22 mei 2014

Eerder schreven correspondent Maurits Martijn en ik over online trackers die ons gedrag registeren via pc's en laptops. Vandaag het vervolg: wat houdt het apparaat in onze broekzak allemaal over ons bij? Na langdurig onderzoek naar 85 populaire apps ontdekte ik hoe de smartphone vol privacygevoelige lekken zit.

Dit gebeurt er allemaal onder de motorkap van je smartphone

Correspondent Data & Transparantie

Dimitri Tokmetzis

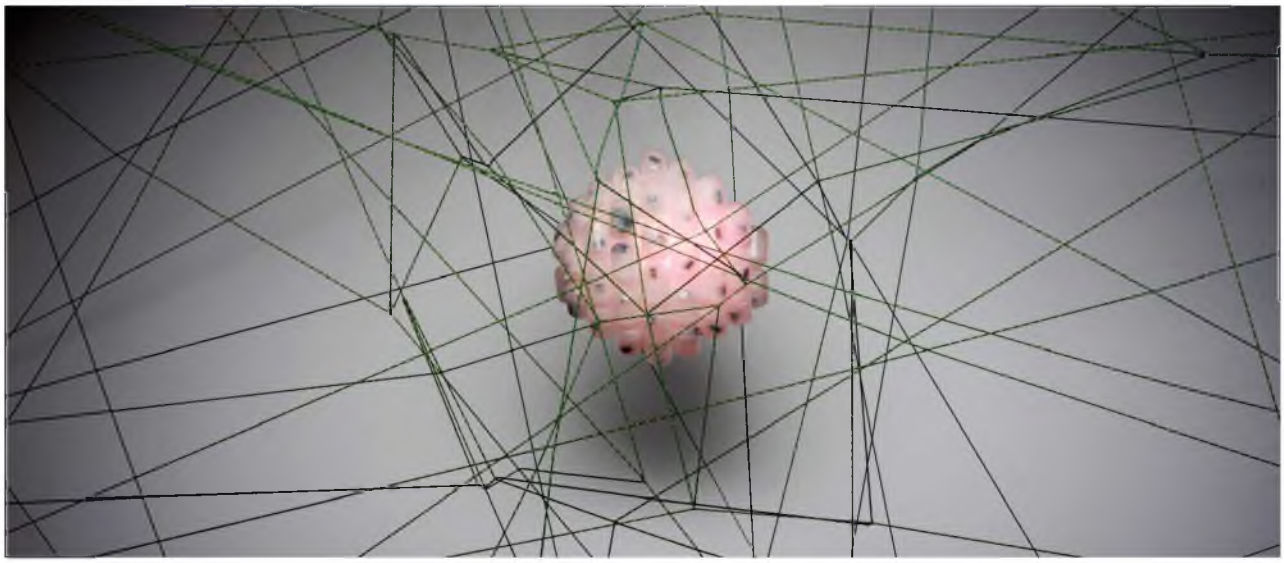

Foto: Rein Janssen (voor De Correspondent)

Ik hou van mijn smartphone. Mijn Samsung Note III is een venster op de wereld, mijn persoonlijke assistent die altijd klaarstaat met de juiste informatie. Waar en wanneer ik wil, lees en luister ik de beste journalistiek, bekijk ik informatieve en vermakelijke filmpjes, plan ik afspraken in en vind ik de weg in vreemde steden. Als ik ver van huis ben, warm ik mezelf

op aan de foto's van mijn kinderen en WhatsApp'jes met vrouw, vrienden en familie. En oh ja, ik bel er weleens mee.

Ja, ik hou van mijn smartphone, maar het apparaat is het laatste halfjaar een totale obsessie voor mij geworden. En een grote bron van frustratie.

Ruim een halfjaar geleden zochten colllega-correspondent Maurits Martijn en ik uit door welke bedrijven we browsend op een pc worden gevolgd. *Lees hier: Big Business is watching you.* We concludeerden dat ons internetgedrag continu door tientallen commerciële partijen bekeken wordt. Saillant was dat de verantwoordelijke websitebeheerders vaak niet op de hoogte waren welke *trackers* hun publiek in de gaten hielden. Maar er was ook goed nieuws. Zelfs als niet-technische internetter kun je je nog aardig wapenen *Lees hier: Hoe kun je trackers blocken?* tegen dit volggedrag, bijvoorbeeld door cookies te blokkeren in je browser.

