Bli medlem: https://portal.isoc.org/join

Nyhetsbrev nr. 1, 2018. Utsendt: 13.02.2018

Innhold:

- Årsmøte ISOC Norge
- ISOC Norge sitt svar på høring om Åndsverksloven
- ISOC er en av organisasjonene som faktisk har innflytelse over Internett – dette kan du være med på ved å bli medlem!

Årsmøte ISOC Norge

Vi minner om vårt årsmøte,

onsdag 28. februar 2018 kl. 19:00 i Frivillighetshuset, K1, Kolstadgata 1, Oslo.

Alle medlemmer kan møte. Nye medlemmer kan registreres på stedet derom du ønsker å ha med deg noen som ennå ikke er medlem.

I tilknytning til årsmøtet, ca. kl. 19:45, vil

Joakim Hammerlin, filosof og saksprosaforfatter, foreleser på Nansenskolen, holde foredraget:
Nedkjølingseffekten eller "Chilling Effect" – hva gjør den med oss?

med påfølgende mulighet for dialog. Foredraget er åpent for alle og vi åpner deretter til sosialt samvær i nærheten.

Underlag og mer informasjon om årsmøtet finner du under "Arrangementer" på vår åpne WEB, isoc.no . Der kan du også melde deg på under, "Booking".

Vel møtt!

ISOC Norge sitt svar på høring om Åndsverksloven

ISOC Norge sitt høringssvar ble gitt 5. februar 2018 i Stortinget og gjengis her i sin helhet:

Høring om Lov om opphavsrett til åndsverk mv. (åndsverkloven)

Internet Society Norge er den norske avdelingen av Internet Society (ISOC). I tillegg til å være IETFs (Internetts standardiseringsorgan) formelle hjem, jobber ISOC med Internet Governance; med fokus på at myndigheter og andre beslutningstakere skal ta sine beslutninger basert på god helhetlig kunnskap også om konsekvenser av tiltak, slik at Internett skal forbli åpent og tilgjengelig for alle.

ISOC Norge bidrar gjerne med videre samtaler med komiteen eller andre for å gi økt forståelse for hvordan Internetteknologi og protokoller fungerer.

I vårt høringssvar forholder vi oss kun til kapittel 6 i den nye åndsverksloven "Særskilte tiltak ved inngrep i opphavsrett m.m. på Internett", §87-§99.

Behandling av personopplysninger og tilgang til abonnementsopplysninger

ISOC Norge sin anbefaling er:

1. **at særordningene der rettighetshavere konsesjonsfritt kan behandle og samle inn personopplysninger, samt få tilgang til opplysninger som identifiserer innehaver av abonnement, fjernes (§87 og §88).**

Vi har følgende innvendinger:

- En IP adresse *kan* brukes til å identifisere *abonnenten* av en Internettjeneste. Den vil aldri kunne identifisere en enkeltperson (se bakgrunnsinformasjon mot slutten av dokumentet).
- Innehaveren av abonnementet kan ikke være ansvarlig for hvordan enkeltbrukere av abonnementet bruker Internett. Abonnementsopplysninger kan *kun* brukes som grunnlag for ytterligere etterforskning.
- Internett abonnementsopplysninger har liten "bruksverdi". Rettighetsindustrien har i stor grad gått bort fra å saksøke kundene sine. Det er vanskelig å se at abonnementsinformasjonen kan brukes til annet enn å etablere nye forretningsmodeller basert på å sende "trusselbrev" til innehavere av Internettabonnementet.
- Vi er alle potensielle skapere av åndsverk, og kan i så måte samle inn IP-informasjon konsesjonsfritt for å drive egen etterforskning. Er dette virkelig intensjonen med loven?

Tiltak rettet mot nettsted:

ISOC Norge sin anbefaling er:

1. **"Tiltak rettet mot nettsted" (§89-§99) fjernes.**
2. **Sekundært anbefaler vi at teksten "å hindre" tilgang til et nettsted fjernes, mens "vanskeliggjøre" består.**

ISOCs syn på blokkering ("hindre eller vanskeliggjøre tilgang til nettsted"):

- ISOC Norge sitt syn er at den mest passende måten for å bekjempe ulovlig innhold og aktiviteter på Internett er å fokusere tiltak der ulovlig handling skjer.
- Blokkering løser ikke problemet. Blokkering fjerner ikke innholdet fra Internett, det stopper ikke ulovlig aktivitet og det får ingen konsekvenser for de som utfører ulovlige handlinger.
- Blokkering fører til utilsiktet skade. For mye eller for lite kan blokkeres, brukere påføres utilsiktet risiko ved å prøve å unngå blokkering, tillit til Internett reduseres, og tjenester drives "under jorda".

