de Correspondent

MAURITS MARTIJN +
DIMITRI TOKMETZIS

JE HEBT WÉL IETS TE VERBERGEN

OVER HET LEVENSBELANG VAN PRIVACY

de Correspondent

MAURITS MARTIJN +
DIMITRI TOKMETZIS

JE HEBT WÉL IETS TE VERBERGEN

OVER HET LEVENSBELANG
VAN PRIVACY

Facebook weet bij wie je gisteren op bezoek ging.
De Belastingdienst zag hoe je er kwam.
Apple hield bij hoelang je er bleef.
Amazon hoorde wat je er zei.
En Google wist al dat je het van plan was.

In deze nieuwe editie van hun bestseller *Je hebt wél iets te verbergen* laten onderzoeksjournalisten Maurits Martijn en Dimitri Tokmetzis zien dat privacy het meest bedreigde mensenrecht van onze tijd is.

Ze leren smartphones kraken en computers hacken, voelen hoge ambtenaren en datahandelaren aan de tand en interviewen de scherpste denkers over privacy en surveillance. Zo leggen ze bloot welke gegevens je allemaal weggeeft en aan wie. En, belangrijker nog: welke ingrijpende gevolgen dat heeft voor ons allemaal.

Dit boek is het resultaat van jarenlange diepgravende onderzoeks- en datajournalistiek naar privacy en surveillance voor *De Correspondent*, waarvoor Maurits Martijn en Dimitri Tokmetzis verschillende journalistieke prijzen wonnen.

Omslagontwerp: Leon Postma (*De Correspondent*) en Martijn van Dam (Momkai)
Creative direction: Harald Dunnink (Momkai)
Redactie: Harminke Medendorp
Eindredactie: Andreas Jonkers
Correctie: Annelieke Tillema
Zetten: Frank August

ISBN 9789083117614
NUR 320

www.decorrespondent.nl

Dit boek is een uitgave van journalistiek platform *De Correspondent*. Wil je vrijblijvend kennismaken? Ga naar corr.es/md21 en ontvang elke zaterdag een gratis artikel in je inbox!

Deze publicatie is tot stand gekomen met steun van het Fonds Bijzondere Journalistieke Projecten.

FONDS Bijzondere JOURNALISTIEKE PROJECTEN

INHOUD

INLEIDING

Op woensdagochtend 9 mei 2018 rent een Nederlander langs een landingsbaan van het vliegveld van de Iraakse stad Erbil. Hij doet het rustig aan. In 29 minuten en 34 seconden legt hij 4,7 kilometer af.

De man, we noemen hem Ton, is een Nederlandse militair die deel uitmaakt van de *capacity-building mission* in Irak, een missie die bij Erbil is gelegerd. Dit is een van de belangrijkste plekken vanwaaruit sinds 2014 de strijd tegen de terroristische groepering Islamitische Staat (IS) wordt gevoerd.

Het is absoluut niet de bedoeling dat wij weten wie Ton is. Als de identiteit van mensen als Ton uitlekt, legt een woordvoerder van Defensie ons later uit, lopen niet alleen deze personen gevaar, maar ook de gehele operatie én de staatsveiligheid van Nederland. Waarom is het dan zo simpel om Tons persoonlijke gegevens te achterhalen?

Ton gebruikt Polar, een populaire fitness-app van Finse makelij. Een app zoals miljoenen hardlopers en fietsers die gebruiken, om hun snelheid, afstand en calorieverbruik te meten.

Als je je aanmeldt voor deze gratis app, krijg je toegang tot een wereldkaart. Op die kaart kun je een locatie bekijken om bijvoorbeeld te zien welke hardlooprondjes er zijn en wie die hebben gerend. Je kunt ook naar bekenden zoeken en zien waar zij allemaal hebben gesport.

Zo komen we Ton op het spoor. We zoeken op de kaart in de buurt van de Iraakse landingsbaan. Daar vinden we Tons werkelijke naam en achternaam en komen we erachter dat hij een Polarhorloge draagt (de Polar V800).

Door op Tons profiel te klikken en zijn geschiedenis te bekijken, ontdekken wij dat veel van zijn Nederlandse hardlooprondjes beginnen en eindigen bij een huizenblok in een Noord-Nederlands dorpje. Met wat aanvullend gegoogel vinden we Tons volledige adres en de namen en foto's van zijn vrouw en kinderen.