We wilden hetzelfde onderzoek uitvoeren op smartphones. Een smartphone is evengoed een computer, maar werkt heel anders dan een lap- of desktop. Een computer is relatief open. Je kunt er zelf programma's voor schrijven en er op installeren wat je wilt. Een computer moet een alleskunner zijn. Maar toen Steve Jobs de iPhone lanceerde, was het gedaan met die openheid: 'Wij bepalen alles wat op de telefoon wordt toegelaten,' zei de grote roerganger tijdens de presentatie van de iPhone.

Smartphones zijn daarom helemaal dichtgetimmerd. Apple en Google bepalen welke apps je kunt downloaden. Het besturingssysteem, iOS of Android bijvoorbeeld, bepaalt welke data die apps kunnen gebruiken. Je kunt *swipen* wat je wilt, je zal nergens zien wat dat besturingssysteem precies doet; wat die regels voor datagebruik precies behelzen.

Hoe een smartphone werkt, blijft verborgen onder de motorkap.

Na lang, heel lang zoeken is het gelukt die motorkap open te breken. Althans, grotendeels. Ik heb 85 populaire apps getest en duizenden datasporen gevolgd. Ik zag hoezeer mijn smartphone onderdeel is van een complex, internationaal web van commerciële datastromen, waarbij mijn data over de hele wereld vliegen en bij honderden verschillende bedrijven terechtkomen. En daar heb je nauwelijks invloed op. Uiteindelijk heb je weinig tot niets over je eigen data te zeggen.

De Bijenkorf vraagt toestemming

De motorkap kreeg ik open door een zogenoemde *man-in-the-middle attack* uit te voeren *Lees hier een uitgebreide methodologie.* met Charles, een programma dat door app- en webontwikkelaars wordt gebruikt. Ik leidde het dataverkeer van mijn smartphone naar de router om via mijn laptop. Door een vals beveiligingscertificaat te installeren, kon ik ook beveiligd verkeer zien. Ik volgde zo milliseconde voor milliseconde met welke servers mijn smartphone contact legde en welke informatie daarbij werd verzonden en ontvangen.

> En nog graag toestemming om mijn agenda te lezen, afspraken te plannen en wijzigen en zonder mijn medeweten mails kunnen sturen aan mensen die in mijn agenda staan

Een voorbeeld.

Ik installeer de populaire shop-app van De Bijenkorf. Voordat de installatie plaatsvindt, vraagt de Google Play Store of ik de app een aantal toestemmingen wil verlenen. De app

wil graag netwerkinformatie kunnen zien - of ik op wifi zit bijvoorbeeld. Of hij gebruik mag maken van de trilfunctie en mag voorkomen dat het toestel in slaapstand sukkelt. De app wil graag gegevens op mijn geheugenkaart schrijven of wijzigen. Hij wil gebruik kunnen maken van de camera. Mijn precieze (gps) en ruwe(netwerkgebaseerde) locatie weten. En: toestemming om mijn agenda te lezen, afspraken te plannen en te wijzigen en zonder mijn medeweten mails te kunnen sturen aan mensen die in mijn agenda staan.

Natuurlijk. Gaat uw gang, beste Bijenkorf. Alles voor het experiment.

Besprongen door commerciële *trackers*

Het is 11.47 uur. Ik druk op het Bijenkorf-icoontje. Nog voordat de app opent en de inhoud wordt geladen, plaatst Google een cookie op mijn toestel waardoor het bedrijf mij kan volgen. Kort daarna zie ik dat de Bijenkorf-app mijn toestel een unieke *id* geeft. Vanaf nu kan De Bijenkorf mij identificeren, ook als ik de app een tijd niet gebruik. Als ik de homepage van de app bekijk, meldt Google Analytics zich in Charles. In de zesde minuut dat ik de app gebruik, zal Google Analytics een trouwe vriend blijken die continu aan mijn zijde blijft.

