Privacyopties Windows 10

Rein de Jong

De Big Brother Awards zijn weer uitgereikt dit jaar. De winnaars zijn minister Plasterk en de korpschef Politie. Beiden zijn daarmee door experts uitgeroepen tot de grootste privacyschenders van Nederland. De korpschef vanwege het inzetten op 'predictive policing' oftewel het voorspellen van strafbaar gedrag zodat ingegrepen kan worden voordat een strafbaar feit is gepleegd. Hiermee wordt *afwijkend gedrag* de graadmeter voor politieoptreden in plaats van *strafbare feiten*. Binnenlandse Zaken en minister 'Tapsterk' beschouwen burgers als verdacht omdat ze iedereen zo ongericht (kunnen) afluisteren.

Privacy is een groot goed, dat moeten we koesteren. Privacy gaat er niet om dat we iets illegaals willen verbergen. Privacy gaat erom dat we ons in onze privéomgeving kunnen en mogen gedragen zoals we dat zelf wensen. **Het recht om jezelf te zijn zonder bang te hoeven zijn voor reacties van anderen**. Onder het mom van veiligheid wordt druk uitgeoefend om dat recht op persoonlijke levenssfeer vergaand op te geven. Hoe erg aanslagen en criminaliteit ook mogen zijn, dat mag nooit een reden zijn om zonder enige grond voor verdenking je privacy te moeten opgeven!

Buiten het feit dat de overheid er alles aan doet om je persoonlijke levenssfeer binnen te dringen, is er een groot aantal bedrijven die ook graag van alles over ons willen weten. Dan gaat het meestal niet om veiligheid, maar om reclame of inzicht in het gebruik van een product. Het zijn echter vooral bedrijven zoals Apple en Microsoft die er van worden beticht onze privacy te schenden. We dienen echter te beseffen dat de overheid een veel grotere schender van onze rechten is; daarvan getuigen de Big Brother Awards van de afgelopen jaren.

Over omgang met de privacy van Windows 10-gebruikers is veel te doen. De vraag is echter: 'Wat wil Microsoft van ons weten om Windows te kunnen verbeteren en wat is een bedreiging voor onze privacy?' Als je Microsoft mag geloven, is de gegevensverzameling vooral gericht op het verbeteren van Windows en de gebruikservaring. Voor meer informatie: lees de artikelen waarvan de links aan het eind van het artikel staan. Wil je, net als ik, (het liefst) volledige privacy, dan moet je in de hedendaagse maatschappij veel laten en veel missen. Wat je wil delen blijft een afweging tussen nut en noodzaak. Die afweging kan ik voor de lezer niet maken. Ik kan alleen wat handvatten geven ter afweging. We willen immers allemaal een beter Windows?
Van de grote vier: Apple, Facebook, Google en Microsoft, geven Apple en Microsoft je veel instellingsmogelijkheden om je privacy te beschermen. Juist die openheid en de instelmogelijkheden in Windows 10 ten aanzien van privacy lijken de argwaan richting Microsoft te versterken. Veel sentiment daarbij is, naar mijn mening, gebaseerd op onderbuikgevoel in plaats van feiten. De advertentienetwerken van Google en Facebook doen het in mijn ogen slechter, en Apple is in mijn ogen een moraalridder. Microsoft heeft het regelmatig met overheden aan de stok over het al dan niet verstrekken van informatie. Ik denk hierbij aan het inzicht geven in de gegevens van Europese burgers, opgeslagen op Ierse servers, aan de Amerikaanse overheid en aan de zaak van de Belgische overheid, die Skype (=Microsoft) aanklaagt na het weigeren van een tap. Vergeet ook niet dat Microsoft op eigen initiatief heeft verklaard 'Safe Harbor' te zullen naleven. Nu de Europese rechter de vloer heeft aangeveegd met 'Safe Harbor' is Microsoft gestart met het inrichten van een groot datacenter in Duitsland. Dat gebeurt onder toezicht van Deutsche Telekom.
Windows 10 biedt je de mogelijkheid om in te stellen wat je

wel en niet deelt met Microsoft. Blokkeer je alles, dan gaat dat ten koste van functionaliteit. Zet je alles open, dan levert je dat een persoonlijke secretaresse op die je leidt en waarschuwt, maar ook gepersonaliseerde reclame. Zelfs dat kan fijn zijn. Dan krijg je als man geen reclame meer over lingerie, damesgeurtjes en andere voor jou niet relevante zaken. Alleen zal dat rond Valentijnsdag van weinig invloed zijn … In dit artikel lopen we de privacy-instellingen van Windows 10 door en geef ik handvatten om zelf te bepalen wat je wel en wat je beter niet met Microsoft kunt delen.

