

FLU



Frequente en Langdurige Uploaders

FLU-Protocol
Stichting BREIN
27 november 2020

Inhoudsopgave

1. Inleiding	3
2. Omvang van de online piraterij via Bittorrent	3
3. Definities	5
4. Doel van het FLU-systeem	7
5. Werkwijze en rechtvaardiging gegevensverwerking in het kader van het FLU-systeem	9
5.1 <i>Verzamelen</i>	9
5.2 <i>Waarschuwingen</i>	12
5.3 <i>Handhaving</i>	14
6. Vastgelegde gegevens; toegang; verstrekking; bewaartermijnen	18
6.1 <i>Verzamelde gegevens</i>	18
6.2 <i>Toegang tot de gegevens</i>	18
6.3 <i>Verstrekking van de gegevens</i>	19
6.4 <i>Bewaartermijn van de gegevens</i>	20
7. Wettelijke grondslag	22
8. Proportionaliteit	25
9. Subsidiariteit	27
10. Rechten van de betrokkene	29
10.1 <i>Informeren van de betrokkene</i>	29
10.2 <i>Rechten van betrokkenen</i>	31
10.3 <i>Minderjarige betrokkenen</i>	31
10.4 <i>Klachtenprocedure</i>	31
10.5 <i>Waarborgen</i>	31
10.6 <i>Geheimhouding</i>	31
11. Beveiliging	32
12. Toezicht op naleving FLU-protocol	32
13.1 <i>Wijziging van het FLU-protocol</i>	32
13.2 <i>Audit</i>	32
BIJLAGE 1 Juridisch kader	33
1 <i>Europees recht</i>	33
2 <i>Nederlands recht</i>	34
3 <i>Handhaving van het auteursrecht</i>	34
4 <i>Jurisprudentie</i>	35
BIJLAGE 2 Veelgestelde vragen	37

1. Inleiding

Dit protocol beschrijft de overwegingen en handelwijze, verbonden aan het voeren van het Frequente en Langdurige Uploaders (FLU) Systeem door Stichting BREIN.

2. Omvang van de online piraterij via Bittorrent

Volgens de meest recente onderzoeken maakt ongeveer een kwart van de Nederlandse bevolking gebruik van illegaal aanbod¹. Naar schatting 60% van het illegaal gebruik van entertainmentcontent in Nederland wordt gemaakt via het peer-to-peer-protocol Bittorrent². Uit diverse studies blijkt dat meer dan 95% van de aangeboden bestanden op Bittorrent auteursrechtelijk beschermde werken betreft. Uiteraard is niet elke illegale download/stream een gemiste verkoop. De meeste studies vinden voor muziek een substitutie-effect van 20%. Het IViR berekende in "Ups And Downs" (2009) samen met TNO en SEO dat de jaarlijkse schade voor de muziekindustrie in Nederland rond de 100 miljoen euro lag.³ Verondersteld werd dat de substitutiegraad voor films, boeken en games hoger ligt omdat minder sprake van sampling is. Inmiddels is daar voor wat betreft film nader onderzoek naar gedaan door Considerati in samenwerking met IViR, CentERdata en MarkMonitor, zie "Omdat Het Gratis Is" (2014).⁴ Daaruit blijkt inderdaad dat de substitutie bij film 0,32 is, dat wil zeggen dat voor elke 10 downloads/streams er 3,2 films minder legaal worden bekeken.

De jaarlijkse hoeveelheid illegale downloads van films en series wordt berekend op minimaal 61 miljoen, waaruit een schade voor de Nederlandse filmindustrie volgt van 78,4 miljoen euro per jaar. Ook hier geldt dat Bittorrent de voornaamste bron voor het illegaal gebruik is. Dit onderzoek dateert overigens van voor de enorme vlucht die diensten als Popcorn Time hebben genomen als bron voor het illegaal streamen van films en series. Omdat dit soort diensten ook gebruik maken van het Bittorrent protocol is het belang van het terugdringen van het illegale gebruik van Bittorrent nog verder toegenomen.

De schade die het illegale gebruik van Bittorrent veroorzaakt beperkt zich niet slechts tot audiovisuele producten, ook de rechtmatige exploitatie van muziek, games en ebooks heeft er ernstig onder te lijden. Zo staat bijvoorbeeld tegenover elk legaal verkocht ebook, minimaal één illegaal gedownload exemplaar⁵ en gebruikt een significant percentage (27% in 2019) van de internettende consumenten illegale bronnen voor muziek⁶.

¹ Zie bijvoorbeeld <https://www.telecompaper.com/nieuws/23-procent-nederlanders-doet-nog-aan-gratis-downloaden--1328432> en het Considerati onderzoek "Feiten Om Te Delen" (2011) dat een wetenschappelijke beoordeling omvat van meer dan 200 verschillende onderzoeken naar online piraterij van muziek

² Zie het rapport van Irdeto "The piracy landscape: Has web video replaced peer-to-peer?" (2018), p. 9, <https://resources.irdeto.com/white-papers-e-books-reports/the-piracy-landscape-has-web-video-replaced-peer-to-peer>

³ https://www.ivir.nl/publicaties/download/Ups_And_Downs.pdf. Deze studie is opgevolgd door "Filesharing 2012" van IViR en CentERdata die ook ingaat op legaal downloadgedrag https://www.ivir.nl/publicaties/download/Filesharing_2012.pdf Een kwart van de Nederlandse bevolking downloadt (ook) illegaal.

⁴ http://otpnederland.nl/upload/pdf/3.Omdat_het_gratis_is_Consid_CentERdat_IViR_small.pdf

⁵ zie bijv. <http://radar.avrotros.nl/testpanel/uitslagen/detail/tevreden-lezers-van-vaak-illegale-e-books/>

⁶ <https://www.ifpi.org/downloads/Music-Listening-2019.pdf>

BREIN is ervan overtuigd dat - om het illegale gebruik van Bittorrent terug te dringen en zo legale distributiemodellen van entertainment producten een eerlijke kans te geven - het belangrijk is dat uploaders gewaarschuwd worden voor hun gedrag en zich bewust worden van de schadelijke gevolgen die makers en rechthebbenden ondervinden als gevolg van het illegaal uitwisselen van bestanden. Daarbij hoort ook de bewustwording dat er een mogelijkheid is dat zij door de rechthebbenden worden aangesproken voor de compensatie van de schade die het illegale bittorrent-gebruik veroorzaakt. BREIN spreekt al zo veel als mogelijk Nederlanders aan die als bron fungeren van illegaal aanbod. Ook doet BREIN aan voorlichting aan consumenten. Dit blijkt echter niet afdoende. Zo zijn Nederlanders die als eerste uploader van content fungeren, zich beter gaan verschuilen sinds BREIN met gerichte aanpak van deze groep uploaders begon.

Om optimaal effectief te zijn, zou het noodzakelijk kunnen blijken om de waarschuwing en voorlichting gepaard te laten gaan met het daadwerkelijk aanspreken door BREIN van de gebruikers die het hart van het Bittorrent netwerk vormen; gebruikers van wie is vastgesteld, dat zij vaker inbreuk maken door entertainment producten te uploaden en zo meewerken aan de verdere verspreiding ervan en/of gebruikers die entertainment content gedurende langere tijd blijven "seeden", waardoor zij op hun beurt weer talloze downloads door andere gebruikers mogelijk maken. Dit soort gebruikers houdt de continue stroom illegaal aanbod op Bittorrent in stand. Of daadwerkelijk tot handhaving wordt overgegaan, hangt af van de resultaten van de waarschuwingsfase.

3. Definities

AFLU: AnalyseProgramma Frequente en Langdurige Uploaders. AFLU is de software van het FLU-systeem, die door BREIN wordt gebruikt om de IP-nummers te verzamelen van frequente en langdurige uploaders. Het is een Bittorrent client die gebouwd wordt rond een standaard open source library voor Bittorrent clients. AFLU draait geheel op de interne servers van BREIN.

AP: Autoriteit Persoonsgegevens.

Auteursrechtlijn: EU-richtlijn 2001/29; Richtlijn betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en de naburige rechten in de informatiemaatschappij.

AVG: Algemene Verordening Gegevensbescherming (EU-verordening 2016/679)

Aw: Auteurswet.

Betrokkene: een abonnee van wie het IP-nummer is aangetroffen in een Bittorrent-zwerm en vastgelegd met behulp van AFLU in FLU. Voor de leesbaarheid in dit protocol steeds aangeduid in de mannelijke vorm.

Bittorrent: peer-to-peer-protocol waarmee bestanden door gebruikers (peers) snel en efficiënt kunnen worden geüp- en download. Een belangrijk kenmerk van Bittorrent is dat iedere gebruiker die een bestand downloadt, elk reeds gedownload deeltje van het bestand direct (en automatisch) weer beschikbaar stelt voor andere gebruikers. Bittorrent is gebaat bij evenwicht: het protocol functioneert optimaal indien alle gebruikers evenveel deeltjes up- als downloaden. Voor een goede werking van Bittorrent is het daarom belangrijk dat gebruikers bestanden die zij compleet hebben gedownload, nog enige tijd beschikbaar blijven stellen voor hun medegebruikers.

Bittorrent client: software waarmee gebruikers deel kunnen nemen aan een Bittorrent-zwerm.

Bittorrent-zwerm: een verzameling van computers van Bittorrent-gebruikers die via een Bittorrent netwerk op een bepaald tijdstip een bepaald bestand onderling uitwisselen.

BOB: Bittorrent OnderzoeksBestand, het met FLU vergelijkbare systeem van BREIN dat gericht is op het verzamelen van bewijs tegen eerste en grote uploaders en dat door de AP rechtmatig is verklaard bij besluit van 12 januari 2016 (z2015-00574).

E-commerce richtlijn: EU-Richtlijn 2000/31; Richtlijn inzake elektronische handel.

FLU: Frequente en Langdurige Uploaders; het FLU Systeem.

Houder van een IP-nummer: een persoon – man of vrouw - die als abonnee door zijn/haar ISP op een bepaald tijdstip een bepaald IP-nummer toegewezen heeft gekregen. Voor de leesbaarheid in dit protocol steeds aangeduid in de mannelijke vorm.

HvJEU: Hof van Justitie van de Europese Unie.

ISP: Internet Service Provider. Een ISP levert (onder andere) de internetverbindingen voor haar abonnees/klanten.

IP-nummer: IP staat voor Internet Protocol. Om het mogelijk te maken dat computers op internet elkaar kunnen vinden en identificeren, heeft elke computer die is aangesloten op het internet of netwerk een IP-nummer (of: IP-adres). Dit kan een IPv4- of een IPv6-nummer zijn⁷. Een IP-nummer is vergelijkbaar met een telefoonnummer, maar zonder dat het in een gids is opgenomen. In Europa en het Midden-Oosten worden IP-nummers toegewezen door

⁷Zie https://nl.wikipedia.org/wiki/Internet_Protocol_versie_6; IPv4-adressen bestaan uit 32 bits, terwijl IPv6-adressen uit 128 bits bestaan. IPv6 heeft daardoor veel meer (een bijna onuitputtelijke voorraad) adressen dan IPv4

RIPE NCC (RIPE Network Coordination Centre). ISP's krijgen gewoonlijk aaneengesloten blokken IP-nummers toegewezen door RIPE en verdelen de afzonderlijke IP-nummers op hun beurt onder hun abonnees.

NAW-verzoek: een verzoek van BREIN aan een ISP om verstrekking van identificerende gegevens (naam, adres, woonplaats, eventueel: e-mailadres) van een abonnee van die ISP.

Notificatie: een waarschuwende en voorlichtende brief of e-mail die op verzoek van Stichting BREIN door een ISP aan een betrokkene wordt gestuurd.

Peer: een Bittorrent-gebruiker die bestand(en) downloadt. Tijdens en na het downloaden stelt hij elk reeds op zijn computer gedownload deeltje van een bestand direct (en automatisch) weer beschikbaar aan de andere gebruikers die zich in dezelfde Bittorrent-zwerm bevinden.

Persoonsgegevens: elk gegeven betreffende een identificeerbare natuurlijke persoon.

Popcorn Time: een populaire Bittorrent client, gericht op het illegaal streamen van films.

Seeder: een Bittorrent-gebruiker die een bestand dat op zijn computer staat beschikbaar stelt aan andere gebruikers van het Bittorrent netwerk.

UAVG: Uitvoeringswet Algemene verordening gegevensbescherming

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens.

Wbp: Wet bescherming persoonsgegevens.

Wnr: Wet naburige rechten.

4. Doel van het FLU-systeem

Stichting BREIN heeft als doel de collectieve bestrijding van auteursrechtinbreuken. BREIN heeft in de afgelopen jaren veelvuldig in rechte en buiten rechte opgetreden tegen het ongeautoriseerd aanbieden van entertainment content op het internet, met name ten behoeve van (de leden van) haar aangeslotenen. Als onderdeel van het optreden tegen illegaal aanbod richt BREIN zich behalve op handhaving ook op voorlichting.

De (leden van de) aangeslotenen van BREIN bestaan uit makers inclusief uitvoerende kunstenaars enerzijds en producenten, uitgevers en distributeurs anderzijds. De werkerreinen zijn muziek, film en tv, boeken, beeld en games. In het bestuur van BREIN nemen (vertegenwoordigers van) muzik auteurs, artiesten, beeldende kunstenaars, fotografen, tekstschrijvers, scenaristen en regisseurs uitgevers, collectieve beheersorganisaties, omroepen, muziek- en filmproducenten zitting. De Nederlandse en internationale (leden van de) aangeslotenen⁸ van BREIN vertegenwoordigen tezamen het leeuwendeel van de rechten die er wereldwijd op commercieel beschikbare entertainmentcontent bestaan en op de Nederlandse markt beschikbaar zijn. Speerpunten van BREIN's beleid zijn: handhaving tegen illegaal aanbod door afsluiting of blokkering van diensten en handhaving tegen uploaders; staking dienstverlening door allerhande tussenpersonen aan hun ongeautoriseerd handelende klanten en afgifte identificerende gegevens van beheerders en uploaders; waarschuwing en voorlichting van inbreukmakende uploaders.

De statuten van BREIN vermelden als doelstelling in artikel 3.1: “het bestrijden van de onrechtmatige exploitatie van informatiedragers en informatie en het te dien einde behartigen van de belangen van de rechthebbenden op informatie en van de rechtmatige exploitanten daarvan, met name van haar aangeslotenen, in het bijzonder door het handhaven, het bevorderen en verkrijgen van een afdoende juridische bescherming van de rechten en belangen van die rechthebbenden en exploitanten, alles in de ruimste zin.”