- Internett er skapt for at informasjonen skal komme frem, og en fullstendig *hindring* av tilgang til nettsted er verken teknologisk eller praktisk mulig.
- Lovteksten har manglende begrensninger på hvilke mekanismer som kan brukes til å hindre eller vanskeliggjøre tilgang til nettsted.
- Faktisk implementering av en pålagt blokkeringsmekanisme velges av tjenesteyter og tjenesten vil følgelig oppleves forskjellig for brukere av forskjellige tjenesteytere.
- Lovteksten åpner for en mulig eskalering av bruk av blokkeringsmekanismer, uten å ta inn over seg hvilke konsekvenser dette vil ha for brukerne av Internett.
- Det er heller ikke klart hvordan tidsbegrensede blokkeringer følges opp.

Hvis likevel blokkering velges, bør følgende anbefalinger følges:

a. Velg blokkering kun som siste alternativ.
b. Gå etter **kilden** til ulovlig innhold.
c. Vær åpen. NKOM bør vedlikeholde en liste av domener som er blokkert.
d. Det teknologiske miljøet bør være involvert i å sette "policy".
e. Vær deres ansvar ovenfor Internett bevisst: Alle brukere av Internett har et ansvar for nettverkets sikkerhet, stabilitet og robusthet. Noen ganger er skaden indirekte, f.eks hvor brukeres sikkerhet svekkes fordi de prøver å omgå blokkering.
f. Ha tydelig dialog med det tekniske miljøet om hva slags blokkering som kan aksepteres.
g. Involver alle "stakeholders". Utvikling av retningslinjer og implementering bør involvere et bredt utvalg av interessenter. Eksperter på Internett teknologi, tjenesteytere, rettighetshavere og representanter for brukerne av Internett.
h. Blokkering må være tidsbegrenset, og fjernes så fort grunnen til blokkeringen forsvinner.
i. Rettslige prosesser: Tjenesteytere, rettighetshavere eller deres representanter bør ikke bli de-facto politimyndigheter.
j. Prioriter og bruk alternative metoder: Informasjon til brukerne, internasjonal samarbeid, oppfordre til foreldrekontroll. Lag lover, reguleringer og tilskuddsordninger som oppfordrer rettighetsindustrien til å lage og tilby innholdet på lovlige plattformer.

Bakgrunn

Behandling av personopplysninger og tilgang til abonnementsopplysninger

IP-adresser kan ikke brukes som identifikatorer. Det finnes to versjoner av internett protokollen; IPv4 og IPv6. Man er tom for IPv4 adresser og man har i mange år jobbet med en overgang til IPv6. Mens denne overgangen foregår må fortsatt endebrukere ha tilgang til IPv4 Internett.

Hvordan kan man gi flere brukere aksess til internett uten å bruke flere adresser? Jo, ved å dele en IPv4 adresse på flere brukere. Denne adressedelingsteknologien [RFC1631] har vært brukt i mange år, og typisk vil en Internett aksessleverandør tildele en enkelt IPv4 adresse til abonnenten og abonnenten vil bruke NAT for å dele denne adressen blant alle enhetene i hjemmet. Basert på dette kommer påstanden om at en IP adresse kan brukes til å identifisere abonnenten av Internettilknytningen.

Ettersom internett fortsetter å vokse har behovet for adresser økt mer enn hva som kan tilfredsstilles ved å gi en IP adresse til hver abonnent. Utviklingen nå er at en IPv4 adresse deles mellom *mange* abonnenter. Det er mange teknologiske mekanismer for dette. CGN [RFC6888], DS-lite [RFC6333], MAP-E [RFC7597] Felles for dem alle er at for å kunne få tilsvarende nøyaktighet for å identifisere abonnenten av Internettilknytningen holder det ikke

lengre med kun en IPv4 adresse, man må også ha transport-lag port [RFC793] og tidspunkt (med relativt høy nøyaktighet).

Det må forutsettes at rettighetshavere som samler inn data forstår dette og har tilstrekkelig teknologi på plass for å sikre at innhenting og lagring av data foregår på en korrekt måte, for å redusere sannsynligheten for at feil abonnent blir identifisert.

Av helt legitime grunner foregår mye av kommunikasjonen på Internett *ikke* direkte mellom endepunktene. Kommunikasjon kan gå via en bedrifts web-proxy, eller VPN, eller brukere som ønsker eller trenger anonymitet kan bruke egne nettverk som TOR. IP adressen vil da være IP adressen til siste node i kjeden, det vil si at IP-adressen er ubrukelig som identifikator.

Det er viktig å huske at

a. En IP-adresse ikke kan brukes til å identifisere en enkeltperson
b. Innsamling av IP-adresser krever presisjon og forståelse av teknologiendringer
c. Aksessleverandørens logger og bruk av adressedelingsmekanismer må også vurderes.