En Ton is niet de enige. Via Polar achterhalen we de namen en adressen van meer dan 6.000 mensen van 69 verschillende nationaliteiten die op

200 gevoelige locaties sportten. Locaties zoals militaire bases, nucleaire opslagplaatsen, dronevliegvelden en kantoren van inlichtingendiensten.

Dit is echt niet de bedoeling. In veel landen geldt een strikte geheimhouding voor namen van mensen in vergelijkbare functies. In de Verenigde Staten kun je een tienjarige celstraf krijgen als je de identiteit van een geheim agent openbaart. Op de militaire basis van Erbil mogen de Nederlandse militairen elkaar alleen met de voornaam aanspreken.

Wij leren Tons geheime achternaam kennen door ons in te schrijven voor een sportapp.[1]

PRIVACY STAAT OP DE KAART

De afgelopen jaren is er gigantisch veel aandacht voor privacy gekomen. Het staat hoog op de politieke agenda. Boeken over data, hacken en surveillance zijn bestsellers. Onderzoeksjournalistiek over de verzameldrift van overheden en bedrijven krijgt hoge journalistieke onderscheidingen. Documentaires met titels als *The Great Hack* en *The Social Dilemma* doen het goed op Netflix.

Dit boek, waarvan je een geactualiseerde editie leest, past in die ontwikkeling. Toen *Je hebt wél iets te verbergen* in september 2016 verscheen, konden we niet vermoeden dat het zo'n succes zou worden.

De aandacht was overweldigend, van *De Wereld Draait Door* tot *Koffietijd* en van *NRC* en *Vrij Nederland* tot iedere Belgische kwaliteitskrant. We mochten praten over het boek bij gemeenten, op ministeries, op grote softwareconferenties, bij techbedrijven, op scholen en universiteiten. Er zijn inmiddels meer dan 60.000 exemplaren verkocht.

We zijn onbescheiden genoeg om te stellen dat de kwaliteit van het boek daarbij een rol speelt. Maar we moeten ook eerlijk zijn: het tij zit mee. Was privacy tot voor kort een onderwerp dat maar weinig mensen kon interesseren, sinds een paar jaar is duidelijk dat de datalust van overheden en bedrijven iedereen kan raken. Nu houden niet alleen juristen, journalisten en politici zich met het onderwerp bezig, maar staat privacy bij een groot publiek op de kaart.

In opiniepeilingen geeft een grote meerderheid aan privacy zeer

belangrijk te vinden. Van de deelnemers aan een onderzoek onder 27.000 Europese burgers in 2019 had slechts 14 procent het gevoel volledige controle te hebben over zijn persoonlijke data. 62 procent van de ondervraagden maakte zich hierover grote zorgen.[2]

En in een poll uit 2016 onder 24.143 internetgebruikers uit 24 landen gaf 79 procent van de ondervraagden aan zich ongerust te maken over het gebrek aan online privacy.[3] In de jaren daarna – 2018 en 2019 – geven de respondenten aan zich hierover steeds meer zorgen te zijn gaan maken.[4]

WE HANDELEN ER NIET NAAR

Kijk je naar ons gedrag, dan zie je iets heel anders. Dan geeft 45 procent van de Nederlanders aan bereid te zijn gezondheidsdata af te staan in ruil voor premiekorting. Dan gebruiken we Google en Facebook nog steeds dat het een lieve lust is. Dan verdiepen we ons totaal niet in privacyvoorwaarden en klikken we klakkeloos op 'ja, ik heb de voorwaarden gelezen' en 'ja, ik ga akkoord'. Dan stemmen we gewoon weer op politieke partijen waarvoor privacy het moetje van hun partijprogramma is.

In het dagelijks leven is privacy een waarde die het heel snel van andere waarden verliest. Als we de keuze hebben tussen privacy en gezondheid, tussen privacy en veiligheid of tussen privacy en gemak, dan kiezen de meesten voor het tweede.

Je kunt stellen dat privacy aan dezelfde kwaal lijdt als het klimaat: het baart ons grote zorgen, zeggen we, om vervolgens stilletjes op dezelfde voet verder te gaan en voor de makkelijkste weg te kiezen – zoals we ook in olieslurpende auto's blijven rijden en het vliegtuig nemen naar onze vakantiebestemming.