Krachtens artikel 3.2 sub a en f van diezelfde statuten tracht BREIN dit doel onder meer te bereiken door: “het voorkomen en bestrijden van onrechtmatige exploitatie van informatiedragers en informatie in de ruimste zin” en “alles wat [hiermee] in de meest uitgebreide zin van het woord verband houdt of daartoe bevorderlijk kan zijn”. Daarnaast is BREIN door rechthebbenden van wie zij de werken bij de voorlichting en handhaving zal betrekken uitdrukkelijk gevolmachtigd om hun intellectuele eigendomsrechten te handhaven.

Het doel van de gegevensverwerking via FLU is voorkoming van inbreuken met Bittorrent op een zo doeltreffend mogelijke wijze. Het verzamelen van IP-adressen uit Bittorrent zwermen waarin inbreukmakende content wordt uitgewisseld is daarvoor noodzakelijk. De voorlichtingsacties en mogelijke handhavingsacties van BREIN zijn gericht op preventie van inbreuk in de toekomst, niet op vergoeding van geleden schade door de rechthebbenden door de gepleegde inbreuk op hun rechten.

⁸ <http://stichtingbrein.nl/aangeslotenen.php>

BREIN beoogt met FLU een zo groot mogelijk resultaat teweeg te brengen op de voor de betrokkenen minst ingrijpende wijze. Hiervoor is een combinatie van algemene en gerichte waarschuwing c.q. voorlichting van de inbreukmakende Bittorrent-gebruikers en – als dat niet voldoende effect heeft - handhaving volgens BREIN de meest geëigende en proportionele weg. In dit kader heeft BREIN het FLU-protocol ontwikkeld. FLU is zo ontworpen en opgezet dat zowel voorlichtende waarschuwingen aan inbreukmakers kunnen worden gestuurd, als handhavend kan worden opgetreden tegen uploaders die vaker in Bittorrentzwermen worden aangetroffen door BREIN.

Omdat BREIN niet in staat is met behulp van AFLU of anderszins zelfstandig de bij de aangetroffen IP-adressen behorende contactgegevens te achterhalen, is zij afhankelijk van de medewerking van de ISP's om de abonnees aan te kunnen spreken van wie de IP-adressen in de Bittorrent-zwermen worden aangetroffen. Hoe beter de samenwerking met de ISP's bij het sturen van de notificaties verloopt, hoe doeltreffender FLU in de eerste fase kan zijn.

In ieder geval gedurende de eerste zes maanden zullen eerst enkel waarschuwingen worden gestuurd aan gebruikers die inbreukmakende content blijven seeden en gebruikers die twee of meer keer in een Bittorrent-zwerm waarmee inbreukmakende content wordt uitgewisseld worden aangetroffen. Het is een beproefde methode om gericht notificaties te sturen aan overtreders om vermindering van onrechtmatig gedrag teweeg te brengen. Deze zullen immers zowel een voorlichtend als een waarschuwend effect sorteren. Met betrekking tot Bittorrent-gebruikers gebeurt dit al in het Verenigd Koninkrijk en de Verenigde Staten. Ook Nederlandse ISP's ontvangen in het kader daarvan met enige regelmaat reeds notificatieverzoeken vanuit deze landen. De Autoriteit Persoonsgegevens heeft voorts in een eerder stadium aan BREIN laten weten dat zij het van belang acht dat gebruikers van het Bittorrent netwerk gewaarschuwd worden voordat er met eventuele handhaving wordt begonnen.

BREIN zal onderzoek laten verrichten naar het effect van de waarschuwingen door het onderzoeksbureau Kantar (voorheen TNS NIPO). Het effectonderzoek zal worden opgezet in de vorm van een voor- en een nameting bij twee onafhankelijke steekproeven. De voormeting vindt plaats voordat het zes maanden durende waarschuwingstraject van start gaat en de nameting vindt (kort) na dit traject plaats. Kantar maakt voor haar onderzoeken gebruik van eigen onderzoekspanels.

Afhankelijk van de uitkomst van het onderzoek naar de effectiviteit van de waarschuwingen - die in hoge mate afhankelijk zal zijn van de mate van medewerking die de ISP's in deze fase van FLU verlenen- zal BREIN na de eerste periode van zes maanden besluiten of meer handavingsgerichte maatregelen tegen de doelgroep waarop FLU zich richt, noodzakelijk worden geacht.

Het doel van de eerste fase van FLU is dat een half jaar na het begin van de gerichte FLU-waarschuwingscampagne Nederlandse Bittorrent-gebruikers in het algemeen verondersteld kunnen worden zich bewust te zijn van het risico, dat zij met hun inbreukmakende gedrag handavingsacties van BREIN over zich afroepen. Het is in elk geval de intentie van BREIN dat het aantal Nederlandse IP-nummers in de bittorrentzwermen als gevolg van de

waarschuwingcampagne reeds aanzienlijk zal zijn afgenomen. Of BREIN direct na de eerste periode daadwerkelijk over zal gaan tot de volgende fase van FLU en handhavingsacties in gang zal zetten, is afhankelijk van de uitkomst van het onderzoek dat BREIN door Kantar zal laten verrichten. Op zijn vroegst na deze eerste periode van zes maanden, zal BREIN FLU indien nodig opschalen en ook handhavend gaan optreden tegen gebruikers die in steekproeven drie keer of vaker in een Bittorrent-zwerm worden aangetroffen. Dit zijn gebruikers die content gedurende lange tijd blijven seeden of die meerdere keren per maand inbreukmakende bestanden down- en uploaden.

Om het daadwerkelijk handhavend optreden tot een minimum te kunnen beperken is het van belang dat het sturen van voorlichtende waarschuwingen tegelijkertijd met de mogelijke handhaving doorgaat.

5. Werkwijze en rechtvaardiging gegevensverwerking in het kader van het FLU-systeem

5.1 Verzamelen

Voor het verzamelen van gegevens in het kader van FLU heeft BREIN een eigen Bittorrent client laten ontwikkelen: AFLU. Hiermee worden de steekproeven uitgevoerd. Medewerkers van BREIN zullen met gebruikmaking van AFLU zelf via het Bittorrent netwerk IP-nummers verzamelen die worden aangetroffen in zwermen waarin een inbreukmakend bestand wordt uitgewisseld. Er wordt daarbij dus geen gebruik gemaakt van diensten van derden. AFLU draait geheel op de interne servers van BREIN.

Met het oog op de bescherming van persoonsgegevens is AFLU zodanig ingericht dat er niet meer IP-adressen worden verwerkt dan strikt noodzakelijk is. Omdat FLU is gericht op Nederlandse gebruikers, wordt AFLU gevoed met een zogenaamde 'whitelist' waarop uitsluitend Nederlandse IP-nummers voorkomen. Buitenlandse IP-nummers - die dus niet op de whitelist voorkomen - zullen als gevolg daarvan buiten beschouwing worden gelaten; deze worden door AFLU automatisch direct geanonimiseerd.

Het 'whitelisten' van Nederlandse IP- adressen kan op twee verschillende manieren plaatsvinden. De eerste manier is door AFLU te configureren met een lijst waarop uitsluitend Nederlandse IP-adressen voorkomen. De tweede manier is om AFLU tijdens het verzamelen van IP-adressen van Bittorrentgebruikers openbare diensten (b.v. RIPE) te laten raadplegen, waaruit geografische informatie van een IP-adres kan worden opgevraagd en aan de hand daarvan buitenlandse IP-adressen automatisch direct te anonimiseren

Uit het oogpunt van efficiëntie maakt BREIN gebruik van de eerstgenoemde manier, waarbij maandelijks een update van de whitelist wordt uitgevoerd. Die update betreft BREIN middels een maandelijks abonnement van een betrouwbare externe partij, te weten DB-IP.com. De lijst met Nederlandse IP-nummers zal, zodra de update van DB-IP is ontvangen (op de eerste dag van elke maand), zo spoedig mogelijk doch uiterlijk binnen drie werkdagen worden bijgewerkt.

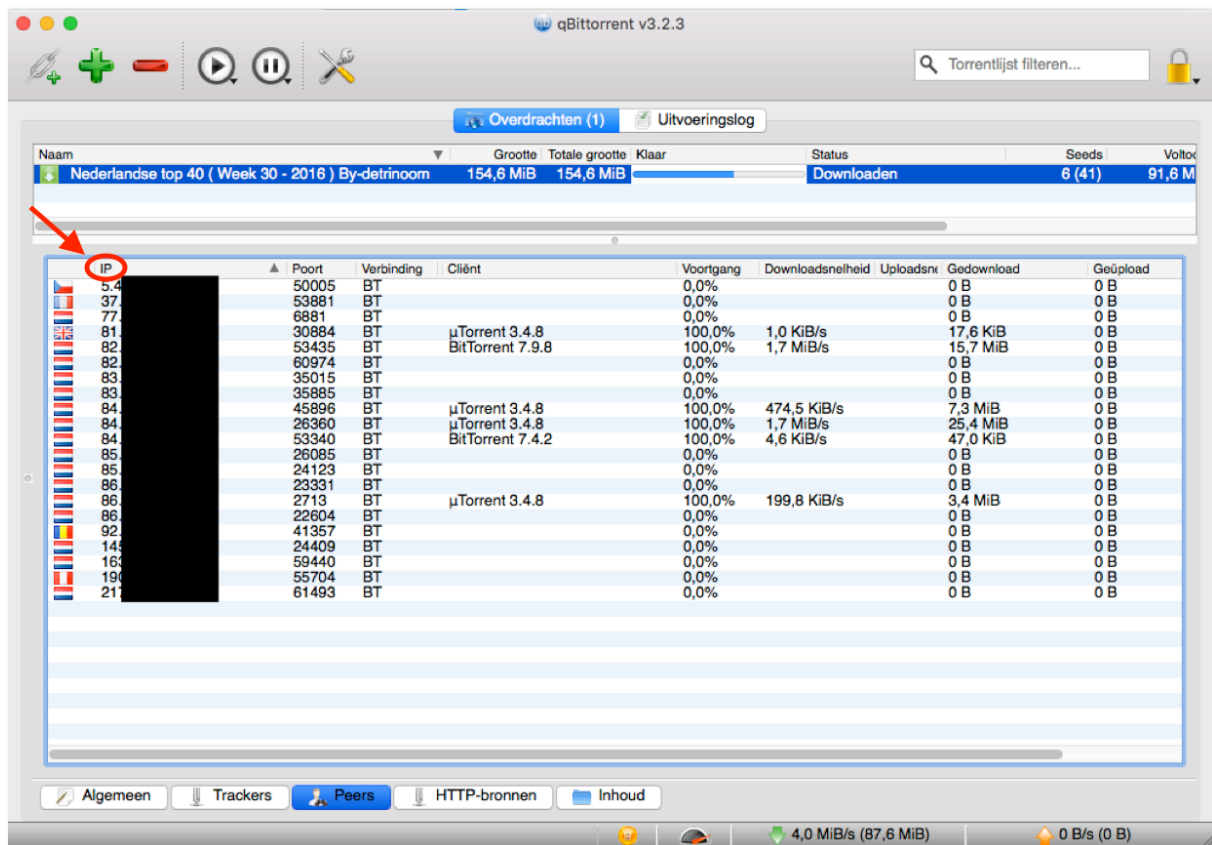
Medewerkers van BREIN monitoren populaire Bittorrent-indexeringswebsites en Popcorn Time op torrents die verwijzen naar bepaalde (mede) op Nederland gerichte

auteursrechtelijk beschermde werken van bij BREIN aangesloten rechthebbenden (o.a. Nederlandse of Nederlands ondertitelde films, Nederlandse muziekalbums of e-books en andere entertainmentcontent van BREIN's aangeslotenen waarin Nederlanders geïnteresseerd zijn), die op het Bittorrent-netwerk zonder toestemming worden uitgewisseld. Daarbij zijn de titels van de aangeboden torrentbestanden een indicatie. BREIN zoekt enkel naar auteursrechtelijk beschermde werken waarvan zij weet dat er door de rechthebbenden geen toestemming is verleend voor het verveelvoudigen/openbaar maken via het Bittorrent netwerk en met betrekking waartoe BREIN uitdrukkelijk gevolmachtigd is handhavend op te treden.

De medewerkers van BREIN openen torrents die verwijzen naar (mede) op Nederland gerichte auteursrechtelijk beschermde werken die zonder toestemming worden aangeboden vervolgens in AFLU. Door het openen van een torrent wordt inzicht verkregen in het specifieke bestand waarnaar de torrent verwijst. Het is immers dit specifieke bestand dat door de houders van de IP-nummers onderling wordt uitgewisseld in die specifieke zwerm. De uitwisseling van elk ander bestand dat de houder van een IP-nummer (dan wel een derde die van dat IP-nummer gebruik maakt) eventueel deelt, vindt plaats in telkens weer een andere zwerm en daar wordt door BREIN geen inzicht in verkregen.

Door het aanklikken van de torrent en deze te openen in AFLU, wordt de medewerker van BREIN deelnemer in de zwerm waarin het betreffende werk wordt uitgewisseld en krijgt hij inzicht in de IP-nummers van de overige deelnemers in de zwerm. Bij (vrijwel) alle desktop Bittorrent clients is dit laatste gebruikelijk.

Het IP-nummer is de enige unieke identifier die gebruikers in een zwerm van elkaar te zien krijgen. Bittorrent-gebruikers zijn er mee bekend, of kunnen dat redelijkerwijze zijn, dat eenieder kan zien met welke IP-nummers zij verbinding maken bij het up- en downloaden via het Bittorrent netwerk. Naast het IP-nummer delen gebruikers in de regel ook gegevens met betrekking tot de gebruikte software client en het gebruikte poortnummer. Hieronder is een schermafbeelding opgenomen van een gewone Bittorrent-client die populair is onder consumenten en waar duidelijk zichtbaar is met welke IP-nummers content wordt uitgewisseld (de anonimisering is specifiek door BREIN aangebracht in deze illustratie).



De IP-nummers die worden aangetroffen in een zwerm die door BREIN is geopend, worden automatisch opgeslagen in AFLU. BREIN-medewerkers blijven vanuit het oogpunt van privacy by default telkens zo kort in de zwerm als nodig is voor het verzamelen van het benodigde bewijs.

BREIN neemt uitsluitend deel aan reeds bestaande zwermen van torrents die door derden zijn geüpload, en creëert dus zelf geen zwermen.