Ik besluit een Bijenkorf Card aan te vragen. Om 11.48 maakt de app contact met een server in Seattle in Amerika. Die is van Amazon, maar wordt gehuurd door Intershop, een groot internationaal bedrijf dat De Bijenkorf helpt bezoekers realtime te analyseren. Ook statistiekbedrijf Shop2Market komt het toneel opgestormd om, net als Google Analytics, mijn kijkgedrag *swipe* na *swipe* te analyseren. Op het moment dat ik mijn account voor de Bijenkorf Card aanmaak, komt ook advertentiegigant Google Doubleclick even kijken wat ik aan het doen ben.

Eindelijk ben ik klaar om te shoppen. En dan gebeurt er iets geks.

Terwijl ik naar een luxe zwartlederen laptoptas kijk (meer dan 500 euro), wordt mijn smartphone besprongen door zeker achttien verschillende online advertentiebedrijven die allerlei data van en naar hun servers sturen. Het is een blitz-aanval. In één enkele seconde wordt contact gelegd met servers in de Verenigde Staten, Zweden, Duitsland, Ierland en Nederland van bedrijven die luisteren naar namen als Improve Digital, Admeta, Adtech, Metrigo, Burst Media, Yieldlab, Switch Concepts, AppNexus, Sociomantic, Adscale, Rubicon Project, OpenX, Smart Adserver en Casale Media.

Illustratie: Momkai

Wat doen die trackers in mijn app?

Wat al deze *trackers* precies doen in deze app, is een heus mysterie. AppNexus is een platform voor *real-time bidding*, een flitsveiling waarin adverteerders in milliseconden tegen elkaar opbieden om mij een advertentie te mogen leveren *Lees hier: Jouw aandacht wordt talloze malen aan de hoogste bieder verkocht.* die bij mijn interesses aansluit. Een aantal andere bedrijven, zoals Admeta, Adtech, Burst Media en Rubicon Project, levert de techniek om te bieden.

Maar de Bijenkorf-app laat helemaal geen externe advertenties toe. Het zou nog kunnen dat deze bedrijven nu bieden om mij later, op andere websites, advertenties van De Bijenkorf te mogen laten zien.

De app laadt de mobiele site in, waardoor ook de *trackers* automatisch worden meegeladen. Daar worden die *trackers* gebruikt om bezoekers te volgen

Met wie praat jouw smartphone?

Hoe vaak communiceerde mijn smartphone met servers in deze landen?

Land	Aantal	Land	Aantal
Verenigde Staten	7384	China	33
Nederland	3116	Oostenrijk	24
Ierland	495	Zweden	20
Duitsland	219	Zwitserland	15
Verenigd Koninkrijk	167	Denemarken	11
Rusland	140	Japan	3
Italië	79	Tsjechië	2
Canada	71	Brazilië	1
Frankrijk	44		

Hoe vaak communiceerde mijn smartphone met deze bedrijven?

Organisatie	Aantal	Organisatie	Aantal
Google	4560	Publieke Omroep Nederland	332
Amazon.com	1302	RTL Nederland Interactief B.V.	299
Akamai Technologies	587	Microsoft Hosting	256
XS4ALL Internet BV	512	Facebook	228
EdgeCast Networks	481	Level 3 Communications	196

Hoe vaak communiceerden deze apps met een server?

App	Aantal	App	Aantal
Google Earth	1153	Nikeplus	163
Bijenkorf	747	McDonald's	159
500px	497	LinkedIn	154
The Guardian	277	Viber	144
Tinder	258	Clean Master	143
KLM	248	Womanlog	140
MyFitnessPal	213	Strava	134
Zite	184	Ingress	119
Shazam	167		

Maar ook dat is hier niet het geval, zegt woordvoerder Michel Bos van De Bijenkorf. Het warenhuis werkt alleen samen met Sociomantic, een bedrijf dat de *retargeting* van bekeken producten verzorgt. En dit is de enige *tracker* die in de *privacy policy* van de Bijenkorf-website wordt genoemd.