Ons onderzoek naar Polar laat zien hoe diep dit zit. Zelfs medewerkers van inlichtingendiensten en militairen – mensen die getraind zijn om met gevoelige data om te gaan – kunnen de verleiding niet weerstaan.

HET PROBLEEM BLIJFT ONZICHTBAAR

Dit zien we al zolang we over privacy en surveillance schrijven. Sinds 2013 doen wij dat voor *De Correspondent*, de jaren daarvoor deden we dat voor andere media. Privacy was nog geen onderwerp voor bestsellers, prijswinnende journalistiek en hitdocumentaires. Je moest als journalist nog het onderste uit de kan halen om je hoofdredacteur ervan te overtuigen dat een verhaal over privacy de moeite waard was.

Zo stuitten we vaak op glazige blikken bij onze bazen. Dat lag aan de tijd – privacy stond nog veel minder op de kaart –, maar ook aan onszelf. We konden het simpelweg niet goed uitleggen. Ja, bedrijven die ons surfgedrag bijhouden zijn griezelig, maar waarom precies? Ja, de risicoprofielen die overheden van ons maken zijn totaal ondoorzichtig, maar die kunnen toch ook heel nuttig zijn? Ja, Google en Facebook kennen ons beter dan onze beste vrienden, maar wat is daar eigenlijk mis mee? Zonder privacy geen democratie, zeiden we, maar hoe zit dat dan? En waarom is 'ik heb niets te verbergen, dus ook niets te vrezen' zo'n naïef argument? Wat hebben we dan wél te verbergen?

Een belangrijke reden dat deze vragen zo moeilijk te beantwoorden zijn, is dat we niet *zien* wat er met onze gegevens gebeurt. We zien niet welke overheden, bedrijven en criminelen op onze data jagen, hoe ze dat doen, waarom ze het doen en wat ze er uiteindelijk mee doen.

Deze onzichtbaarheid verklaart ook onze onverschilligheid. Althans: ons gebrek aan daadkracht. Ze verklaart waarom wij het belang van privacy vooral met de mond belijden. Ze verklaart waarom wij denken niets te verbergen te hebben. Ze verklaart waarom geheim agenten en militairen op missie – mensen die niets minder dan hun identiteit te verbergen hebben – gedachteloos hun app aanzetten als ze een rondje gaan rennen.

We zien het niet en daardoor begrijpen we het niet en daardoor voelen we de urgentie niet.

PRIVACY ZICHTBAAR MAKEN

Dus toen wij acht jaar geleden bij *De Correspondent* besloten samen op te trekken in ons journalistieke onderzoek, realiseerden wij ons dat dit de

sleutel kon zijn: als wij erin zouden slagen om het onzichtbare zichtbaar te maken, dan konden we het belang van privacy laten zien. Dit boek is het resultaat van die zoektocht.

Goed onderzoek begint bij een scherpe definitie van het onderwerp. Dat is met privacy geen eenvoudige opgave: over de vele vormen en betekenissen van privacy zijn bibliotheken volgeschreven. Er bestaat bijvoorbeeld zoiets als 'fysieke' privacy, het idee dat mensen jou niet mogen aanraken als je daar geen zin in hebt. Er is 'ruimtelijke' privacy, daarbij gaat het over iemands huis als de plek waarvan onbevoegden niet horen te weten wat er gebeurt. Er is ook 'relationele' privacy, waarbij het draait om vertrouwen binnen verschillende relaties.[5]

In dit boek staat privacy als de bescherming van persoonlijke informatie centraal, 'informationele' privacy volgens de wetenschappelijke literatuur. Onze opvatting van persoonlijke informatie – of 'data' en 'gegevens' – is breed. Van telefoonnummer tot e-mailadres, van online zoekgedrag tot burgerservicenummer, van huisadres tot IP-adres.

Wij volgen daarbij twee sporen. Allereerst onderzoeken wij wat er dagelijks met onze persoonlijke informatie gebeurt. Tegelijkertijd zoeken wij naar het belang van privacy. Waarom moeten wij ons hier zorgen over maken?