5.2 Waarschuwingen

BREIN zal allereerst gedurende een periode van zes maanden beginnen met het voeren van een op inbreukmakende Bittorrent-gebruikers gerichte waarschuwingscampagne. De waarschuwingscampagne bestaat uit het sturen van verzoeken aan ISP's om notificaties door te sturen aan gebruikers die in een zwerm zijn aangetroffen waarmee inbreukmakende content zoals hierboven beschreven wordt uitgewisseld. Met het oog op de proportionaliteit zullen door BREIN maximaal 1000 van dergelijke verzoeken per maand aan ISP's worden gestuurd. BREIN zal zowel met een persbericht in de media als op haar website aankondigen wanneer de FLU-waarschuwingscampagne van start gaat.

Niet iedere willekeurig inbreukmaker van wie het IP-nummer door BREIN in een zwerm is aangetroffen komt bovendien in aanmerking voor een notificatie. Uitsluitend aan ISP's van abonnees van wie het IP-nummer steekproefsgewijs gedurende een periode van vier weken tenminste twee keer door BREIN is aangetroffen, zal door BREIN worden verzocht een notificatie door te sturen.

De criteria die BREIN hanteert voor het sturen van notificaties zijn:

- Is het aangetroffen IP-nummer betrokken geweest bij het uitwisselen van (delen van) entertainmentbestanden met titels van aangeslotenen bij BREIN;
- Is het IP-nummer in beheer bij een Nederlandse ISP;
- Is in een periode van vier weken een IP-nummer van een uploader minimaal twee keer in een Bittorrent-zwerm aangetroffen. Dit kan - met een tussenpoos van minimaal 7 uur - twee keer in dezelfde zwerm zijn of in twee verschillende zwermen.

De IP-nummers die voldoen aan deze criteria worden na verzending van een notificatie (via de ISP) niet verder verwerkt en worden vernietigd. Voorwaarde is wel dat ISP's bereid zijn om de notificaties door te sturen, anders zal BREIN hen verzoeken de e-mailadressen van de betreffende abonnees te verstrekken, zodat BREIN die zelf een notificatie kan sturen. Mocht een ISP ook dat weigeren, dan zal BREIN in rechte medewerking van de ISP vorderen.

In de notificatie worden de uploaders gewaarschuwd, dat met hun handelwijze inbreuk wordt gemaakt op auteursrechten van bij BREIN aangesloten rechthebbenden en dat zij dus onrechtmatig handelen, waardoor schade wordt berokkend aan de rechthebbenden, omdat die daardoor een passende beloning voor het gebruik van hun werk mislopen. Deze doelgroep van de waarschuwingscampagne bestaat grotendeels uit uploaders die belangrijk zijn voor de instandhouding van de uitwisseling van inbreukmakende bestanden met entertainment content, dan wel uit uploaders die in potentie tot die groep behoren.

De waarschuwingstekst van de notificaties zal erop gericht zijn een zo groot mogelijk effect te sorteren. De uploaders in kwestie zullen in de notificatie worden geattendeerd op de legale alternatieven voor het inbreukmakende gebruik van Bittorrent. BREIN zal in haar notificatieverzoeken aan de ISP's in elk geval aanbevelen om in de notificaties een verwijzing op te nemen naar een voorlichtende site als <https://auteursrecht.nl/kies-voor-legale->

[content](#) waar onder andere de beschikbare legale digitale distributiemodellen van entertainment content overzichtelijk staan vermeld.

Teneinde een zo groot mogelijk effect te sorteren is het belangrijk dat het sturen van de notificaties zo efficiënt mogelijk gebeurt. Met het oog daarop is het van cruciaal belang dat BREIN erin slaagt afspraken te maken met de ISP's over de wijze waarop de houders van de aangetroffen IP-adressen kunnen worden benaderd. De ISP's zal verzocht worden hetzij de notificaties aan hun abonnees door te sturen, hetzij e-mailadressen te verstrekken waarop de betreffende abonnees door BREIN zelf bereikt kunnen worden.

Indien ISP's aan die laatste optie de voorkeur geven, zijn er wederom twee mogelijkheden: ofwel de ISP's verstrekken BREIN de e-mailadressen waarmee zijzelf contact onderhouden met hun abonnees, ofwel zij stellen de betreffende abonnees ervan op de hoogte dat BREIN voornemens is hen een notificatie te sturen naar speciaal voor dit doel aangemaakte nieuwe e-mailadressen. Deze laatste optie brengt met zich mee dat BREIN dan – zoals ook het geval is wanneer de ISP's de notificaties zelf door zouden sturen - nog steeds geen enkel aanknopingspunt heeft met betrekking tot de identiteit van de personen in kwestie, waardoor de inbreuk op hun privacy zo minimaal mogelijk blijft, wat in overeenstemming is met het privacybeleid dat BREIN voert (privacy by default).

BREIN zal onderzoek laten verrichten naar het effect van het sturen van de notificaties. Dit onderzoek zal worden verricht door onderzoeksbureau Kantar dat voorafgaand aan de voorlichtende fase van FLU het inbreukmakende gebruik van Bittorrent in kaart zal brengen. Na verloop van de zes maanden waarin BREIN uitsluitend notificaties zal hebben gestuurd, zal worden gemeten of, en in welke mate de notificaties effect hebben gesorteerd.

Indien de samenwerking met de ISP's naar wederzijdse tevredenheid verloopt en het inbreukmakende gebruik van Bittorrent significant mocht blijken af te nemen, dan zal deze fase van FLU met nog eens zes maanden verlengd kunnen worden, waarna BREIN nogmaals onderzoek zal laten doen naar de effectiviteit. Zolang het sturen van notificaties een effectief middel blijkt te zijn bij het terugdringen van de grootschalige inbreuk die met Bittorrent wordt gemaakt, zal BREIN er niet toe overgaan om handhavend op te treden. Maar de mogelijkheid om dat op enig moment toch te doen blijft aanwezig. Mocht het uitsluitend sturen van de notificaties onvoldoende effect blijken te sorteren of mocht het effect in de loop der tijd blijken af te nemen, dan kan dat voor BREIN een reden zijn om te besluiten het effect van de voorlichting te ondersteunen door alsnog over te gaan tot handhaving tegen de doelgroep waarop BREIN zich met FLU richt.

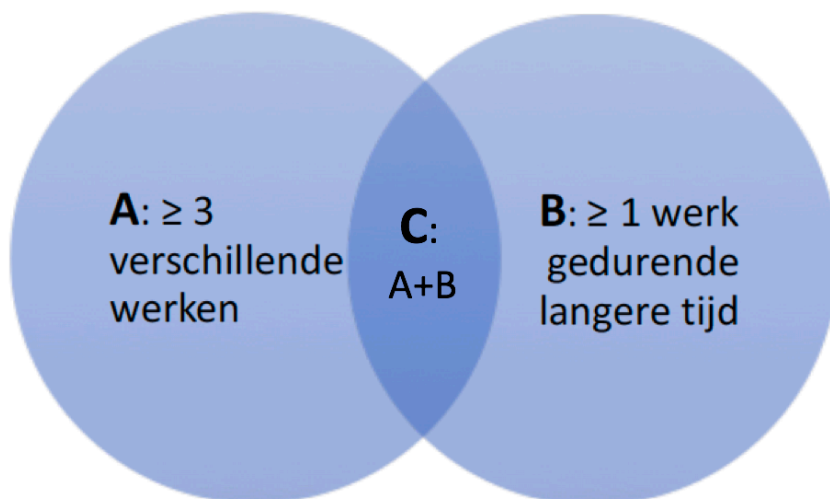
BREIN houdt ook rekening met de mogelijkheid dat ISP's niet bereid zijn om in overleg afspraken met BREIN te maken over medewerking bij het sturen van notificaties. BREIN zal zich in dat geval genooddacht zien om via de rechter medewerking af te dwingen. Naar verwachting zal een gang naar de rechter de effectiviteit van de notificatiefase van FLU ernstig belemmeren, omdat het dan langer duurt voordat er notificaties gestuurd kunnen worden en het aantal gestuurde notificaties naar alle waarschijnlijkheid een stuk lager zal uitvallen. In een dergelijke situatie zal BREIN hoogstwaarschijnlijk na de minimale periode van zes maanden al overgaan tot handhaving tegen de uploaders in de doelgroep van wie de IP-adressen in de Bittorrent-zwermen worden aangetroffen.

5.3 Handhaving

De mogelijke handhaving met FLU zal zich richten op uploaders van wie het IP-nummer – op zijn vroegst zes maanden na het begin van de waarschuwingscampagne - in steekproeven minimaal drie keer wordt aangetroffen in Bittorrent-zwermen waarin zonder toestemming van de rechthebbenden bestanden met entertainment content worden uitgewisseld. Zoals hierna verder zal worden toegelicht gaat het om uploaders waarvan is vastgesteld dat zij binnen een bepaalde periode verschillende beschermde werken uploaden en om uploaders van wie is vastgesteld dat zij als 'seeder' van illegaal uitgewisselde content functioneren en dus gedurende langere tijd bepaalde content aanbieden.

Mocht BREIN besluiten dat naast het sturen van notificaties ook daadwerkelijke handhaving noodzakelijk is, dan hanteert BREIN de volgende criteria voor het starten van een handhavingsactie:

- Is het aangetroffen IP-nummer betrokken geweest bij het uitwisselen van (delen van) entertainmentbestanden met titels van aangeslotenen bij BREIN;
- Is het IP-nummer in beheer bij een Nederlandse ISP;
- Is in een periode van vier weken een IP-nummer van een uploader drie keer of vaker in een Bittorrent-zwerm aangetroffen. Hierbij geldt dat een IP-nummer van een gebruiker drie of meer keer per vier weken wordt aangetroffen in:
 - A. hetzij telkens een andere Bittorrent-zwerm,
 - B. hetzij in dezelfde Bittorrent-zwerm met een tussenpoos van meer dan zeven uur tussen de vaststellingen,
 - C. hetzij een combinatie van deze beide varianten,



IP-nummers die aan bovenstaande criteria voldoen komen in aanmerking voor een handhavingsactie.

Deze beide groepen uploaders zijn relevant voor het in stand houden van het illegale aanbod op het Bittorrent-netwerk, omdat zij een relevante rol vervullen voor het evenwicht in het

systeem waardoor de uitwisseling met Bittorrent van illegale entertainmentbestanden mogelijk wordt gemaakt. Als zoveel mogelijk gebruikers evenveel up- als downloaden functioneert het Bittorrent-systeem namelijk optimaal⁹. Daarbij zij opgemerkt dat een enkele ongeautoriseerde up- of download zelfstandig inbreuk maakt op intellectuele eigendomsrechten. BREIN heeft er evenwel voor gekozen enkel handhavingsacties te starten jegens gebruikers die voldoen aan bovenstaande criteria, om daarmee een extra proportionaliteitstoets in te bouwen.

Tegen uploaders die vaker dan drie keer worden aangetroffen onderneemt BREIN daarnaast de volgende stappen, indien BREIN dit nodig acht voor een effectieve handhaving tegen verdere inbreuk op de auteursrechten van de aangeslotenen bij BREIN.

1) *Opvragen contactgegevens*

Uit de IP-nummers zelf kan BREIN niet de identiteit van de gebruiker afleiden, zodat de gebruiker niet door BREIN kan worden aangeschreven. Voor het sturen van waarschuwingen is het voor BREIN niet noodzakelijk de identiteit van de gebruikers te kennen. Indien ISP's notificaties van BREIN door willen sturen, zal BREIN dan ook geen enkel aanknopingspunt omtrent de identiteit van hun klanten krijgen. Aan ISP's die niet bereid zijn notificaties door te sturen, zal BREIN verzoeken – en eventueel in rechte vorderen - de e-mailadressen van de betreffende abonnees te verstrekken, teneinde die zelf een notificatie te kunnen sturen.

In de gevallen waarin overgegaan wordt tot handhaving is de noodzaak de identiteit van de gebruikers te kennen er voor BREIN wel. De eerste stap zal dan derhalve zijn dat BREIN de NAW-gegevens van de abonnees, gekoppeld aan de in aanmerking komende IP-nummers, zal opvragen bij de betreffende ISP. Indien een ISP niet bereid is vrijwillig aan een verzoek tot afgifte van NAW-gegevens te voldoen, zal BREIN mogelijk overgaan tot het starten van een gerechtelijke procedure jegens de ISP om afgifte van de NAW-gegevens te vorderen.

2) *Mogelijke handhavingsacties*

Nadat BREIN de contactgegevens van de betrokkene heeft verkregen zal zij, afhankelijk van de omstandigheden van het geval, de volgende stappen kunnen nemen:

- a. aan de abonnees van ISP's die niet bereid zijn notificaties op verzoek door te sturen, stuurt BREIN zelf per e-mail een waarschuwing zonder dat verder handhavingsacties zullen worden ondernomen, in de andere gevallen worden de notificaties door de ISP's verzonden;
- b. In de gevallen waarin een IP-nummer in vier weken tijd drie keer in een zwerm is aangetroffen, stuurt BREIN een waarschuwing aan de betrokkene wiens internetverbinding wordt gebruikt om inbreuk te maken, waarin hij wordt gesommeerd schriftelijk te bevestigen dat hij de inbreuk zal staken en gestaakt houden en hem wordt medegedeeld, dat wanneer hij dat niet doet BREIN nadere (rechts)maatregelen tegen hem zal treffen. Indien de betrokkene de gevraagde

⁹ In Bittorrent-jargon wordt van 'peers' die een bestand niet 'seeden', d.w.z. een compleet gedownload bestand beschikbaar houden voor mede-peers, gezegd dat zij 'hit 'n run' plegen. Dit type gebruiker downloadt in verhouding veel meer dan dat zij uploadt, waardoor zij de werking van Bittorrent verstoort.