De verklaring is veel banaler. De app laadt de mobiele site in, waardoor ook de *trackers* automatisch worden meegeladen. Daar worden die *trackers* gebruikt om bezoekers te volgen.

Volgens Bos zijn die *trackers* 'functieloos.' Ze registreren niets in de app. 'We begrijpen dat hier verwarring over kan ontstaan bij experts en zullen binnenkort de app aanpassen zodat de gegevens niet worden opgeslagen. Dank dat je ons hier attent op hebt gemaakt.'

Websites weten zelf niet wie hun publiek allemaal volgt.

Diarree en gevoelige borsten

Soms leidt die onwetendheid van app-aanbieders tot ronduit onveilige apps.

Op verzoek van een lezer test ik WomanLog, een app waarmee vrouwen inzicht kunnen krijgen in hun menstruatiecyclus. Die is wereldwijd meer dan 5 miljoen keer gedownload in de Google Play Store. De app toont een kalender waarin ik allerlei informatie over mijn lichaam kan invullen. Vervolgens maak ik een *back-up*, een feature die app-maker Pro Active App in de gratis versie heeft ingebouwd.

In die *back-up* zit echter een veiligheidslek.

Want wat zie ik terug in Charles? Dat ik, volgens WomanLog, op 10 april seks had. Dat ik last heb van gevoelige borsten, diarree en mij hongerig voelde. Dat ik de pil gebruik en mij op 6 april verdrietig voelde. De meest intieme informatie vliegt onbeschermd door de ether. Iedereen die op hetzelfde wifi-netwerk zit, kan probleemloos dit soort informatie onderscheppen.

Van de 85 onderzochte apps vond twee derde van het dataverkeer zo open en bloot plaats.

Veelzeggender dan je dna-profiel

Terug naar de *trackers*. Wie volgen jou op je smartphone, welke data kunnen ze onderscheppen en wat doen ze daarmee?

Op de 85 onderzochte apps vond ik 67 verschillende *trackers*. Ruim twee derde van die *trackers* wordt gebruikt door advertentiebedrijven. Zestien bedrijven leveren *analytics*-diensten: die bekijken dus hoe je je gedraagt op de app, waar je naar kijkt en waar je op klikt. Deze *analytics* worden doorgaans door de websites zelf gebruikt om inzicht te krijgen in hun bezoekers. Er is één bedrijf dat deze mobiele surveillance domineert: Google. Op de 85 apps kwam ik minstens 104 keer een *tracker* van Google tegen.

Een ander interessante *tracker* is Flurry, die ik op 25 apps ben tegengekomen.

> Flurry volgt gemiddeld zeven apps op 1,3 miljard smartphones en tablets. Iedere maand ziet en noteert het bedrijf 150 *miljard* keer dat een app, die Flurry volgt, wordt gebruikt

Naar eigen zeggen volgt Flurry gemiddeld zeven apps op 1,3 miljard toestellen

(smartphones en tablets). Iedere maand ziet en noteert het bedrijf 150 *miljard* keer dat een app, die Flurry volgt, wordt gebruikt. Hiermee kan Flurry gedetailleerde gedragsprofielen opbouwen. '*Your app signature is more distinctive than your DNA*,' pocht het bedrijf.

Maar Flurry verzamelt meer: locatiegegevens, identificatienummers van je toestel, taal, soort smartphone of tablet, telefoonaanbieder. Het biedt ook zogenoemde '*Enhanced Personas*' aan. Dit zijn (potentiële) klanten over wie uit *offline* databases extra informatie wordt verzameld, zoals inkomen, aantal kinderen en reisvoorkeuren. Adverteerders kunnen die inzichten vervolgens kopen om zeer gerichte aanbiedingen te doen.

Flurry voert een nogal discutabel privacybeleid, blijkt uit onderzoek van Privacychoice.org. Het enige positieve dat deze organisatie hierover te zeggen heeft, is dat Flurry gebruikers anonimiseert. Maar in de online wereld is anonimiteit betrekkelijk. Als je iemand kunt blijven volgen aan de hand van een uniek identificatienummer maakt het niet uit of hij Pietje of Jantje heet. Je kan nog steeds een uitgebreid gedragsprofiel van iemand opbouwen.

