retten til en privat sfære, vernet mot statlig innsyn i det digitale rommet er vitalt for vårt demokrati og rettstat - og for den tilliten vi har til hverandre. Dette er høyt verdsatte verdier som kan forspilles.

EFN støtter ikke høringsforslaget om innføring av DGF/TI.
Vi mener det er lovstridig og ute av proporsjoner – og sansynligvis få uønskede sideeffekter, inklusive svekkelse av datasikkerhet og et kappløp for krypterte og metodiske omgåelser av dette regimet.