- bevestiging stuurt, houdt het handhavingstraject in beginsel op, tenzij het IP-nummer van de betrokkene daarna nogmaals in een zwerm met inbreukmakende content wordt aangetroffen;
- c. In de gevallen waarin een IP-nummer vaker dan drie keer in vier weken in een zwerm met inbreukmakende content wordt aangetroffen of na de onder b bedoelde bevestiging nogmaals in een inbreukmakende zwerm wordt aangetroffen, tracht BREIN een minnelijke schikking met de betrokkene te treffen bestaande uit een onthoudingsverklaring waarin een boetebeding is opgenomen. Er wordt geen schadevergoeding gevraagd;
 - d. Indien de betrokkene niet op eerste verzoek een schikking treft met BREIN en BREIN door toedoen van de betrokkene extra kosten moet maken (bijvoorbeeld doordat een externe advocaat moet worden ingeschakeld), verlangt BREIN naast de ondertekening van een onthoudingsverklaring met boetebeding tevens een tegemoetkoming in de gemaakte kosten;
 - e. Indien de betrokkene geen minnelijke schikking wenst te treffen, stuurt BREIN hem een dagvaarding, waarin een verbod met dwangsommen en vergoeding van de kosten op voet van art. 1019h Rv kan worden gevorderd conform de indicatietarieven in IE-zaken¹⁰;
 - f. In gevallen waarin het IP-nummer na het treffen van een minnelijke schikking met boetebeding (stap c of d) opnieuw wordt aangetroffen - zal door BREIN opnieuw een minnelijke schikking worden beproefd waarbij BREIN aanspraak maakt op het bedrag aan verbeurde boetes; indien eerder een rechterlijk vonnis met een verbod op verbeurde van dwangsommen is gewezen (stap e), zal BREIN aanspraak maken op de verbeurde dwangsommen;
 - g. Indien een inbreukmaker na recidive geen minnelijke schikking wenst te treffen volgt een dagvaarding, waarin naast verbeurde boetes vergoeding van kosten zal worden gevorderd op voet van art. 1019h Rv. Indien jegens een recidivist al eerder een gerechtelijke veroordeling met dwangsommen is uitgesproken en hij geen schikking wenst te treffen, zal BREIN het vonnis inclusief dwangsommen executeren.

BREIN zal steeds per geval beoordelen of de hierboven genoemde stappen wenselijk zijn en per geval een beslissing nemen. BREIN kan altijd beslissen om minder zware maatregelen tegen een betrokkene te nemen dan de hierboven genoemde maatregelen.

In alle gevallen waarin BREIN (via de ISP's of anderszins) de beschikking heeft gekregen over de contactgegevens (a t/m g), zal BREIN zo spoedig mogelijk de betrokkene aanvullend inlichten over de verwerking van zijn persoonsgegevens en het doel van de gegevensverwerking. BREIN beoogt met deze aanpak tevens een waarschuwend signaal af te geven aan zowel potentiële nieuwe gebruikers van Bittorrent als aan incidentele gebruikers, waardoor het waarschuwend effect wordt versterkt.

¹⁰ <https://www.rechtspraak.nl/SiteCollectionDocuments/indicatietarieven-in-ie-zaken-rechtbanken-04-2017.pdf>

Ook als BREIN besluit over te gaan tot het ondernemen van handhavingsacties blijft BREIN maximaal 1000 notificaties per maand sturen aan uploaders die twee keer in vier weken in de steekproeven worden aangetroffen, zoals hierboven beschreven onder 5.2

6. Vastgelegde gegevens; toegang; verstrekking; bewaartermijnen

6.1 Verzamelde gegevens

BREIN verzamelt in het kader van FLU IP-nummers die in zwermen, waarmee inbreukmakende content wordt uitgewisseld, worden aangetroffen. Van Bittorrent-gebruikers kan op eenvoudige manier het IP-nummer worden achterhaald dat zij gebruiken en welke ISP het betreffende IP-nummer in beheer heeft. In andere unieke identificatoren van de inbreukmakers verkrijgt BREIN zonder medewerking van de ISP's geen inzicht. De verzamelde IP-nummers zullen worden opgeslagen op een speciaal voor AFLU ingerichte server.

In voorkomende gevallen kan het poortnummer, altijd in combinatie met het IP-nummer, van belang zijn bij identificatie indien bijvoorbeeld meer personen gebruik maken van hetzelfde IP-nummer maar via verschillende poorten. Ook de gebruikte BitTorrent software client kan een rol spelen bij de uiteindelijke identificatie van de inbreukmaker, evenals het eveneens vastgelegde tijdstip waarop de inbreuk plaatsvond en het geüploade auteursrechtelijk beschermde werk/het inbreukmakende bestand zelf. Deze gegevens worden ook door BREIN verwerkt maar zijn als zodanig geen unieke identificatoren.

Slechts de ISP die de inbreukmakers toegang verleent tot het internet, is van de identiteit van haar abonnees, de houders van de betreffende IP-nummers, op de hoogte. BREIN zal zich daarom tot de ISP's in kwestie richten met verzoeken om de e-mailadressen te verstrekken, voor zover zij geen notificaties wensen door te sturen. Indien wordt overgegaan tot de handhavingfase (na minimaal zes maanden na aanvang van de waarschuwingscampagne) zullen van alle abonnees van wie het IP-nummer vanaf dat moment in vier weken drie keer of vaker is aangetroffen in inbreukmakende Bittorrent-zwermen de NAW-gegevens bij hun ISP's worden opgevraagd. Die categorie inbreukmakers wil BREIN rechtstreeks aanspreken. Daarvoor is het dus noodzakelijk dat het IP-nummer waarvan bij het maken van de inbreuk gebruik wordt gemaakt, eerst door BREIN aan de ISP wordt verstrekt.

De NAW-gegevens van laatstgenoemde categorie die BREIN van de ISP's verkrijgt, zullen worden verwerkt in het Antipiraterij databestand, dat door het College Bescherming Persoonsgegevens (CBP, thans AP) rechtmatig is verklaard bij besluit van 16 april 2004 (z2003-1660).

6.2 Toegang tot de gegevens

Medewerkers van BREIN hebben slechts toegang tot die gegevens die noodzakelijk zijn om het nagestreefde doel te bereiken. Binnen BREIN zelf hebben uitsluitend die medewerkers die betrokken zijn bij het verzamelen van de IP-nummers met AFLU toegang tot alle verzamelde IP-nummers.

6.3 Verstreking van de gegevens

In het kader van de waarschuwingcampagne zal BREIN IP-nummers verstrekken aan ISP's in de maximaal 1000 doorzendverzoeken per maand met betrekking tot Bittorrent-gebruikers van wie het IP-nummer bij steekproeven in een periode van vier weken twee keer of meer is aangetroffen in een zwerm met inbreukmakende content. Dit zal slechts een fractie zijn van alle IP-nummers die deel uitmaken van de te onderzoeken Bittorrentzwermen, zo heeft BREIN met de ervaring met BOB geleerd (zie hieronder fig.1 op p.21). Het verzoek van BREIN zal zijn om de waarschuwingen door te sturen aan de betreffende abonnee. Mits aan dit verzoek tegemoet wordt gekomen, verkrijgt BREIN daarbij dus niet de e-mailadressen of andere contactgegevens van de abonnees. Indien de ISP ervoor kiest om de notificaties door BREIN te laten sturen, verkrijgt BREIN wel de e-mailadressen van de betreffende abonnees. BREIN zal deze e-mailadressen direct na het versturen van de waarschuwing uit haar systeem verwijderen.

Indien BREIN tot de conclusie komt dat het uitsluitend sturen van notificaties niet (meer) het gewenste effect sorteert en besluit de waarschuwing en voorlichting te ondersteunen met daadwerkelijke handhaving, neemt BREIN na het begin van de mogelijke handhavingcampagne (minimaal zes maanden na aanvang van de waarschuwingcampagne) tevens contact op met de ISP van de houder van een IP-nummer met een verzoek tot verstrekking van NAW-gegevens van een abonnee, indien is vastgesteld dat dit IP-nummer in een periode van vier weken drie keer of vaker is gebruikt (door de houder zelf dan wel door een derde die via dit nummer actief is geweest) om middels Bittorrent ongeautoriseerd bestanden uit te wisselen en dat daarmee inbreuk is gemaakt op de rechten van de rechthebbenden die BREIN vertegenwoordigt. Dit zullen maximaal 500 verzoeken per maand betreffen.

De Bittorrent-zwermen die BREIN zal onderzoeken, zullen naar verwachting ook deels bestaan uit computers van buitenlandse gebruikers met buitenlandse IP-nummers. FLU is echter gericht op Nederlandse gebruikers. Alle buitenlandse IP-nummers zullen dan ook sowieso buiten beschouwing worden gelaten. Dit is in overeenstemming met het principe van privacy by default. Praktisch betekent dit, dat AFLU zodanig wordt geprogrammeerd dat buitenlandse IP-nummers automatisch direct worden geanonimiseerd door het laatste deel van het IP te vervangen door een 'x'¹¹, wat tegemoet komt aan het uitgangspunt van privacy by design. Uitsluitend aan de ISP's die weigeren notificaties door te sturen en aan de ISP's van de houders van Nederlandse IP-nummers die drie keer of vaker in bittorrent-zwermen worden aangetroffen, zal dus mogelijk een verzoek worden gestuurd om contactgegevens te verstrekken.

De IP-nummers zullen uitsluitend worden verstrekt aan de ISP's die ze in beheer hebben. Dit is noodzakelijk omdat slechts die ISP's beschikken over de contactgegevens van hun abonnees. BREIN heeft zelf geen kennis van de identiteit of de contactgegevens van de houders van de IP-nummers en is voor het verkrijgen van contactgegevens dus aangewezen op de medewerking van de ISP's. De verzoeken aan de ISP's zullen aan de geëigende afdelingen (abuse of juridische zaken) van de desbetreffende ISP per e-mail en per aangetekende post of koerier worden toegezonden.

¹¹ b.v. IP-nummer 151.139.128.10 zou automatisch 151.139.128.x worden

FLU past binnen de huidige gangbare werkwijze die mede is gebaseerd op de rechtspraak en ook in de algemene voorwaarden van ISP's nader is geregeld. In die gevallen waarin abonnees betrokken zijn bij inbreukmakende handelingen, kunnen rechthebbenden de ISP's daarop wijzen onder verstrekking van het IP-nummer met een omschrijving van (het inbreukmakende karakter) van de gepleegde handelingen, teneinde nadere actie mogelijk te maken. Dit is noodzakelijk nu op ISP's geen algemene verplichting rust om het gedrag van hun abonnees te monitoren op het maken van inbreuk en dat dus ook niet doen¹². De ISP's wijzen hun klanten erop dat het niet is toegestaan om inbreuk op intellectuele eigendomsrechten van derden te maken en dat als dat toch gebeurt, de ISP contact hierover op kan nemen¹³. De ISP's behouden zich ook het recht voor de gegevens van hun klanten te verstrekken als sprake is van illegaal downloaden¹⁴ - en zijn dit op grond van de wet en jurisprudentie ook verplicht¹⁵. Klanten kunnen verder bijvoorbeeld gehouden zijn de instructies van de ISP op te volgen¹⁶. Aldus is duidelijk dat ISP's er op zijn ingericht om informatie van derden over mogelijke inbreukmakende handelingen van hun klanten te ontvangen en te verwerken, welke informatie ook gegevens over mogelijke strafbare feiten kan omvatten. Vrijwel zonder uitzondering benadrukken ISP's in de algemene voorwaarden die zij hanteren, dat zij zorgvuldig met de persoonsgegevens van hun klanten omgaan¹⁷. Persoonsgegevens worden niet langer dan nodig is bewaard en ook niet langer dan wettelijk toegestaan of verplicht is. Er worden passende technische en organisatorische maatregelen genomen om persoons-, verkeers- en gebruiksgegevens te beschermen¹⁸.

De IP-nummers zullen behalve aan deze ISP's, niet aan derden worden verstrekt. De gegevens uit het FLU-systeem zullen op geen enkele wijze en met geen enkel ander oogmerk verder worden verwerkt dan om te waarschuwen of in of buiten rechte op te treden tegen (en waar mogelijk schikkingen te treffen met) de betrokken houders van de IP-nummers.

Indien BREIN een betrokkene in rechte aanspreekt om intellectuele eigendomsrechten te Handhaven, zullen de persoonsgegevens van de betrokkene noodzakelijkerwijs worden opgenomen in processtukken die worden verstrekt aan een beperkte groep derden, waaronder de betreffende rechtbank en mogelijkerwijs een externe advocaat van BREIN.

6.4 Bewaartermijn van de gegevens

Persoonsgegevens zullen niet langer worden bewaard dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verwerkt.

¹² art. 15 lid 1 van de EU-Richtlijn 2000/31

¹³ zie bijv. art. 17 van de algemene voorwaarden van Ziggo

(https://cdn.vodafoneziggo.nl/content/dam/ziggo/voorwaarden/Algemene_voorwaarden_Ziggo_per_1_dece_mber_2019.pdf) en art. 7.2 van de algemene voorwaarden van KPN

(<https://www.kpn.com/w3/file?uuid=5a8ed28d-a59c-4c38-8d22-4e9d1fbb70cd&owner=8de86c61-bdc8-4848-872e-e5b380e682fc&contentid=12621>)

¹⁴ zie bijv. art. 4.2.4 van het privacy statement van KPN

¹⁵ HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers),

¹⁶ zie bijv. art. 5.8 van de algemene voorwaarden van XS4ALL <https://www.xs4all.nl/klant/voorwaarden/>

¹⁷ zie bijv. het privacy statement van KPN <https://www.kpn.com/algemeen/missie-en-privacy-statement/privacy-statement.htm>

¹⁸ zie bijv. §5.7 van het privacy statement van Vodafone Ziggo <https://cdn-master.aem.prod.aws.ziggo.io/content/dam/ziggo/privacy/vodafone-ziggo%20privacy-statement.pdf>

In het FLU-systeem zal een aantal categorieën IP-nummers naar bewaartermijn worden onderscheiden.

a) Buitenlandse IP-nummers die in beheer zijn bij buitenlandse ISP's worden automatisch onmiddellijk geanonimiseerd.

b) IP-nummers van houders met een Nederlandse ISP die slechts één maal in een onderzochte Bittorrent-zwerm zijn aangetroffen, of ten aanzien waarvan BREIN om een andere reden besluit geen waarschuwing te sturen of handhavingsactie te ondernemen, worden twee weken na de vier weken termijn waarbinnen deze gegevens worden verzameld, vernietigd.

c) Een doorstuurverzoek, respectievelijk een notificatie door BREIN zal niet later dan twee weken na afloop van de verzameltermijn van vier weken respectievelijk na ontvangst door BREIN van het adres van de abonnee worden verzonden. De termijn is alleen dan langer indien een ISP medewerking weigert aan het sturen van notificaties en BREIN genoodzaakt is dit in rechte af te dwingen. In dat geval zullen de betreffende IP-nummers onderdeel vormen van het procesdossier. IP-nummers van houders met een Nederlandse ISP ten aanzien waarvan een verzoek tot het sturen van een waarschuwing aan de ISP is verzonden, worden – indien met de ISP de afspraak is gemaakt dat het verzoek doorgestuurd wordt – één maand na versturen van het verzoek aan de ISP vernietigd en anders één maand na het sturen van een waarschuwing per e-mail door BREIN zelf. De voor de notificaties gebruikte e-mailadressen zullen direct na versturen van een notificatie worden vernietigd. Het bewaren van het IP-nummer gedurende de genoemde ene maand na versturing heeft louter als doel om als bewijs te kunnen worden gebruikt mocht een ontvanger van een voorlichtende waarschuwing hiertegen binnen die maand bezwaar maken.