Tiltak rettet mot nettsted

For et nærmere blikk på problemstillingen rundt blokkering og filtrering henviser vi til IETF publikasjonen [RFC7754] - *Technical Considerations for Internet Service Blocking and Filtering* og ISOC publikasjonen *Internet Society Perspectives on Internet Content Blocking: An Overview* [ISOC].

Å hindre tilgang til et nettsted for brukere med en viss motivasjon er teknisk sett meget vanskelig. Man kan vanskeliggjøre tilgang og gjøre det mindre sannsynlig at brukere *snubler* over rettighetsbeskyttet materiale. En rettslig inndragelse av et domene er etter vårt syn et mer akseptabelt tiltak i motsetning til blokkering, fordi tiltaket skjer mot nettstedet hvor den ulovlige handlingen foregår.

DNS basert blokkering (DNS poisoning)

I de dommene som har falt har Oslo tingrett pålagt DNS basert blokkering. Denne mekanismen er bare effektiv så lenge brukerne bruker tjenesteyterens navnetjenere. I endel tilfeller har brukeren valgt å bruke andre navnetjenere, og da er blokkeringen ikke effektiv. Det finnes også produkter som leveres med forhåndsprogrammerte navnetjenere uavhengig av tjenesteyter. Det er mulig å forsøke å tvinge brukeren til å bruke en gitt navnetjener (f. eks. ved å filtrere TCP og UDP port 53). Utviklingen i DNS teknologi går mot at både innhold og transport av DNS blir kryptert (og signert). En fordel med denne metoden er at den i hovedsak berører de som utøver rettighetsbrudd.

IP adresse filtrering

Det vil være tilsvarende argumenter for IP-adresse filtrering (som vil ha en mye større sjanse for utilsiktet blokkering, jmf tidligere noter om IPv4). I moderne CDN (content distribution networks) har ikke nettsted lengre faste adresser, i tillegg vil brukeren kunne gå forbi slike sperrer ved å bruke proxier / VPN tjenester.

DPI basert filtering

Dette er filtering som baserer seg på å kikke lengre inn i pakkene og filtrere f.eks URLer i HTTP. Dette er en svært intrusiv metode, som har større personvernkonsekvenser siden tjenesteyter vil her måtte inspisere *alle* pakker fra *alle* kunder. Ikke bare de som bedriver

rettighetskrenkelser. Nye web standarder har kryptering i utgangspunktet og slike mekanismer vil være høyst ineffektive.

Konsekvens av å virkelig "hindre tilgang til nettsted"

Det er meget vanskelig rent teknologisk å hindre utveksling av informasjon over Internett. Det finnes et utall av måter man kan skjule informasjon på, om det er kryptering eller steganografi. Selv med ekstreme tiltak som å forby kryptering eller å tvinge brukeren til en tjenesteyters "proxy".

Referanser:

IP adresse som identifikator:
RFC1631 - The IP Network Address Translator (NAT). https://tools.ietf.org/html/rfc1631
RFC793 - TRANSMISSION CONTROL PROTOCOL. https://tools.ietf.org/html/rfc793
RFC7597 - Mapping of Address and Port with Encapsulation MAP-E). https://tools.ietf.org/html/rfc7597
RFC6333 - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion. https://tools.ietf.org/html/rfc6333
RFC6888 - Common Requirements for Carrier-Grade NATs (CGNs). https://tools.ietf.org/html/rfc6888
Forbrukerrådet om trusselbrev fra Njord Law Firm: https://www.forbrukerradet.no/siste-nytt/ikke-betal-krav-fra-njord-law-firm/

Blokkering:
RFC7754 - Technical Considerations for Internet Service Blocking and Filtering. https://tools.ietf.org/html/rfc7754

ISOC - Internet Society Perspectives on Internet Content Blocking: An Overview
https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

ISOC er en av organisasjonene som faktisk har innflytelse over Internett – dette kan du være med på ved å bli medlem!

Vi rekrutterer nye medlemmer – snakk med kollegaer, familie, venner og bekjente og fortell om arbeidet til ISOC Norge. Her er noen ord om hva vi driver med.

- Vi er med og former fremtidig policy for domener internasjonalt og i Norge.
- Vi arrangerer medlemsmøter om bruken av internett og aktuelle tema rundt dette, inkludert historien, personvernet og politikken.
- Vi er med i samfunnsdebatten, og skriver svar på høringer

Internet Society sin hovedside: http://www.internetsociety.org/
ISOCs formål: https://www.internetsociety.org/who-we-are/mission
Innmelding: https://portal.isoc.org/join (velg “Norway Chapter”)

Du finner oss på Facebook, Twitter og Linkedin. Medlemmer har også tilgang til et webgrensesnitt (“Connect”) for dialog om aktuelle emner.

ISOC Norge har opprettet en gruppe på tjenesten, Meetup. Se info.