1 Wat is er in te stellen?

Als basis neem ik de laatste Windows 10-versie (1511). Per relevant scherm een hoofdstuk met afwegingen voor het beschermen van je privacy in Windows 10 en soms gewoon een bot advies: uit of aan. Ik kijk vooral naar het nut van een instelling, wat krijg ik ervoor terug en wat kost mij dat aan informatie die ik met Microsoft deel. Oftewel: '*What's in it for Me*'. Elk plaatje toont mijn instellingen. De basisinstellingen vind je bij Instellingen (**Win+i**) > **Privacy**. Daar starten we gewoon van boven naar beneden.

1.1 Algemeen

Wanneer je geen gepersonaliseerde reclame wenst te gebruiken zet je het **reclame-id** uit. Het id kan door zowel het besturingssysteem als individuele apps worden gebruikt. Saillant detail is dat veel gebruikers niet weten dat hun browser vaak ook uniek te identificeren[1] is, zonder gebruikmaking van het reclame-id.

Het **SmartScreen-filter** laat ik aanstaan. Het draagt bij aan de veiligheid van het systeem doordat het, bij download of installatie, applicaties oormerkt als veilig of onbekend. Onbekend wil echter niet zeggen dat de applicatie onveilig is. Heb je de applicatie opgehaald bij een betrouwbare bron, dan kun je dat melden zodat de app, na controlemeldingen, uiteindelijk als veilig wordt gemeld bij de servers van Microsoft[2].

Bovenstaande melding komt binnen omdat ik KeePass wil downloaden van codecpack.nl. Dat is een uitvoering van KeePass waarin de NL-taalmodule al is geïnstalleerd. Door de integratie van het Nederlands is het minder bekend. Dat maakt het iets lastiger te downloaden via Edge. Eigenlijk was ik al overtuigd van de betrouwbaarheid van het programma, maar ter controle heb ik het aan virustotal.com voorgelegd en, zoals verwacht, is de download 100% veilig.

Omdat het SmartScreen filter aan Microsoft rapporteert over elke applicatie die op jouw systeem wordt uitgevoerd, kan het een privacy-probleem zijn wanneer het wordt gekoppeld met jouw persoonlijk profiel. Microsoft geeft echter aan dat er geen database is met programma's die zijn gelinkt aan specifieke gebruikers.

Wat Microsoft wil met de informatie die ik schrijf of typ weet ik niet. Denkelijk voor het inleren van Cortana en de voorspelling en correctie van typfouten. Wel weet ik dat ze mijn getyp voorlopig niet krijgen. Hetzelfde geldt voor de **taallijst**. Tenzij je natuurlijk Windows als secretaresse wenst.

Vergeet ook niet te klikken op de rood omrande link; die leidt je naar een Microsoftpagina waar je de privacy-instellingen betreffende je browsers kunt instellen. Open die pagina in elke door jou gebruikte browser.

1.2 Locatie/Camera/Microfoon

Op mijn desktop staan die uit. Op mijn telefoon en laptop heb ik de **locatieservices** meestal aan staan. Het is immers makkelijk om je locatie paraat te hebben wanneer je reist of het weerbericht wil hebben. Vaak zijn gebruikte applicaties daarvan afhankelijk om goed te kunnen functioneren. Het is wel juist deze instelling die veel van je gedragingen prijsgeeft. Gelukkig is ook op app-niveau in te geven welke app al dan niet gebruik mag maken van je locatiegegevens. In dit scherm heb je ook de mogelijkheid om je locatiegeschiedenis lokaal te wissen.

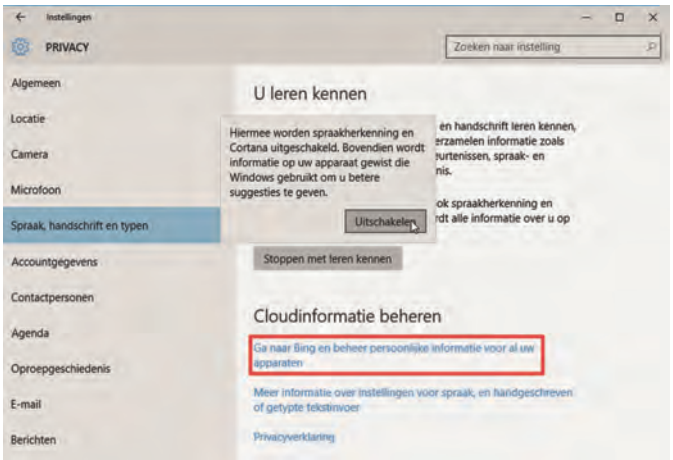
Toch de voordelen, en niet alles blijft bewaard! Jammer dat het alleen maar handmatig kan. Het zou fijn zijn wanneer je informatie 'ouder dan x dagen' automatisch zou kunnen wissen. Met *Geofencing* wordt een afgekaderd gebied bedoeld, zodat een app bijvoorbeeld 'weet' of je thuis of op je werk bent. Dit biedt vooral voordelen voor allerlei domotica en het automatiseren van zakelijke versus privéinstellingen. De instelling is per app te regelen.