Bovendien is Privacychoice.org kritisch over het feit dat Flurry zwijgt over hoe lang gegevens bewaard worden. De *tracker* sluit daarnaast niet uit dat er ook gevoelige gegevens worden opgeslagen, zoals bijvoorbeeld van gezondheidsapps. Het eindoordeel van Privacychoice.org is duidelijk: 'Zorgelijk.'

Illustratie: Momkai

WhatsApp-berichten stelen

Flurry doet iets wat niet de bedoeling is: het volgen van gebruikers door verschillende apps. Het besturingssysteem van de iPhone en Android-toestellen is erop gericht de datastromen van apps zoveel mogelijk te scheiden. Dit wordt ook wel *sandboxing* genoemd. App-aanbieders mogen alleen zien wat er in hun eigen app gebeurt.

Maar in de praktijk blijken die harde grenzen behoorlijk poreus. Bas Bosschert, een Nederlandse webontwikkelaar, toonde *Lees hier Bosscherts artikel: 'Stealing WhatsApp database.'* begin maart aan dat hij via een zelfgebouwde app de chats en berichten van WhatsApp kon ontfutselen op Android-toestellen.

En dat komt door de toestemming die wordt gebruikt bij het installeren van apps: '*modify or delete the contents of your USB storage*.' In mijn onderzoek werd deze toestemming bij 58 van de 85 apps gevraagd.

Met deze toestemming heeft een app toegang tot je geheugenkaart. Veel apps hebben dat nodig. Spelletjes willen bijvoorbeeld scores kunnen opslaan. Een camera-app wil foto's opslaan in het geheugen. Maar met deze toestemming kun je dus óók bij de opslag van andere apps komen.

Wat Android anders doet dan iOS

Dit roept de vraag op waar je eigenlijk toestemming voor geeft als je een app installeert.

Dit verschilt erg per besturingssysteem. Als je een app installeert op je iPhone geef je nergens toestemming voor. Pas als een app daadwerkelijk gevoelige data wil gebruiken, word je toestemming gevraagd.

Android werkt heel anders. Als je een app installeert, moet je van tevoren akkoord gaan met de zogenoemde 'permissies' die de app van je vraagt. Iedere app moet een *Permission Manifest* hebben waarin de verleende permissies staan opgesomd. Android zorgt er dan

Welke gegevens probeerden deze apps van mijn smartphone te halen?

Identificerende gegevens

App	Aantal
Torchy Tiny Flashlight	12
Runtastic	12
Facebook messenger	5
Clean Master	4
Snapchat	4
Viber	4
Hill Climb Racing	4
LinkedIn	4
Outlook.com	3
Temple Run 2	3

Locatiegegevens

App	Aantal
Runtastic	22
Facebook messenger	11
Skype	9
Ingress	7
LinkedIn	7
Foursquare	6
Viber	6
Buienalarm	5
Shazam	4
Instagram	4

Telefoongegevens (oproepen, caller-id)

App	Aantal
Runtastic	36
Torchy Tiny Flashlight	34
NPO	34
Facebook messenger	18
Clean Master	15
Hill Climb Racing	13
Viber	12
Skype	9
Spotify	9
Netflix	9

Contactgegevens

App	Aantal
Skype	6
Viber	3
LinkedIn	3
Tinder	2
GTST	2
Noufree	2
Jelly Splash	2
Telegraaf	2
Lingo Nederlands	2
Crack My Screen	2

voor dat de app nooit méér data kan krijgen dan in het manifest staan, dus waar je toestemming voor hebt gegeven.

> Wat moeten Angry Birds, LinkedIn, Shazam, Skype, Snapchat, TVGids en Viber bijvoorbeeld met je locatie?

Het Android-systeem is om verschillende redenen problematisch.

Ten eerste is het slikken of stikken. Je moet *alles* goedkeuren om de app te kunnen gebruiken. Het is logisch dat muziek-app Shazam toegang vraagt tot je microfoon en internet: hij moet immers een melodie horen en die vergelijken met zijn eigen database. Maar is het nodig dat Shazam je precieze locatie opslaat?