De methode die wij daarbij hanteren, is enerzijds klassiek journalistiek: we beantwoorden de wie-, wat-, waar-, waarom- en hoe-vragen over persoonlijke data. Anderzijds maken we gebruik van nieuwe journalistieke onderzoeksmethodes. In de onderzoeksjournalistiek geldt dat je, als je het naadje van de kous wilt weten, het geldspoor moet volgen: *follow the money*. Als je het geld volgt, stuit je op belangen en macht en leg je bloot wat onder de oppervlakte ligt.

Voor onze zoektocht houden wij vast aan een ander adagium: *follow the data*.

Door datasporen te volgen, net zoals bij de Polar-zaak, kunnen we laten zien wat voor informatie wij allemaal over onszelf weggeven en hoe tientallen bedrijven en instanties die data onderling verhandelen en delen. Zo kunnen wij uitvinden welke beslissingen er worden genomen op basis van die data en aantonen hoe die beslissingen onze levens bepalen.

Onze zoektocht brengt ons van dataslurpende apps naar de achterdeuren

van de Belastingdienst, en van zwarte markten in de krochten van het internet tot aan de Amerikaanse douane. We hebben smartphones gekraakt, wifinetwerken gehackt, internetverkeer onderschept, sociale media ontleed, databases leeggetrokken, hackbijeenkomsten gehouden, honderden privacyvoorwaarden uitgekamd, tientallen openbaarheidsverzoeken ingediend en honderden deskundigen en denkers in binnen- en buitenland gesproken.

Voor deze herziene editie hebben we nieuwe bronnen aangeboord, de laatste onderzoeken bekeken, actuele voorbeelden toegevoegd en een nieuw hoofdstuk geschreven over de macht van de grote techbedrijven. We kunnen alvast verklappen: je hebt wél iets te verbergen.

EEN PUBLIEK GOED

Sterker nog: *we* hebben iets te verbergen. Uit ons onderzoek blijkt dat de verzameling, het analyseren en het gebruik van persoonsgegevens grote maatschappelijke gevolgen kunnen hebben, die verder gaan dan het individu. Gevolgen voor de democratie, zoals de Facebook-Cambridge Analytica-zaak laat zien. Voor de staatsveiligheid, zoals uit ons Polar-onderzoek blijkt. Voor de wereldeconomie, waar de dataslurpende Big Techs het besturingssysteem van zijn geworden.

Als wij één les over privacy hebben geleerd de afgelopen acht jaar dan is het deze: privacy is óók een fundamentele waarde voor de hele samenleving. Privacy gaat niet alleen over jou, het gaat over ons allemaal. Het is als drinkwater: een essentieel publiek goed waar wij niet zonder kunnen.

'Als een machine efficiënt loopt [...] dan hoeft men zich alleen te richten op de input en de output, en niet op zijn interne complexiteit. Dus, paradoxaal genoeg, hoe meer succes wetenschap en technologie boeken, hoe intransparanter en obscuurder ze worden.'[6]

– FILOSOOF BRUNO LATOUR

'Als een onbekende man je vraagt je kleren uit te trekken, denk je dat hij gek is; als de onbekende man een dokter is, zou het gepast zijn; als het iemand is met wie je voor het eerst datet, zou het bruusk zijn; op een tweede of derde date is dat misschien wél gewenst.'[7]

– PRIVACYEXPERTS OMER TENE EN JULES POLONETSKY

1

SMARTPHONES EN ANDERE ZWARTE DOZEN

HOE ONS PRIVACYBEGRIP HOPELOOS IS VEROUDERD

Wij beginnen onze zoektocht naar het belang van privacy met het credo: beter goed gejat dan slecht bedacht. In de geweldige verhalenreeks 'What They Know' onderzocht een team van onderzoeksjournalisten en technisch experts van *The Wall Street Journal* de verborgen economie achter het internet.[8] Gedurende twee jaar onthulde de kwaliteitskrant hoe de Amerikaanse internetgebruiker al surfend continu wordt bespied door honderden – vaak onbekende – bedrijven. De journalisten slaagden erin een internationale marktplaats bloot te leggen waar onze persoonlijke gegevens en datastromen handelswaar zijn zonder dat wij het zien.

Wij willen nagaan of we op Nederlandse sites net zoveel door bedrijven bespioneerd worden als in de Verenigde Staten. Alleen: hoe onderzoek je dit? Voor ons is dit nieuw terrein, ook al gaan wij beiden zeker niet bleu dit onderwerp in. Dimitri publiceerde in 2012 al uitvoerig over privacy en digitale profielen in zijn boek *De digitale schaduw*. Maurits schreef een aantal jaar voor *Vrij Nederland* over hackerscultuur, de surveillance-industrie en de datahonger van de Nederlandse overheid. Maar dit is andere koek.