Indien tot de handhavingsfase wordt overgegaan, gelden voorts de volgende bewaartermijnen:

d) IP-nummers van houders met een Nederlandse ISP, die voldoen aan alle criteria van 5.3, zonder dat de ISP van BREIN een NAW-verzoek heeft ontvangen, worden maximaal twee weken na afloop van de termijn van vier weken vernietigd. Daarmee is de bewaartermijn voor deze categorie maximaal zes weken.

Toelichting op categorie d: om te voorkomen dat IP-nummers worden verwerkt die niet ter zake dienend en bovenmatig zijn, hanteert BREIN een zo kort mogelijke termijn (twee weken na afloop van de verzameltermijn van vier weken) voor het sturen van een verzoek om verstrekking van identificerende gegevens aan de ISP, nadat is vastgesteld dat een IP-nummer drie keer of vaker in vier weken is aangetroffen. Wordt binnen de gestelde termijn om welke reden dan ook geen NAW-verzoek verstuurd, dan vernietigt BREIN de IP-nummers. BREIN heeft twee weken na afloop van de termijn van vier weken nodig om de maximaal 500 NAW-verzoeken aan de ISP's in kwestie te versturen. Een kortere termijn zou de kans op onnauwkeurigheid te veel vergroten.

Dit betekent dus dat alle IP-nummers maximaal zes weken worden bewaard, behalve de maximaal 500 IP-nummers per maand van houders van wie de ISP binnen uiterlijk zes weken na verzamelen van de gegevens een NAW-verzoek van BREIN heeft ontvangen en de maximaal 1.000 IP-nummers per maand van abonnees aan wie BREIN een waarschuwing wil versturen.

e) de maximaal 500 IP-nummers per maand van houders die voldoen aan de criteria onder 5.3 en van wie de ISP binnen uiterlijk zes weken na verzamelen van de gegevens een NAW-verzoek van BREIN heeft ontvangen, en de daarbij behorende NAW-gegevens die BREIN van de ISP ontvangt, worden door BREIN in het Antipiraterij databestand (besluit z2003-1660) bewaard. Hiervoor gelden de bewaartermijnen uit het Antipiraterij databestand. Dit zijn:

- Onderzoeksgegevens: maximaal vijf jaar na afsluiting van het dossier.
- Gegevens van betrokkenen waarmee een schikking is getroffen waarbij een onthoudingsverklaring met boetededing is afgegeven en gegevens van betrokkenen waartegen door BREIN een rechterlijk vonnis is behaald: maximaal 20 jaar.

Bij het bepalen van bovenstaande termijnen, heeft BREIN rekening gehouden met de diverse in het geding zijnde belangen van de betrokken partijen, met name belang van de betrokkene dat zijn gegevens niet te lang worden bewaard en correct worden verwerkt, het belang van ISP's om van BREIN correcte informatie te ontvangen en het belang van BREIN om uitsluitend correcte informatie in het anti-piraterij databestand op te nemen.

7. Wettelijke grondslag

De wettelijke grondslag voor de verwerking van IP-nummers is artikel 6 sub f AVG. De verwerking van IP-nummers is noodzakelijk voor de behartiging van het gerechtvaardigde belang van BREIN zelf en van de rechthebbenden waarvan BREIN de belangen behartigt. In hoofdstuk 2 van dit protocol is de omvang van de inbreuken die via Bittorrent netwerken plaatsvinden en de schade die rechthebbenden daardoor lijden omschreven. Het belang bij optreden tegen deze grootschalige inbreuk is groot. Omdat Bittorrent netwerken worden gebruikt zonder dat daarbij direct herleidbare gegevens van gebruikers te zien zijn, is het verwerken van het IP-nummer in deze context het enige aanknopingspunt om de personen die vermoedelijk inbreukmakende handelingen verrichten op het spoor te komen.

BREIN is van mening dat het belang bij het verminderen van grootschalige inbreuk via Bittorrent, in dit geval en onder de door BREIN getroffen waarborgen, zwaarder moet wegen dan de privacybelangen van de betrokkenen. Dit geldt zowel voor de waarschuwingscampagnes als de mogelijke handhavingsacties.

BREIN krijgt bij de waarschuwingscampagnes op geen enkele wijze inzicht in de identiteit van de betreffende gebruikers, tenzij ISP's weigeren notificaties door te sturen en BREIN e-mailadressen zal moeten opvragen zodat BREIN zelf de notificaties kan opsturen. Dit laatste zou bij voorkeur kunnen gebeuren naar speciaal voor dit doel aangemaakte nieuwe e-mailadressen, waardoor de anonimiteit van de gebruikers alsnog gewaarborgd blijft (maar ook deze route vergt medewerking van de ISP's). Voor BREIN is het sturen van notificaties een effectieve methode om het aantal inbreuken met Bittorrent aanzienlijk te verminderen

en nieuwe inbreuken te voorkomen. Omdat het aantal inbreukmakers dat een notificatie ontvangt ook nog eens gelimiteerd is, dient het belang van BREIN hier de doorslag te geven.

Dit geldt ook voor de mogelijke handhavingsacties. Het opvragen van identificerende gegevens van de Bittorrent- uploaders die voldoen aan de criteria onder 5.3 kan van groot belang blijken te zijn voor BREIN en de bij haar aangesloten rechthebbenden om hun intellectuele eigendom te kunnen beschermen. Indien alleen waarschuwingen niet voldoende effect hebben, is het volgens BREIN noodzakelijk de mogelijkheid te hebben om deze categorie inbreukmakers aan te kunnen spreken op hun gedrag met het doel dit ten goede te wijzigen. Bij de doelgroep waar de mogelijke handhavingsmaatregelen op gericht zijn, prevaleert daarom BREIN's handhavingsrecht en haar belang om civiele rechtsvorderingen in te kunnen stellen. Het verzamelen van persoonsgegevens is op grond van de rechtspraak ook gerechtvaardigd wanneer voldoende aannemelijk is dat sprake is van onrechtmatig handelen jegens degene die over de persoonsgegevens wenst te beschikken.¹⁹

Door de waarschuwingscampagne van FLU en door de publiciteit die dit met zich mee zal brengen, zullen veel inbreukmakers naar verwachting afzien van verder illegaal gebruik van Bittorrent. Indien dit niet voldoende effect sorteert (bijvoorbeeld omdat het niet mogelijk blijkt deze snel en effectief uit te voeren omdat ISP's niet vrijwillig willen meewerken) en tot handhavingsacties moet worden overgegaan, zullen de handhavingsacties tegen maximaal 500 uploaders per maand die BREIN vervolgens zal ontplooien, het effect verder versterken. Met het FLU-systeem beoogt BREIN te bereiken dat consumenten die zich niet volledig bewust zijn van de mogelijke gevolgen van illegaal Bittorrent-gebruik, hun gedrag zullen beteren zonder in eerste instantie blootgesteld te hoeven worden aan inbreuk op hun privacy - hoe gering ook- en mogelijke handhaving. Zodoende voorkomt het FLU-systeem dat een veel grotere categorie gebruikers mogelijk bloot komen te staan aan handhavingacties.

De Autoriteit Persoonsgegevens heeft in eerdere besluiten ten aanzien van het verwerken van IP-adressen van uploaders van inbreukmakende content (onder meer het besluit inzake anti-piraterijbestand BREIN, z2003-1660; besluit inzake bittorrent onderzoeksbestand BREIN, z2015-00574 en besluit inzake Dutch FilmWorks, z2017-02053) geconcludeerd dat persoonsgegevens over personen waartegen een min of meer gegronde verdenking bestaat van handelingen die inbreuk maken op auteursrecht, aangemerkt moeten worden als strafrechtelijke persoonsgegevens. Hoewel BREIN zich afvraagt of er bij een verwerking van persoonsgegevens uitsluitend ten behoeve van civielrechtelijke handhaving daadwerkelijk sprake kan zijn van strafrechtelijke persoonsgegevens, doet zij – voor zover nodig – een beroep op de artikelen 32 sub d en 33 lid 2 sub b van de UAVG nu de verwerking strekt ter bescherming van de belangen van BREIN en haar aangeslotenen en de mogelijk strafbare feiten de belangen van BREIN en haar aangeslotenen rechtstreeks treffen, en omdat de verwerking noodzakelijk is voor de (voorbereiding op) een eventuele instelling, uitoefening of onderbouwing van een rechtsvordering.

Op grond van artikel 33 lid 2 sub b van de UAVG mogen persoonsgegevens van strafrechtelijke aard worden verwerkt door de verwerkingsverantwoordelijke die deze gegevens ten eigen behoeve verwerkt, ter bescherming van zijn belangen. Het moet daarbij

¹⁹ Vgl. HR 25 november 2005, NJ 2009, 551 (Lycos/Pessers) en Vzr. Rechtbank Amsterdam 14 mei 2013, IER 2013/62 (BREIN/ING)

gaan om strafbare feiten die zijn of naar verwachting zullen worden gepleegd jegens hem of jegens personen die in zijn dienst zijn. BREIN zal enkel gegevens verzamelen van deelnemers aan een Bittorrent-zwerm waarbinnen titels worden uitgewisseld van bij haar aangesloten rechthebbenden, die BREIN uitdrukkelijk volmacht hebben verleend hun intellectuele eigendomsrechten te handhaven. Conform het oordeel van de AP in het kader van de verklaring omtrent de rechtmatigheid van online handhaving van intellectuele eigendomsrechten door Dutch FilmWorks, valt deze verwerking onder de uitzondering van artikel 33 lid 2 sub b UAVG.²⁰

Daarnaast kan BREIN zich beroepen op artikel 32 sub d UAVG. BREIN zal (uiteindelijk) betrokkenen aanschrijven en indien nodig rechtsvorderingen instellen. De daarmee gepaarde verwerkingen zijn noodzakelijk ter verdediging van de door BREIN vertegenwoordigde intellectuele eigendomsrechten. Dat geldt ook voor de verwerkingen in het kader van de te versturen waarschuwingen. FLU is immers als geheel een systeem waarmee BREIN de door haar vertegenwoordigde rechten handhaaft, met het doel inbreuken op deze rechten te terug te dringen, door zowel te waarschuwen als (uiteindelijk) mogelijk betrokkenen aan te schrijven. De waarschuwingsfase is ingevoerd op advies van de AP, en is noodzakelijk voor de mogelijke handhavingfase: slechts indien waarschuwingen alleen niet voldoende effect sorteren zullen de gebruikers die, na het versturen van de waarschuwingen, en de daar naar verwachting mee gemoeide publiciteit, doorgaan met het uitwisselen van auteursrechtelijk beschermde bestanden van door BREIN vertegenwoordigde rechthebbenden, met handhavingsacties te maken krijgen.

Omdat het (althans voor BREIN) niet duidelijk was of onder het begrip “ten behoeve van derden” zoals bedoeld in artikel 33 lid 4 UAVG ook valt het verwerken van persoonsgegevens ter behartiging van de belangen van derden (zonder dat zij toegang hebben tot de persoonsgegevens) en daar voor zover BREIN weet door de AP (nog) geen uitleg aan is gegeven, heeft BREIN zekerheidshalve een vergunning als bedoeld in artikel 33 lid 4 onder c UAVG aangevraagd bij de AP.

De AP heeft in reactie op de vergunningaanvraag geoordeeld dat FLU buiten de reikwijdte van de vergunningplicht van artikel 33 lid 4 sub c AVG valt. De AP handhaaft haar oordeel dat er sprake zou zijn van verwerking van persoonsgegevens van strafrechtelijke aard, maar concludeert dat er geen sprake is van een verwerking ‘ten behoeve van derden’, waardoor er dus geen vergunning nodig is. De AP acht daarvoor blijkbaar doorslaggevend dat BREIN geen persoonsgegevens verstrekt aan derden, zoals BREIN’s aangeslotenen. De AP vindt de omstandigheid of er persoonsgegevens aan de aangeslotenen bij BREIN worden verstrekt daarmee kennelijk doorslaggevend voor de vraag of er sprake is van een verwerking ten behoeve van derden. Dat de verwerking van persoonsgegevens dient ter behartiging van de belangen van de aangeslotenen van BREIN, brengt volgens de AP dus niet met zich mee dat er sprake is van een verwerking ‘ten behoeve van derden’. Een vergunning is volgens de AP dus niet nodig.

²⁰ Besluit van de AP 5 december 2017, z2017-02053, p. 5: “Het constateren van inbreuk op de intellectuele eigendomsrechten ten aanzien waarvan DFW kan handhaven valt naar het oordeel van de AP hier onder. Daarbij is van belang dat DFW alleen gegevens verzamelt van deelnemers aan een zwerm waarbinnen een titel van DFW wordt uitgewisseld.”

8. Proportionaliteit

Bij het nemen van maatregelen dienen de verschillende in het geding zijnde grondrechten tegen elkaar te worden afgewogen, met name het belang van BREIN om op te kunnen treden tegen de inbreuk op de intellectuele eigendomsrechten van haar aangeslotenen en de privacybelangen van partijen die inbreuk maken op die rechten, alsmede hun recht om informatie te verspreiden en te ontvangen. De bescherming van de grondrechten van de laatstgenoemde partijen gaat in elk geval niet zover, dat zij met een beroep op hun privacybelang anoniem inbreuk zouden mogen maken op de exclusieve rechten van derden²¹.

IP-nummers zijn voor BREIN zelf op geen enkele manier tot natuurlijke personen te herleiden en daarom is de enkele verwerking van IP-nummers gedurende korte tijd niet ingrijpend te noemen. BREIN streeft er voorts naar om de verwerking van IP-nummers op de minst ingrijpende manier mogelijk te doen plaatsvinden. Dat is zowel in het belang van het onderzoek zelf als dat van de betrokkenen.

Bij FLU is BREIN uitgegaan van het principe van privacy by default. De privacy van de betrokkenen staat voorop tenzij het handhavingsbelang zwaarder weegt. Enkel indien de waarschuwingsfase niet voldoende effect sorteert, komt een relatief klein deel van de IP-nummers die met FLU worden verwerkt in aanmerking voor (mogelijke) nadere (handhavings)stappen. Het streven van BREIN is erop gericht het deel van de Bittorrent-gebruikers te waarschuwen en mogelijk aan te spreken die een relevante rol vervult bij de verdere verspreiding van illegaal entertainment aanbod, zodat het overgrote deel van de IP-nummers door BREIN zonder verdere opvolging binnen vier weken zal worden vernietigd.