Ten tweede vragen apps vaak om onnodig toestemmingen. Toegang tot het internet bijvoorbeeld (vrijwel alle 85 onderzochte apps vragen daarom). Veel apps hebben dat niet nodig. En wat moeten Angry Birds, LinkedIn, Shazam, Skype, Snapchat, TVGids en Viber bijvoorbeeld met je locatie?

Waar geef je eigenlijk toestemming voor?

Het grootste probleem is dat je na dit permissiecircus nog steeds niets weet.

Ten eerste zwijgen de toestemmingen over alle *trackers* die een app laadt, maar die wel degelijk allerlei informatie van je opslurpen. Als je daar inzicht in wilt krijgen, moet je eerst de vaak lange *privacy policy* van de app doorlezen. Als die er al is.

Ten tweede, waar geef je nu eigenlijk toestemming voor? Wat betekent het dat een app jouw 'Google *service configuration*' kan lezen? Is het bezwaarlijk dat een app kan zien welke andere apps actief zijn? Voor een gewone gebruiker zal dit abracadabra zijn.

Ten derde zijn deze toestemmingen maar een deel van het verhaal: onder iedere permissie schuilen weer allerlei 'subtoestemmingen.' Via de app Xprivacy *Lees hier meer over XPrivacy, een app die ik van harte aanbeveel aan Android-gebruikers.* kan ik bijvoorbeeld zien dat de 85 onderzochte apps 53 keer mijn '*hardware serial number*' hebben opgevraagd. Dit valt waarschijnlijk onder de categorie '*personal information*', maar dat is giswerk.

Illustratie: Momkai

Jailbreaken en *rooten*

Het gebrek aan informatie is vervelend. Echt frustrerend is dat het zo moeilijk is controle te krijgen over je smartphonedata.

Paradoxaal genoeg moet je de beveiliging van je smartphone dus breken om je eigen data beter te beschermen. Maar dat gaat niet zonder slag of stoot.

De terminologie is veelzeggend. Als je meer zeggenschap wilt over je iPhone, moet je hem '*jailbreaken*.' Een Android-toestel moet je '*rooten*.' Dit vereist echter flink wat technische kennis. En als het misgaat, zit je met een probleem: de garantie op je smartphone vervalt. Apple heeft zelfs via de rechter geprobeerd een verbod op *jailbreaking* af te dwingen.

Met welke trackers communiceerde mijn smartphone?

Type tracker

Type	Aantal
Ad network of Ad exchange	27
Advertentie-leveranciers	22
Analytics en meten	16
Retargeter	3
Web tool of widget	3
Onbekend	2
Koper van advertenties en data	2
Uitgever (dus website)	1
Datahandelaar	1

Hoeveel verschillende trackers zijn waargenomen?

App	Aantal trackers
Bijenkorf	22
Shazam	9
AntiVirus Security Free	8
MyFitnessPal	8
KLM	7
Runtastic	6
Nikeplus	6
Where is my droid	5
Sleep Cycle	5
Crack My Screen	5

Welke trackers kwamen het meest voor?

Trackers	Aantal keren waargenomen
Google Doubleclick	37
Google Analytics	32
Flurry	25
Google Adsense	12
ComScore	9
Chartboost	8
Ad-x (Criteo)	6
Adobe	5
Mobileapptracking	4
Adtrack King	4

Hoe vaak maakten trackers gebruik van een beveiligde verbinding?

Beveiligd?	Aantal keer onbeveiligd
Nee	1721
Ja	776

Je intieme smartphone

Is dit gebrek aan controle erg?

Als je erg bezorgd bent over je privacy, dan moeten smartphones een gruwel zijn. Je hebt als gewone gebruiker geen zicht op wie met welke data aan de haal gaat. Daarnaast heb je nauwelijks mogelijkheden om die datastromen af te knijpen of te sturen.