Dit is een nieuwe, opwindende vorm van onderzoeksjournalistiek.

De journalisten van *The Wall Street Journal* werkten intensief samen met techneuten en onderzoekers. Het team bouwde zelf software om het web af te kunnen struinen en combineerde klassieke vormen van journalistiek met baanbrekende datajournalistiek. De serie werd geprezen en genomineerd voor een Pulitzerprijs.

Via via komen we in contact met Ashkan Soltani, de hoofdonderzoeker van 'What They Know'. In een Amsterdamse koffietent legt hij ons uit hoe we ons onderzoek op kunnen zetten. 'Journalistiek zal in toenemende mate dit soort onderzoek nodig hebben,' vertelt hij. Soltani raadt ons aan te beginnen bij de websites die we allen dagelijks bezoeken op onze desk- of laptop. Helaas kan hij ons daar niet bij helpen, zegt hij. Niet veel later begrijpen wij waarom: hij is ingehuurd door *The Washington Post* om de technische analyse te doen van de honderden documenten die via Edward Snowden zijn uitgelekt. De krant en Soltani zullen voor hun berichtgeving dit keer wel bekroond worden met een Pulitzerprijs.

DE GLUURDERS OP ONZE LAPTOPS

Op advies van Soltani schakelen we de hulp in van wetenschappers die ervaring hebben met dit soort onderzoek: Lonneke van der Velden en Anne Helmond van de Universiteit van Amsterdam. Beiden zijn betrokken bij het Digital Methods Initiative van de universiteit, waar zij met collega's de zogenoemde Tracker Tracker-tool ontwikkelden.[9] Deze software kan voor een belangrijk deel hetzelfde als de software van de onderzoekers van *The Wall Street Journal.* Met de tool is het mogelijk om een site te scannen en zo de zogenoemde *trackers* op de site te identificeren en in kaart te brengen.

Trackers worden door bedrijven ingezet om informatie over websitebezoekers te verzamelen. Meestal zijn dit cookies: data die op jouw computer of laptop worden achtergelaten als je een site bezoekt. Daarmee kunnen bedrijven je surfgedrag, locatie en informatie over je computer aan elkaar koppelen om daarmee een persoonlijk dossier op te bouwen. Vaak wordt meer geavanceerde technologie ingezet. Dan registreren bedrijven bijvoorbeeld de instellingen van je browser: de taal, welke plug-ins je hebt geïnstalleerd, het besturingssysteem. Soms werken trackers ook met geluid. Er bestaan apps op smart-tv's die een voor ons onhoorbare toon versturen die wordt opgevangen door een app op je telefoon.[10] Zo is te achterhalen naar welke programma's je kijkt en welke apparaten er bij elkaar in de buurt zijn.[11]

Bedrijven trekken alles uit de kast om online zo veel mogelijk over ons te weten te komen. Want hoe meer zij weten, hoe beter en effectiever zij ons online advertenties kunnen voorschotelen. Dit gaat over miljarden. In 2015 werd er wereldwijd voor het eerst meer aan webadvertenties besteed dan aan tv-reclames: zo'n 125 miljard euro.[12] In 2020 liep dit op tot ruim 330 miljard en in 2024 zouden de onlineadvertentiebestedingen een haast onvoorstelbare 500 miljard kunnen bedragen.[13] Ruim twee derde van die onlineadvertentiebestedingen ging in 2020 naar Google, Facebook en Amazon.[14]

Met de Tracker Tracker-tool van de Universiteit van Amsterdam is het mogelijk om te achterhalen welke trackers websites achterlaten op de computers van bezoekers. We gaan aan de slag en nemen op onze laptop de honderd populairste sites van Nederland onder de loep: van nu.nl tot

marktplaats.nl en van zalando.nl tot voetbalzone.nl. En plotseling ziet het internet er onherkenbaar uit. Aan de voorkant doet het zich voor als een verzameling sites, geklets op sociale media, kattenfilmpjes en links, aan de achterkant zien we met de tool een verzameling commerciële partijen die aan elkaar vastgeklonterd zitten rond onze datastromen.