In het kader van de proportionaliteit zal BREIN eerst gerichte waarschuwingscampagne voeren waarbij notificaties worden gestuurd aan inbreukmakende Bittorrent-uploaders van wie het IP-nummer in vier weken tijd twee maal of meer wordt aangetroffen. In gesprekken met de Autoriteit Persoonsgegevens, bleek dat ook zij het in het kader van de proportionaliteit van belang vindt dat gebruikers van het Bittorrent eerst via notificaties worden gewaarschuwd voor de mogelijke gevolgen daarvan.

Pas indien de waarschuwingsacties niet voldoende effect hebben (bijvoorbeeld omdat het niet mogelijk blijft deze snel en effectief uit te voeren omdat ISP's niet vrijwillig willen meewerken) zal tot handhaving worden overgegaan. BREIN verwacht mede op basis van haar ervaring die zij met name met het BOB-systeem heeft opgedaan, dat de uitwisseling op Bittorrent van op Nederlands publiek gericht illegaal aanbod voldoende zal worden verstoord, indien minimaal zes maanden na het begin van de gerichte waarschuwingscampagne mogelijk ondersteund wordt door handhavingsacties waarbij maximaal 500 gebruikers per maand zullen worden aangesproken van wie het IP-nummer toch nog vaker dan twee keer in Bittorrent-zwermen wordt aangetroffen in een periode van vier weken en dat de uitwisseling via Bittorrent van dat aanbod daardoor aanzienlijk zal kunnen worden teruggedrongen.

²¹ Rb. Den Haag, 30 april 2020, <http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2020:3980> (Dish Network LLC tegen Worldstream), ov. 4.21

In het kader van BOB is gebleken dat - afgezien van buitenlandse IP's - Nederlandse IP-nummers die in vier weken tijd één keer in inbreukmakende zwermen worden aangetroffen, veruit de grootste groep inbreukmakende Bittorrent-gebruikers vormt (zie figuur 1 hieronder). De eenmalig aangetroffen abonnees beschouwt BREIN als incidentele Bittorrent-gebruikers die vooral gericht zijn op het downloaden van inbreukmakende content zonder dat zij bestanden blijven seeden. Omdat deze IP-nummers niet aan de gestelde criteria voldoen, worden ze automatisch vernietigd en worden deze IP-nummers niet verder verwerkt. Dit is voor deze categorie houders van IP-nummers de minst ingrijpende manier van gegevensverwerking denkbaar. Deze gegevensverwerking maakt nauwelijks inbreuk op het privacy-belang van de betrokkenen, omdat de gegevens na 4 weken meteen weer worden verwijderd.

De groep die twee keer wordt aangetroffen, is al veel kleiner en ziet BREIN als potentiële gewoontegebruikers of gebruikers die hun computer aan laten staan waardoor zij bestanden seeden. Door dit seeden wordt het mogelijk voor grote groepen andere gebruikers om het betreffende bestand te downloaden, waardoor het Bittorrent netwerk in stand kan blijven. Deze tweede groep beoogt BREIN in de eerste plaats te bereiken met waarschuwing en voorlichting zonder dat het nodig wordt geacht de NAW-gegevens te achterhalen.

De groep die drie keer wordt aangetroffen is aanmerkelijk kleiner dan beide eerstgenoemde groepen en die vier keer of vaker wordt aangetroffen is nog weer veel kleiner. Dit zijn de inbreukmakers waarop BREIN zich indien nodig een half jaar na het begin van de waarschuwingscampagne met de handhavingsmaatregelen richt. Met het kunnen aanspreken van maximaal 500 betrokkenen per maand verwacht BREIN deze groep inbreukmakers aanzienlijk kleiner te kunnen maken en daarmee uiteindelijk de ruggengraat te treffen van het op Nederland gerichte illegale aanbod op Bittorrent.

Het zoveel mogelijk verstoren van bestaande zwermen waarin zonder toestemming populaire entertainment content wordt uitgewisseld is de reden dat BREIN zich met de handhavingsactiviteiten van FLU specifiek wil kunnen richten op deze groep Bittorrent-uploaders. Deze groep functioneert als het ware als de smeerolie van het systeem van uitwisseling op Bittorrent doordat de uploaders de door hen gedownloade inbreukmakende content beschikbaar blijven houden of met regelmaat beschikbaar hebben voor medegebruikers, waardoor de continuïteit van het illegale aanbod op Bittorrent bevordert wordt. Door het aanspreken van deze categorie uploaders, zal deze vorm van illegaal uploaden naar verwachting aanmerkelijk worden verminderd wat weer tot gevolg heeft dat de computers van de meest fanatieke uploaders ('seeders'), die dienst doen als servers, alsmede hun internetverbindingen mogelijk eerder overbelast raken, waardoor de uitwisseling van de inbreukmakende bestanden niet langer optimaal functioneert²².

²² zie bijv. de uitleg van de werking van Bittorrent door Advocaat-Generaal bij het HvJEU M. Szpunar in de conclusie d.d. 8 februari 2017 in Zaak C-610/15 (Stichting Brein tegen Ziggo BV en XS4ALL Internet BV), ov. 24, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=187646&pageIndex=0&doclang=NL&mode=req&dir=&occ=first&part=1&cid=634431>

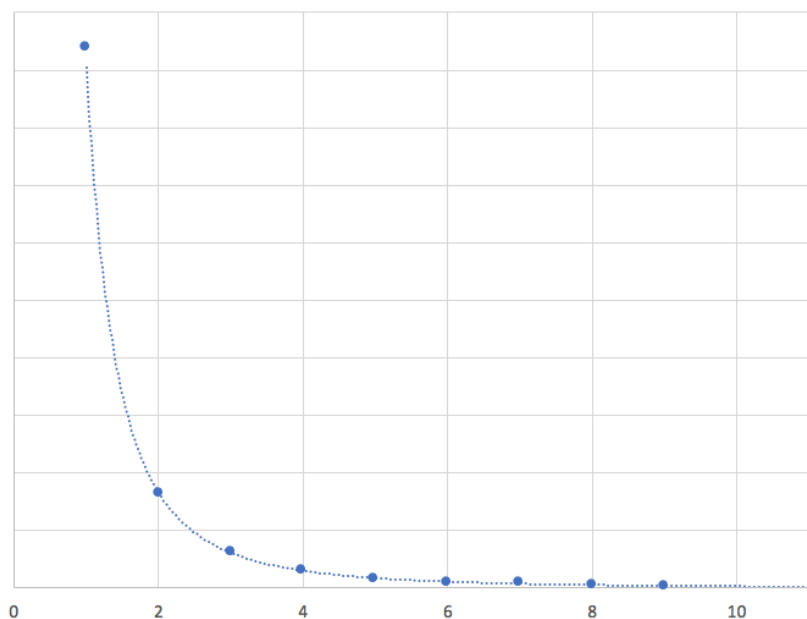


Fig 1. Met BOB is gebleken dat een minderheid van de IP-nummers meer dan één of twee keer wordt aangetroffen

BREIN zal FLU, mede met het oog hierop regelmatig evalueren. Afhankelijk van de uitkomst van de evaluatie zal worden besloten of het maximumaantal van 500 per maand voldoende is, of dat dit aantal verhoogd dient te worden. Indien dit noodzakelijk blijkt, zal er een aangepaste DPIA worden uitgevoerd.

9. Subsidiariteit

BREIN's collectieve handhaving is civielrechtelijk. De aanpak is een mozaïek van maatregelen die door de wet en een raamwerk van rechtspraak gestaafd worden. Waar nodig bouwt BREIN middels rechtszaken voort aan het raamwerk van rechtspraak waaruit de (zorg-) plichten van alle spelers op het internet blijkt en dat het kader geeft waarbinnen haar handhaving plaatsvindt.

Het doel van de handhaving door BREIN op het Bittorrent-netwerk is de verstoring van het illegale aanbod en het gebruik daarvan. BREIN hanteert daarbij een breed scala van aanknopingspunten: sites/diensten; uploaders; hosting providers; access providers; betaaldiensten; adverteerders en agencies/networks; zoekmachines; eindgebruikers. De handhavingsstrategie van BREIN ten aanzien van Bittorrent-websites is er in de eerste plaats op gericht af te dwingen dat illegale activiteiten door sites zelf gestaakt en voorkomen worden. Als dat niet mogelijk is, verlangt BREIN van de hosting providers dat de sites offline gehaald worden en dat de sitehouders geïdentificeerd worden. Als ook die aanpak geen soelaas blijkt te bieden, richt BREIN zich tot de access providers om de toegang tot de sites te blokkeren.

In de praktijk blijkt dat vooral dit laatste een zeer langdurig proces kan zijn. In 2009 heeft BREIN bijvoorbeeld de eerste stappen ondernomen om 's werelds bekendste Bittorrent-

website ThePirateBay afgesloten te krijgen. Na talloze juridische procedures heeft de Hoge Raad uiteindelijk vragen van uitleg gesteld aan het HvJEU. Na de bevestigende beantwoording door het HvJEU van de vraag of ThePirateBay inbreuk maakt, heeft de Hoge Raad de zaak weer terugverwezen naar het Gerechtshof Amsterdam. Dat heeft uiteindelijk op 2 juni 2020 arrest gewezen en bepaald dat de providers Ziggo en XS4all voortaan de IP-adressen en domeinnamen van ThePirateBay, die op een lijst staan die BREIN aanlevert, voor hun gebruikers moeten blokkeren²³.

De providers hebben geen cassatie aangetekend tegen dit laatste arrest. Na meer dan 10 jaar procederen is deze zaak daarmee tot een definitief einde is gekomen. De voorzieningenrechters in Den Haag en Midden Nederland hebben de service providers in Nederland die tezamen in totaal meer dan 95% marktaandeel hebben - naast Ziggo en XS4all ook KPN, T-Mobile etc.- eveneens geboden de website te blokkeren voor hun abonnees. Hoewel dit een belangrijke stap is in het uitbannen van het illegale gebruik van Bittorrent, blijven er uiteraard andere websites over die (nog) niet geblokkeerd worden.

Verder richt BREIN haar pijlen ook op grote illegale uploaders. Bij de aanpak wordt in ernstigere gevallen gebruik gemaakt van ex parte rechterlijke bevelen. Uploaders krijgen de mogelijkheid tot een civielrechtelijke schikking, die kan bestaan uit een tegemoetkoming in gemaakte kosten en geleden schade voor het verleden en een onthoudingsverklaring met boetebeding voor de toekomst. De schikkingen die daarbij getroffen worden, hebben zowel een repressieve als preventieve werking.

BREIN vraagt, of vereist zo nodig, ook assistentie van andere op zich min of meer neutrale tussenpersonen en spelers zoals zoekmachines (bijv. Google), Content Delivery Networks (bijv. Cloudflare), betaaldiensten en adverteerders/adnetworks. Ook bij juridisch neutraal geachte tussenpersonen is de inzet van BREIN dat naast effectieve NTD aanvullende maatregelen zoals specifieke filterverplichtingen kunnen worden verlangd.

Het hiervoor omschreven brede scala aan handhavingsactiviteiten heeft er tot op heden niet toe geleid dat BitTorrent niet langer massaal voor het maken van inbreuk wordt gebruikt. Daarom is het essentieel dat BREIN uploaders kan waarschuwen (en indien dit nodig blijkt aanspreken) die meer dan eens in BitTorrentzwermen worden aangetroffen zoals met FLU en dit Protocol is voorzien. Daarbij heeft BREIN ervoor gekozen om in eerste instantie enkel over te gaan tot het (laten) versturen van waarschuwingen. Pas als dat niet voldoende effectief blijkt zal tot het opvragen van NAW gegevens worden overgegaan. Er staat BREIN geen andere, minstens zo doeltreffende mogelijkheid tot haar beschikking om de mogelijke inbreukmakers te identificeren, dan om de NAW-gegevens bij hun ISP's op te vragen.²⁴

²³ Hof Amsterdam, 2 juni 2020, ECLI:NL:GHAMS:2020:1421 (BREIN/Ziggo en XS4all)

²⁴ Zie ook Hof Arnhem-Leeuwarden, 5 november 2019, ECLI:NL:GHARL:2019:9352 (DutchFilmWorks/Ziggo), ov. 5.12

Geen overlap met BOB of andere handhavingsacties

FLU draait fysiek gescheiden van BOB. Beide systemen zullen niet tegelijkertijd draaien. Er zal dus geen sprake van overlap tussen beide systemen zijn.

De waarschuwing en handhaving van FLU zien op een andere categorie inbreukmakers dan BOB. BOB is expliciet gericht op het verzamelen van bewijs tegen de harde kern van doelbewuste inbreukmakers die functioneren als de bevoorraders van het Bittorrent-systeem. De uploaders in deze categorie zijn in veel gevallen te herkennen aan de door hen gebruikte aliassen (nicknames), die vaak gezien worden als een soort keurmerk. Kenmerkend voor de uploaders in de BOB-categorie is dat ze in de door hen geïnitieerde zwermen aanwezig blijven, totdat er voldoende nieuwe seeders zijn om de zwermen verder in stand te houden. Bij populaire bestanden zal dit na vrij korte tijd het geval zijn, wat tot gevolg heeft dat de BOB-categorie vaak vrij snel weer uit die zwermen verdwijnt.

De handhaving van FLU is gericht op de categorie uploaders die het 'stokje overneemt' van de uploaders uit de BOB-categorie en het illegale Bittorrent-aanbod in stand houdt door dit te blijven delen na het te hebben gedownload, en zij die drie maal per maand of vaker inbreuk maken middels Bittorrent.

Ter voorkoming van een mogelijke overlap tussen FLU en de individuele handhavingsactiviteiten van de aangeslotenen van BREIN zal er onderlinge afstemming zijn tussen BREIN en de aangeslotenen. Zo zullen er afspraken worden gemaakt over de handhaving tegen inbreuk tijdens bepaalde periodes op bepaalde titels van rechthebbenden, indien die rechthebbenden daar zelfstandig op handhaven. BREIN zal gedurende de periode dat rechthebbenden met betrekking tot bepaalde werken zelf naar inbreukmakende gebruikers zoeken met het oog op handhaving, de titels van hun werken uitzonderen van FLU. Cumulatie van sancties voor dezelfde inbreuk is dan ook uitgesloten.