Een smartphone is méér dan een telefoon. Een smartphone is een krachtige pc. En heel intiem. Hij houdt bij wat je doet, waar je bent, met wie je communiceert, hoe je reist, waar je naar kijkt en luistert, wat je leest, wie je leuk vindt, wat je graag doet. En onze smartphones komen steeds dichter op onze huid te zitten. Letterlijk. Je draagt straks wellicht een Google Glass op je neus. Onlangs is er een Android-versie opgeleverd voor *wearables*, zoals slimme horloges. Deze *wearables* zullen ook weer allerlei data opzuigen over je gedrag. *Niet overtuigd? Lees dan dit verhaal: Hoe je onschuldige smartphone bijna je hele doorgeeft aan de geheime dienst.*

Die nieuwe rijkdom aan data maakt het voor advertentiebedrijven mogelijk meer gedetailleerde profielen op te bouwen. Omdat er zoveel gedragsdata worden onderschept, zijn er steeds meer mogelijkheden voor manipulatie. Advertentiebedrijven meten waar en op welke sites ze je het beste kunnen bestoken, op welke momenten je het meest geneigd bent iets te kopen. Als één bedrijf dat doet, is dat niet zo problematisch. Als honderden bedrijven je continu proberen te sturen, thuis, onderweg en op je lijf, krijg je een andere discussie. *Lees hier het verhaal van Maurits Martijn: 'Hoe reclameman Don Draper het aflegt tegen Big Data.'*

Volgens Frederik Borgesius, promoverend internetjurist aan de UvA, is smartphonesurveillance totaal uit de hand gelopen. Hij durft wel te stellen dat via smartphones de Europese wetgeving (grotendeels uit 1995!) grootschalig wordt geschonden. Hij schetst het dilemma. 'Wie moet daar tegen optreden? Privacytoezichthouder College Bescherming Persoonsgegevens heeft slechts enkele tientallen werknemers om te handhaven. Waarschijnlijk helpen alleen zeer hoge boetes. Daar wordt nu in Brussel aan gewerkt.'

Een belangrijker probleem, aldus Borgesius, is wellicht de smartphonegebruiker zélf die overal maar 'ja' op klikt. De vraag die al jaren wordt gesteld, maar waar nog steeds geen goed antwoord op lijkt te bestaan, is deze: hoe zorg je ervoor dat de gebruiker een geïnformeerde én gebruiksvriendelijke én echte keuze kan maken?

Smartphonesurveillance is een politiek probleem

Tot slot is het gebrek aan controle ook een dringende politieke kwestie. *The Washington Post* onthulde begin dit jaar dat de National Security Agency (NSA) gulzig smartphones leegtrok, op zoek naar locatiedata, contactgegevens en belgeschiedenissen. *Lees hier het stuk in The Washington Post.* De NSA maakt ook gebruik van advertentienetwerken en gebruikt bijvoorbeeld commerciële cookie-data om smartphonebezitters te volgen. *The Guardian* onthulde *Lees hier het verhaal in The Guardian.* dat data van het spelletje Angry Birds, verwerkt door advertentiebedrijf Millennial Media, ook systematisch werden onderschept. De NSA kon hiermee op grote schaal mensen online volgen.

> Gebruiksgemak en schoonheid brengen kosten met zich mee die we nog niet goed kunnen beprijzen

Bij het maken van dit verhaal moest ik daarom vaak denken aan het boek *The Future of*

Internet and how to stop it *Je kunt het boek hier gratis downloaden.* van Jonathan Zittrain, een invloedrijke internetjurist aan het Massachusetts Insitute of Technology. Hij schrijft: '*The iPhone is both a product of fashion and fear.*' En dat geldt net zo goed voor Android.

Smartphones zien er mooi uit. Ze werken. Doen wat ze moeten doen. En kunnen waarschijnlijk nog veel meer dan we weten. Maar gebruiksgemak en schoonheid brengen kosten met zich mee die we nog niet goed kunnen beprijzen.

Ja, ik hou nog steeds van mijn smartphone. Maar de liefde is wel aanmerkelijk bekoeld.

Ik kon dit artikel niet schrijven zonder hulp van de volgende personen, die ik bij dezen wil bedanken: Maurits Martijn, Lysander Vogelzang, Tieme van Veen, Marcel Bokhorst, Guido Rus, Mark Steenbakkers, James Sellwood, Lukasz Olejnik, Michael Bevz, Jeroen van Raalte en Manon van den Brekel.