Camera en **Microfoon** staan bij mij ook uit. Wanneer een app toegang wenst, vraagt die daarom en is het vroeg genoeg om de afweging te maken. Cortana benutten en Skypen zonder microfoon lijkt mij bijzonder lastig. Zonder camera lukt het evenwel prima totdat je elkaar iets wenst te laten zien. Overigens is het wijs om de camera sowieso af te schermen wanneer deze niet wordt gebruikt.

1.3 Spraak, Handschrift en Typen

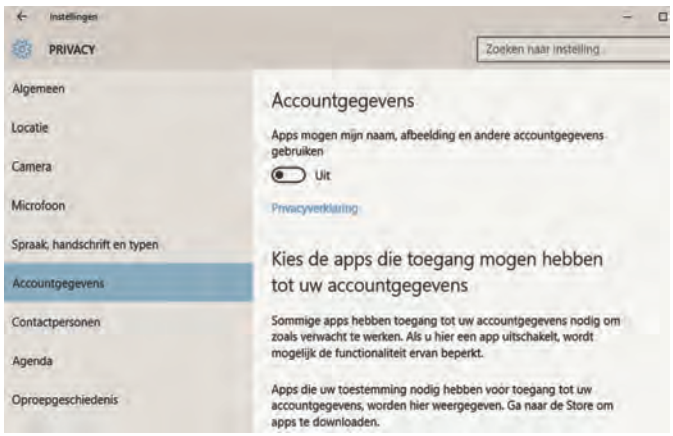
Dit is eigenlijk pas van toepassing zodra je Cortana wenst te gebruiken. Tot dan: *Uit!* Dat geef je aan door op de knop [**Stoppen met leren kennen**] te klikken.

Klik ook nog even op de roodomrande link om de persoonlijke informatie voor al je apparaten te wissen. Je ziet dat op de website onder de kop **Persoonlijke informatie wissen.**



1.4 Accountgegevens

Wil je apps toestaan in je accountgegevens te bladeren? Dat lijkt mij niet. Laten de apps eerst maar aangeven wat ze willen, dan kan eventueel op app-niveau toestemming worden gegeven. En niet eerder. Bij mij staat er nog geen app die toestemming wenst. Waarom hiervoor op voorhand toestemming gegeven moet worden is mij een raadsel.



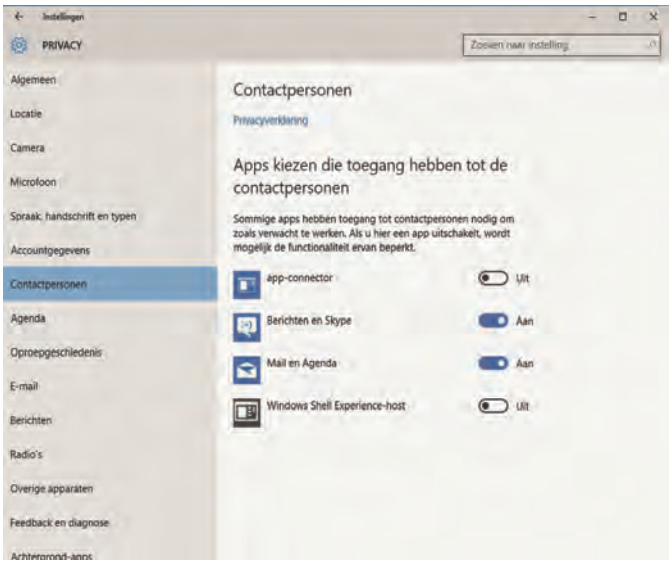
1.5 Contactgegevens/Agenda en Oproepgeschiedenis

Aangeven welke apps toegang mogen tot al deze gegevens? Alleen wanneer het meerwaarde heeft. Mocht je Skype wensen te gebruiken, dan is het wel zo handig dat Skype toegang heeft tot je Contactpersonen. Het is niet makkelijk om uit je contactgegevens een telefoonnummer of e-mailadres over te tikken (knippen/plakken) om dan met Skype contact te gaan zoeken. Tussen de toegang vragende apps, staat altijd de app 'app-connector'. Hierover vind ik alleen verwarrende informatie. Het zou gegevens naar MS-partners zenden voor reclamedoeleinden (paranoïdeverklaring). Een andere, meer plausibele verklaring is, dat het een soort tussenpersoon is die andere apps op een uniforme wijze toegang tot gegevens biedt en dan vooral toegespitst op Internet of Things (IoT). Met IoT worden alledaagse apparaten bedoeld die, voorzien van sensors, verbonden zijn met het internet, zoals slimme thermostaten, schakelaars en detectoren. Er zijn ook meldingen dat Skype zonder app-connector geen toegang heeft tot je camera. Wellicht is het alleen maar een laagje tussen de hardware en de toepassing. Voorlopig laat ik de app-connector uit.