BREIN zal in het kader van FLU uitsluitend uitgaan van het door haar zelf verzamelde bewijs. Er zal dus geen uitwisseling van persoonsgegevens (noch IP-adressen, noch NAW-gegevens) plaatsvinden tussen BREIN en aangeslotenen die eigen handhavingsactiviteiten ontplooiën en vice versa. Voor de AP is deze omstandigheid doorslaggevend voor haar vaststelling dat BREIN met FLU geen (strafrechtelijke) persoonsgegevens ten behoeve van derden verwerkt en dat BREIN daarom geen vergunning voor FLU nodig heeft.

10. Rechten van de betrokkene

10.1 Informeren van de betrokkene

Betrokkenen zullen schriftelijk op de hoogte gesteld worden van de verwerking van hun persoonsgegevens en de doeleinden waarvoor deze zijn verwerkt zodra dit redelijkerwijs mogelijk is.

De maximaal 1000 notificaties per maand die aan uploaders zullen worden gestuurd, die voldoen aan de criteria van 5.2, zullen een passage bevatten waarin de betrokkene wordt geïnformeerd dat zijn IP-nummer door BREIN is verwerkt.

Indien wordt overgegaan tot de handhavingfase zullen de ISP's van de houders van de IP-nummers, die voldoen aan de onder 5.3 genoemde criteria, per maand maximaal 500 NAW-verzoeken van BREIN ontvangen. Na verstrekking door de ISP van contactgegevens van een houder van een IP-nummer, zal deze eveneens door BREIN geïnformeerd worden over de verwerking van zijn persoonsgegevens en zullen aan hem de in artikel 14 AVG bedoelde gegevens worden verstrekt conform de privacyverklaring van BREIN. Daarbij zullen de betrokkenen nadrukkelijk gewezen worden op de waarborgen van de rechten van de betrokkenen die BREIN heeft getroffen (met name de door BREIN gehanteerde klachtenprocedure en de waarborgen ten aanzien van minderjarige inbreukmakers, zie hierna). Bij het verzoek tot verstrekken van de NAW-gegevens aan de ISP's zal BREIN tegelijk ook de ISP's verzoeken door te geven aan de relevante klanten dat BREIN de betreffende IP-nummers verwerkt heeft opdat de betreffende abonnees zo vroeg mogelijk na verwerken van de gegevens daarvan op de hoogte kunnen geraken.

Indien BREIN besluit over te gaan tot handhaving, zal BREIN in de te zenden brieven aan de houder van het IP-adres tevens informeren wat - in het geval hij niet zelf de illegale downloader is - rechtezins zijn positie is en daarbij impliciet dan wel expliciet verwijzen naar de overwegingen uit het arrest Bastei Lübbe van het HvJEU²⁵. Uit dit arrest volgt dat de houder van een internetaansluiting, die ook aan anderen ter beschikking is gesteld (o.a. gezinsleden), niet automatisch aansprakelijk is voor een via die aansluiting gemaakte inbreuk. Op deze persoon rust wel een zogenaamde secundaire stelplicht, inhoudende dat hij dient aan te geven dat anderen mogelijk inbreuk hebben gemaakt via zijn internetaansluiting en dat hij ook de identiteit van de betreffende personen vermeldt, ook indien het gaat om gezinsleden.

BREIN zal via algemene aankondigingen op websites en in de media informatie verstrekken over de voorgenomen werkwijze, zodat Bittorrent-gebruikers in het algemeen op de hoogte zijn van de voorgenomen gegevensverwerkingen. In deze publicaties zal naar voren komen welke persoonsgegevens BREIN zal verwerken (IP-nummers) en met welk doel (handhaving en waarschuwing om afname van het illegale gebruik van Bittorrent te bewerkstelligen). BREIN voldoet daarmee aan de verplichting van artikel 14 AVG ten aanzien van betrokkenen van wie de IP-nummers worden vastgelegd in het kader van FLU, ook ten aanzien van die Bittorrent-gebruikers van wie de IP-nummers worden vastgelegd, maar van wie BREIN geen contactgegevens ontvangt.

BREIN zal op haar website <https://stichtingbrein.nl/> een Q&A-pagina aanmaken waarop antwoorden te vinden zullen zijn op de vragen die naar verwachting het meest gesteld zullen worden, en waar een verwijzing naar de privacyverklaring van BREIN wordt opgenomen. Deze pagina is aan dit protocol gehecht als Bijlage 2. Mogelijk zal deze pagina in de toekomst uitgebreid of aangepast worden indien de ontwikkelingen daar aanleiding toe geven.

²⁵ Bastei Lübbe, HvJEU van 18 oktober 2018, C-149/17, <http://curia.europa.eu/juris/documents.jsf?num=C-149/17>

10.2 Rechten van betrokkenen

De betrokkene kan bij BREIN zijn recht op inzage, correctie, verwijdering, beperking, bezwaar en/of gegevensoverdraagbaarheid uitoefenen. Indien een betrokkene een dergelijk verzoek doet, zal dit door BREIN in behandeling worden genomen en conform de AVG worden afgehandeld. Indien blijkt dat gegevens inderdaad feitelijk onjuist zijn zullen de gegevens verbeterd, aangevuld of verwijderd worden.

10.3 Minderjarige betrokkenen

BREIN verwacht dat de IP-nummers die zij verwerkt geen gegevens over minderjarigen zullen bevatten. Houders van IP-nummers zullen immers meerderjarig zijn, nu zij een overeenkomst hebben gesloten met een ISP.

Indien na contact te hebben opgenomen met de houder van het IP-nummer komt vast te staan dat het IP-nummer voor de inbreukmakende handelingen werd gebruikt door een minderjarige, zal BREIN rekening houden met de leeftijd van de minderjarige ten tijde van de eerste verwerking van zijn gegevens. Indien de betrokkene op het moment van de eerste verwerking de leeftijd van 16 jaar nog niet had bereikt, wordt afgezien van verdere handhaving en zullen de betreffende persoonsgegevens onmiddellijk worden vernietigd. Indien de minderjarige tussen de 16 en 18 jaar was ten tijde van de eerste verwerking, en op grond van de wet zelf aansprakelijk is voor het onrechtmatig handelen, zal BREIN naar de omstandigheden van het geval beoordelen of verdere handhaving conform artikel 5.3 gerechtvaardigd is. Eventueel te nemen vervolgstappen zullen door BREIN in samenspraak met de ouder(s) of voogd(en) van de betrokkene worden genomen.

10.4 Klachtenprocedure

De betrokkene kan zich tot de Klachtenfunctionaris van BREIN wenden indien hij een klacht heeft over de wijze waarop BREIN met zijn persoonsgegevens omgaat. De klachtenregeling staat vermeld op de website van BREIN op <https://stichtingbrein.nl/klachten-en-geschillenregeling-persoonsgegevens/>. In de privacyverklaring van BREIN (<https://stichtingbrein.nl/privacyverklaring.php>) en de klachtenregeling worden betrokkenen tevens gewezen op hun recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

10.5 Waarborgen

AFLU maakt gebruik van de voor FLU relevante functies van de Bittorrent-library, waarbij voorop staat dat de gegevensverwerking ter zake dienend is en niet bovenmatig wordt. De vastlegging en filtering naar categorie van de IP-nummers in een zwerm vindt volledig geautomatiseerd plaats. Het tijdstip van de vastlegging wordt daarbij eveneens automatisch geregistreerd. De instelling van de systeemklok wordt daarbij nauwkeurig gecontroleerd door middel van het Network Time Protocol (zie ntp.org).

10.6 Geheimhouding

Alle medewerkers van Stichting BREIN hebben bij indiensttreding een geheimhoudingsbeding ondertekend, waarin zij verklaard hebben dat zij alle vertrouwelijke informatie geheim zullen houden op straffe van een boete. De informatie uit het FLU systeem wordt beschouwd als vertrouwelijke informatie.

In haar NAW-verzoeken aan de betreffende ISP's zal BREIN expliciet vermelden dat de IP-nummers niet aan derden mogen worden verstrekt, tenzij de betrokkene daarvoor toestemming heeft gegeven.

11. Beveiliging

BREIN heeft haar informatiebeveiligingsbeleid schriftelijk vastgelegd en geïmplementeerd. BREIN heeft binnen haar organisatie een Security Manager en een Security Officer aangesteld, die de taak hebben erop toe te zien dat de regels over bescherming van persoonsgegevens worden nageleefd in de praktijk. De uiteindelijke verantwoordelijkheid voor het informatiebeveiligingsbeleid ligt bij de directie van BREIN.

De verzamelde gegevens zullen worden opgeslagen op een beveiligde speciaal voor AFLU ingerichte interne server. Om AFLU te kunnen gebruiken is autorisatie door de Security Officer van BREIN vereist.

12. Toezicht op naleving FLU-protocol

BREIN heeft binnen haar organisatie een Security Manager en een Security Officer aangesteld, die de taak hebben erop toe te zien dat het informatiebeveiligingsbeleid wordt nageleefd. Daarnaast heeft BREIN een Functionaris Gegevensbescherming die toeziet op naleving van de wetgeving op het gebied van persoonsgegevens en de interne regels van BREIN. Het belang van naleving van de interne regels van BREIN over bescherming van persoonsgegevens is een dagelijks punt van aandacht voor alle medewerkers binnen BREIN.

Medewerkers van BREIN worden continu gecontroleerd op naleving van het protocol. In de regel gebeurt dit mondeling. In het wekelijkse werkoverleg van BREIN wordt dit eveneens aan de orde gesteld. Voor alle medewerkers van BREIN geldt de 'Gedragsregeling inzake de verwerking van persoonsgegevens'. Alle medewerkers van BREIN hebben deze gedragsregeling middels de ondertekening van een verklaring onderschreven.

13.1 Wijziging van het FLU-protocol

BREIN kan besluiten tot aanpassing of wijziging van het protocol als dat noodzakelijk blijkt uit het oogpunt van doeltreffendheid dan wel om de privacy van de betrokkenen te garanderen.

13.2 Audit

BREIN zal periodiek, doch ten minste eens per vijf jaar, een auditrapport opstellen waaruit blijkt dat gecontroleerd is dat BREIN werkt volgens het onderhavige FLU-protocol en in overeenstemming met de geldende wetgeving op het gebied van gegevensbescherming. Dit auditrapport zal worden opgesteld door de Functionaris Gegevensbescherming van BREIN in samenspraak met de Security Officer van BREIN.

BIJLAGE 1 Juridisch kader

1 Europees recht

In de overwegingen 9 en 10 van de Europese Auteursrechtlijn is vastgelegd dat de belangrijkste doelstelling van deze richtlijn is om een hoog beschermingsniveau voor auteurs en uitvoerende kunstenaars te verwezenlijken, omdat die rechten van wezenlijk belang zijn voor scheppend werk. Hierbij wordt overwogen dat de bescherming van het auteursrecht en de naburige rechten bijdraagt tot de instandhouding en ontwikkeling van de creativiteit in het belang van auteurs, uitvoerend kunstenaars, producenten, consumenten, cultuur, industrie en het publiek in het algemeen. Auteurs en uitvoerend kunstenaars moeten, willen zij hun scheppende en artistieke arbeid kunnen voortzetten, een passende beloning voor het gebruik van hun werk ontvangen, evenals de producenten om dat werk te kunnen financieren. De productie van fonogrammen, films en multimediatproducten, en van diensten, zoals "diensten-op-aanvraag", vereist aanzienlijke investeringen. Een adequate rechtsbescherming van de intellectuele eigendomsrechten is noodzakelijk om de mogelijkheid tot het verkrijgen van een dergelijke beloning en de mogelijkheid van een behoorlijk rendement van dergelijke investeringen te waarborgen²⁶.

Uit overweging 20 van de richtlijn betreffende de handhaving van intellectuele-eigendomsrechten (richtlijn 2004/48) blijkt met name dat het bewijs een uiterst belangrijk element voor de vaststelling van inbreuken op intellectuele-eigendomsrechten is en dat ervoor moet worden gezorgd dat er effectieve middelen voor het overleggen, verkrijgen en beschermen van bewijsmateriaal beschikbaar zijn. In haar arrest van 18 oktober 2018 in de zaak *Bastei Lübbe v Strotzer* heeft het HvJEU hier nogmaals op gewezen²⁷.

In artikel 8 lid 1 Auteursrechtlijn is dan ook bepaald dat de lidstaten voorzien in passende sancties en rechtsmiddelen met betrekking tot inbreuken op de in deze richtlijn omschreven rechten en verplichtingen en er zorg voor dragen, dat deze sancties en rechtsmiddelen daadwerkelijk worden toegepast. De aldus vastgestelde sancties moeten doeltreffend en evenredig zijn en bijzonder preventieve werking hebben.

Artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: 'het Handvest') bepaalt onder meer dat beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen, en dat uit de rechtspraak van het Hof blijkt dat een maatregel die leidt tot een ernstige aantasting van een in het Handvest beschermd recht, niet voldoet aan het vereiste dat een juist evenwicht wordt verzekerd tussen de met elkaar in overeenstemming te brengen grondrechten²⁸.

De rechten en plichten van ISP's zijn onder andere vastgelegd in de E-commerce richtlijn, waarbij in dit verband met name de artikelen 12-15 relevant zijn.

²⁶ <http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32001L0029&from=en>

²⁷ Zaak C-149/17: *Bastei Lübbe v Strotzer*, <http://curia.europa.eu/juris/documents.jsf?num=C-149/17>

²⁸ Zaak C-580/13 - *Coty Germany*, <http://curia.europa.eu/juris/liste.jsf?num=C-580/13>, ov. 35

Op 25 mei 2018 is in de EU de Algemene Verordening Gegevensbescherming (AVG) in werking getreden, die, samen met de Uitvoeringswet AVG, voor de Wbp in de plaats is gekomen. Belangrijke uitgangspunten in de AVG zijn onder andere privacy by design en privacy by default, die er in het kort op neerkomen dat persoonsgegevens goed moeten worden beschermd, dat er niet meer gegevens mogen worden verzameld dan noodzakelijk voor het doel van de verwerking en dat gegevens niet langer worden bewaard dan nodig.