In totaal ontdekken we op de honderd geteste sites trackers van 215 verschillende bedrijven. We besluiten de privacyvoorwaarden van deze bedrijven door te vlooien: welke data verzamelen ze, hoelang bewaren ze die en met wie delen ze die?

We schrikken van de resultaten. Neem nieuwssite nu.nl. In totaal vinden we 44 trackers op die site, onder meer van bedrijven die in hun voorwaarden schrijven dat ze de recente surfgeschiedenis en ingevoerde zoektermen van jou als sitebezoeker verzamelen, je type computer registreren en je demografische gegevens achterhalen. Twee bedrijven zeggen in hun privacyvoorwaarden daar 'persoonlijk identificerende informatie' aan te kunnen koppelen die ze van andere partijen kopen of ontvangen, zoals je naam en geboortedatum, je financiële situatie en informatie over je werkgever.

Als we surfen en browsen zijn we geneigd ons alleen en onbespied te wanen, zoals we ons alleen en onbespied wanen als we 's ochtends de krant lezen aan de keukentafel. Maar online worden we constant gestalkt door onbekende partijen die van alles van ons willen weten. Ze begluren en analyseren ons. Zij zien ons, we zien hen niet.

DE GLUURDERS OP ONZE SMARTPHONES

Na de huis-tuin-en-keukenlaptop vervolgen we ons onderzoek met het apparaat dat we de hele dag door gebruiken: de smartphone. De smartphone is zonder enige twijfel de succesvolste consumententechnologie van de afgelopen tien jaar. Er zijn nu bijna 4 miljard gebruikers en dat aantal stijgt rap. We gebruiken de smartphone ook steeds méér: meer minuten per dag, meer dataverbruik.[15]

Tegelijkertijd begrijpen we nagenoeg niks van dat ding.

Het is een ultiem voorbeeld van wat de Franse filosoof Bruno Latour een ‘black box’ noemt: een apparaat dat werkt als een trein maar waarvan de échte werking mysterieus blijft. ‘Als een machine efficiënt loopt,’ schrijft Latour, ‘dan hoeft men zich alleen te richten op de input en de output, en niet op zijn interne complexiteit.’

Ja, je weet waar je op moet drukken om de smartphone te gebruiken (input) en begrijpt *wat* hij als reactie daarop zal doen (output) – bellen, surfen, appen, et cetera – maar *hoe* het apparaat dat allemaal doet? Niet voor niets luidde de slogan van Apple jarenlang: ‘*It just works*.’

Bij de smartphone is het een bewuste keus geweest om ’m dicht te houden. In principe is een smartphone een computer, met dit verschil: een normale computer is relatief open. Je kunt er zelf programma’s voor schrijven en erop installeren wat je wilt. Toen Steve Jobs in 2007 de iPhone lanceerde, maakte hij direct duidelijk dat dit niet voor zijn kroonjuweel zou gelden. ‘Wij bepalen wat op de telefoon wordt toegelaten,’ zei Jobs tijdens de presentatie van het apparaat. Een aanpak die de standaard zou worden in de booming smartphonebusiness. Want je kunt swipen wat je wilt, nergens zul je zien wat het besturingssysteem precies doet en welke data jouw apps gebruiken.

En dat is raar. Want als je nagaat welke rol de smartphone in ons leven speelt, dan kun je eenvoudig beargumenteren dat wij het ding juist wél zouden moeten doorgronden. De smartphone is – nog meer dan onze laptop – ons venster op de wereld, ons primaire communicatiemiddel, onze assistent.

Wie toch onder die motorkap wil kijken, heeft geen andere keus dan zijn eigen smartphone te hacken; die motorkap open te breken met een digitale koevoet. De terminologie om het apparaat binnen te kunnen dringen is wat dat betreft veelzeggend. Als je meer te zeggen wilt hebben over een iPhone, moet je hem ‘jailbreaken’. Op een Androidtoestel moet je ‘*root access*’ zien te krijgen. In de computerwereld is degene met root access de beheerder. De boodschap is duidelijk: jij bent dat niet.

Ashkan Soltani van *The Wall Street Journal* heeft ons gewaarschuwd dat het blootleggen van trackers op een desk- of laptop kinderspel is vergeleken met het doorgronden van de datastromen van een smartphone. De Tracker Tracker-tool die wij gebruikten voor ons onderzoek naar de