2 Nederlands recht

De bepalingen van de E-commerce richtlijn die betrekking hebben op de rechten en plichten van ISP's met betrekking tot de gedragingen van hun abonnees zijn voor een belangrijk deel geregeld in art. 6:196c BW. In dit artikel zijn onder andere de (niet-) aansprakelijkheidsregels opgenomen die voor ISP's gelden. Ook is hierin (in art. 6:196c lid 5 BW) bepaald dat ISP's - los van hun eventuele aansprakelijkheid - een bevel opgelegd kan worden om actie te ondernemen. Aan ISP's kan echter geen algemene toezichtsverplichting worden opgelegd met betrekking tot de informatie die zij doorgeven of opslaan²⁹. In de regel zullen het dus derden zijn die ISP's op het onrechtmatig handelen van hun klanten wijzen en hen verzoeken actie te ondernemen. In de gevallen dat persoonsgegevens van de betreffende klanten aan de ISP's worden verstrekt is het onvermijdelijk, dat ten minste een IP-nummer en het tijdstip van de constatering wordt doorgegeven aan de ISP, zodat deze de juiste klant aan kan spreken. Wat betreft de omstandigheden waaronder ISP's verplicht zijn NAW-gegevens af te geven, is nog altijd het arrest van de Hoge Raad in Lycos-Pessers³⁰ relevant. Ook kan een vordering tot afgifte NAW in auteursrechtzaken gebaseerd worden op artikel 28 lid 9 auteurswet.

3 Handhaving van het auteursrecht

In Nederland is de handhaving van de rechten van auteurs en uitvoerende kunstenaars geregeld in de Auteurswet en de Wet op de naburige rechten. Hierin is onder andere bepaald dat (voorwaardelijk) opzettelijke inbreuk op deze rechten als misdrijf wordt gekwalificeerd (zie o.a. art. 33 Aw. en art. 26 Wnr). In de door het College van Procureurs-Generaal (de landelijke leiding van het openbaar ministerie) vastgestelde Aanwijzing intellectuele-eigendomsfraude³¹ is echter bepaald dat civielrechtelijke handhaving door de rechthebbenden het uitgangspunt vormt bij de bestrijding van inbreuken op door intellectuele eigendomsrechten. De aanwijzing is op 31 maart 2017 overigens ingetrokken, hetgeen echter niet betekent dat het beleid op dit punt is gewijzigd. Van het uitgangspunt dat civielrechtelijke handhaving het uitgangspunt vormt, kan slechts worden afgeweken als het algemeen belang dat vereist, aldus het Hof Den Haag. Omdat er in casu geen sprake was van winstoogmerk, beroepsmatig handelen, betrokkenheid van een criminele organisatie of relevante recidive, was volgens het hof het algemeen belang niet aan de orde.³² In de praktijk wordt de handhaving tegen uploadende Bittorrent-gebruikers uitsluitend aan de civielrechtelijke partijen overgelaten.

²⁹ art. 15 lid 1 EU-Richtlijn 2000/31

³⁰ HR 15 november 2005, ECLI:NL:HR:2005:AU4019 (Lycos / Pessers)

³¹ nummer 2005A022; zie <http://wetten.overheid.nl/BWBR0021180/2006-02-01>

³² <http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2014:84>

Om toch tegemoet te komen aan de hoofddoelstelling van auteursrechtlijn - een hoog beschermingsniveau voor auteurs en uitvoerende kunstenaars – is het van het grootste belang dat aan civiele partijen als Stichting BREIN de juridische middelen worden geboden om de handhaving tegen de inbreuk van intellectuele eigendomsrechten op de meest doelmatige manier vorm te geven. Het zou indruisen tegen de gedachte van een rechtvaardig evenwicht tussen de in het geding zijnde concurrerende grondrechten als aan het grondrecht op intellectuele eigendom deze bescherming wordt ontnomen³³.

4 Jurisprudentie

Het Europese Hof van Justitie (HvJEU) heeft in een aantal arresten bepaald dat dienstverleners op internet, waaronder ISP's, gehouden zijn medewerking te verlenen bij het tegengaan van inbreuken die worden gepleegd via de internetverbindingen die door hen worden geleverd. In het arrest l'Oreal/eBay heeft het HvJEU bijvoorbeeld bepaald dat aan hen kan worden gelast om maatregelen te treffen die niet slechts bijdragen tot het doen eindigen van de door de gebruikers van die marktplaats gepleegde inbreuken op die rechten, maar ook tot het voorkomen van nieuwe inbreuken van die aard³⁴. Het verstrekken van NAW-gegevens is een maatregel die erop is gericht de geconstateerde inbreuken te doen eindigen en nieuwe inbreuken van dezelfde aard te voorkomen.

In het arrest UPC Telekabel Wien bepaalde het HvJEU onder meer dat van ISP's verlangd kan worden dat "zij internetgebruikers die gebruikmaken van de diensten van de adreassaar van dat bevel ernstig ontraden om zich toegang te verschaffen tot deze in strijd met het intellectuele-eigendomsrecht voor hen beschikbaar gestelde werken"³⁵. Het verstrekken door een ISP aan BREIN van NAW-gegevens van een abonnee die middels Bittorrent inbreuk maakt, komt aan dit minimumvereiste tegemoet. In Coty Germany/Stadtparkasse Magdeburg³⁶ bepaalde hetzelfde Hof dat zelfs een bankinstelling die een betaling heeft verwerkt voor inbreukmakende goederen in beginsel verplicht is om op gerechtelijk bevel informatie te verschaffen over de rekeninghouder.

In het arrest van 18 oktober 2018 in de zaak Bastei Lübbe v Strotzer heeft het HvJEU bepaald dat beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden de wezenlijke inhoud van die rechten en vrijheden moeten eerbiedigen. Nationale regelgeving die de nationale rechterlijke instantie waarbij een vordering wegens aansprakelijkheid is ingesteld, kan beletten om op verzoek de overlegging en verkrijging van bewijsmateriaal (i.c. inzake de gezinsleden van de wederpartij) te gelasten, waardoor de vaststelling van de vermeende inbreuk op het auteursrecht en de identificatie van de inbreukmaker onmogelijk worden gemaakt en bijgevolg de grondrechten op een doeltreffende voorziening in rechte en op intellectuele eigendom waarop de auteursrechthebbende aanspraak kan maken,

³³ zie arrest HvJEU van 15 september 2016, Mc Fadden, C-484/14, EU:C:2016:689, punt 98

<http://curia.europa.eu/juris/liste.jsf?language=nl&td=ALL&num=C-484/14>

³⁴ HvJEU, 12 juli 2011, zaak C-324/09, (l'Oreal/eBay) ov. 144

<http://curia.europa.eu/juris/document/document.jsf?docid=107261&doclang=NL>

³⁵ HvJEU 27 maart 2014, zaak C-314/12 (UPC Telekabel Wien), ov. 64

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=149924&pageIndex=0&doclang=NL>

³⁶ zie voetnoot 20

ernstig worden aangetast, voldoet niet aan het vereiste dat een juist evenwicht wordt verzekerd tussen de verschillende grondrechten.³⁷

In Nederland heeft de Haagse voorzieningenrechter in een vonnis van 30 april 2020 in de zaak van de Amerikaanse aanbieder van betaaltelevisie Dish Network tegen de Nederlandse ISP Worldstream bepaald, dat de grondrechten van klanten van WorldStream niet zover gaan dat zij met een beroep op die rechten anoniem inbreuk zouden mogen maken op de exclusieve rechten van Dish Network. De voorzieningenrechter ging daarbij voorbij aan het betoog van WorldStream dat de belangen van haar klanten zwaarder zouden moeten wegen omdat Dish Network niet heeft onderbouwd hoe zij de rechten van de klanten van Dish Network zal waarborgen en/of wat de schade behelst, wat de hoogte van die schade is en wat dit per individuele klant gaat betekenen en/of welke actie(s) Dish Network daarbij zal inzetten³⁸.

³⁷ zie voetnoot 19

³⁸ Zie voetnoot 21

BIJLAGE 2 **Veelgestelde vragen**

Veelgestelde vragen bij het voorlichtingsproject voor frequente en langdurige uploaders

V: Wat is een IP-adres?

A: IP staat voor internet protocol. Elke computer die is aangesloten op het internet heeft een nummer dat zichtbaar is voor alle andere computers op het internet zodat ze elkaar kunnen vinden en kunnen communiceren. Deze nummers zijn de IP-adressen. Bij mensen thuis identificeert het IP-nummer hun internet service provider (ISP). Het werkelijke adres van de abonnee is alleen via de ISP te achterhalen.

V: Mag BREIN IP-adressen van Bittorrent-gebruikers verzamelen?

A: De verwerking van IP-nummers door BREIN in het kader van het FLU systeem is noodzakelijk ter behartiging van het gerechtvaardigde belang van BREIN en haar aangeslotenen om grootschalige auteursrechtinbreuk via Bittorrent te beperken en te voorkomen.

Om het illegale gebruik van Bittorrent terug te dringen en zo legale distributiemodellen van entertainment producten ('content') een eerlijke kans te geven is het belangrijk dat uploaders gewezen worden op hun gedrag zodat zij zich bewust worden van de schadelijke gevolgen die makers en rechthebbenden ondervinden als gevolg van het illegaal uitwisselen van bestanden. Daarbij is ook van belang dat zij zich bewust worden van de mogelijkheid dat zij worden aangesproken voor compensatie van de schade die het illegale bittorrent gebruik veroorzaakt als zij op dezelfde voet verdergaan met het maken van inbreuk.

BREIN heeft met een privacy en data protection expert een Data Protection Impact Assessment uitgevoerd. Hierin is geconcludeerd dat de waarborgen en beveiligingsmaatregelen die BREIN heeft getroffen ertoe leiden dat de verwerking geen hoog risico voor de privacy van betrokkenen met zich meebrengt.

V: Welk doel wil BREIN met FLU bereiken?

A: BREIN beoogt met FLU de massale inbreuken terug te dringen die met Bittorrent worden gemaakt.

V: Kan dat doel niet op een andere manier worden bereikt?

A: Het bestrijden van het illegale gebruik van Bittorrent vergt een veelzijdige aanpak. FLU is daarbij één van de methoden die BREIN hanteert om dat doel te bereiken. BREIN's aanpak richt zich bijvoorbeeld ook op eigenaars van illegale Bittorrent websites en op de dienstverlenende tussenpersonen zoals hosting providers, betaaldiensten en access providers teneinde de inbreuken te (doen) staken. Desondanks blijven er sites en gebruikers die doorgaan met inbreuk maken. Daarom wil BREIN gedurende minimaal zes maanden individuele uploaders voorlichten en waarschuwen en in een latere fase eventueel aanspreken op hun gedrag. Dit past in het mozaïek van maatregelen dat BREIN neemt.

V: Schendt BREIN de privacy niet door IP-nummers te verzamelen?

A: Het uitgangspunt bij FLU is proportionaliteit, dat wil zeggen dat als standaard geldt dat alléén persoonsgegevens worden verwerkt die noodzakelijk zijn voor het specifieke doel dat BREIN met FLU wil bereiken. Minimaal het eerste half jaar is dat doel uitsluitend voorlichting en waarschuwing zonder daarbij te hoeven weten wie de mensen achter de IP-nummers precies zijn, al is BREIN voor het doorsturen van de notificaties wel afhankelijk van de medewerking van de service providers die de IP-nummers in beheer hebben.

V: Gaat BREIN de IP-nummers van zoveel mogelijk Bittorrent gebruikers vastleggen?

A: BREIN verzamelt niet meer IP-nummers dan nodig is om het massale inbreukmakende gebruik te beteugelen. BREIN neemt steekproeven die erop gericht zijn IP-nummers van Nederlandse gebruikers vast te leggen die betrokken zijn bij het uploaden van inbreukmakende bestanden met muziek, films, games of ebooks.

V: Loopt iedereen die Bittorrent gebruikt evenveel kans dat zijn IP-nummer door BREIN wordt vastgelegd?

A: Hoe vaker en langer je als uploader in een inbreukmakende Bittorrent-zwerm aanwezig bent, hoe meer kans je loopt door BREIN aangesproken te worden.

V: Mag ik wel af en toe een illegaal bestand met Bittorrent downloaden?

A: Illegaal downloaden, d.w.z. zonder toestemming verveelvoudigen van een auteursrechtelijk beschermd werk, maakt inbreuk op auteursrechten en mag dus niet. Bovendien is een belangrijk kenmerk van Bittorrent dat iedere gebruiker die bezig is met het downloaden van een bestand, elk gedownload deeltje van het bestand automatisch direct weer beschikbaar stelt voor andere gebruikers. BREIN zal Bittorrent gebruikers in eerste instantie met waarschuwing en voorlichting trachten te overtuigen geen inbreuk meer te maken.

V: Hoe lang bewaart BREIN de verzamelde IP-nummers?

A: De buitenlandse IP-nummers die BREIN aantreft, worden meteen geanonimiseerd. Nederlandse IP-nummers worden gedurende maximaal zes weken bewaard. Alleen als IP-nummers in vier weken tijd twee keer of vaker in steekproeven worden aangetroffen komen ze in aanmerking om langer bewaard te worden zodat BREIN aan de houders van de verbinding notificaties kan sturen. Indien ISP's weigeren vrijwillig waarschuwingen door te sturen, zal het noodzakelijk zijn dit in rechte af te dwingen en dus om IP-adressen langer te bewaren in de desbetreffende procesdossiers, totdat onherroepelijk vonnis is gewezen.

V: Gaat BREIN 'lok'bestanden uploaden om Bittorrent-gebruikers te betrappen?

A: Neen. BREIN neemt in het kader van FLU nooit zelf het initiatief om inbreukmakende bestanden te uploaden. Het gaat om reeds bestaande illegale bittorrent zwermen. Uitsluitend IP-nummers in die zwermen die al over de ongeautoriseerde kopie van het beschermde werk beschikken komen in aanmerking om te worden vastgelegd.

V: Hoe weet BREIN van wie een IP-nummer is?

A: BREIN weet niet van wie een IP-nummer is maar kan wel eenvoudig achterhalen bij welke Internet Service Provider een IP-nummer hoort. Het is niet de bedoeling van BREIN om aan

de hand van de IP-nummers bijbehorende identiteitsgegevens van inbreukmakers op te vragen bij de provider. Daar zal BREIN pas toe overgaan als providers niet mee willen werken aan het doorsturen van de notificaties aan de abonnees van wie de IP-nummers door BREIN in het kader van FLU zijn aangetroffen.

V: Ik heb een klacht over de verwerking van mijn persoonsgegevens door BREIN, waar kan ik die indienen?

Klachten kunnen worden ingediend bij de klachtenfunctionaris van BREIN en zullen worden behandeld volgens de interne klachtenregeling van BREIN. Die is hier gepubliceerd: <https://stichtingbrein.nl/klachten-en-geschillenregeling-persoonsgegevens/>

Betrokkenen hebben ook het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens. Meer informatie over klachten over de verwerking van persoonsgegevens is te vinden op de website van de Autoriteit Persoonsgegevens: <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten/privacyklacht-indienen>

FLU-protocol van Stichting BREIN, 27 november 2020