Naast de app-connector is er vaak nog een mysterieuze app te vinden, de Windows Shell Experience-host. Deze app zorgt voor integratie tussen de nieuwe Universal apps en de Windows-schil (met name de Taakbalk).

Het voorziet in een uniforme wijze van interactie tussen de app en de gebruikersinterface, opdat de maker van de app zich niet hoeft af te vragen hoe informatie wordt gepresenteerd op pc, tablet of smartphone. Waarom, Microsoft, is er zo weinig informatie te vinden over het doel van deze apps en de informatie die zij delen? Wees duidelijk!

Oproepgeschiedenis toont met wie en wanneer er telefonisch contact is geweest. Je kunt hier vastleggen welke app dat mag inzien. Welke apps dat zijn hangt af van de maker. Ik verwacht dat universal apps zoals Skype in dit overzicht staan.



1.6 E-mail/Berichten/Radio's

Eigenlijk spreken deze categorieën voor zich. E-mail staat bij mij aan. De andere twee op uit. Gebruik je bijvoorbeeld Skype om berichten te verzenden, dan zet je het aan. En Radio's staat voor apps die radiosignalen gebruiken om data uit te wisselen zoals Bluetooth, wifi en NFC. Mogen apps die in- of uitschakelen, geef dat dan aan.

1.7 Overige apparaten

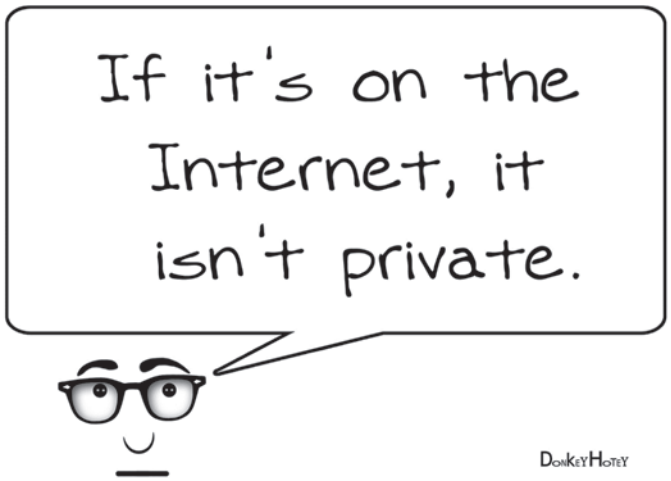
Hier is in te stellen welke apps met welke apparaten mogen communiceren, ook toekomstige! Ook hier naar eigen inzicht handelen. Rhino ziet alleen smartphones die aan de pc hangen of gehangen hebben en toegang tot de app Telefoonassistent voor het uitwisselen van data waaronder foto's, video's en muziek.

1.8 Feedback en Diagnose

Wil je meewerken om Windows 10 beter te maken, dan laat je dit staan zoals het staat. Er wordt geanonimiseerde data met Microsoft uitgewisseld over het functioneren van Windows.

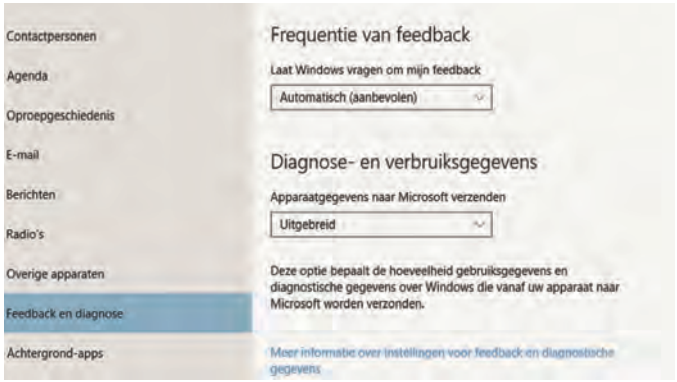
Feedback
Wanneer dit aanstaat zal Microsoft je, via het actiecentrum, om Feedback vragen over functies die je gebruikt. De vraag wordt over het algemeen gesteld wanneer er iets vreemds op je pc gebeurt. Wil je Microsoft maximaal helpen, dan zet je dit op Automatisch. Automatisch wil zeggen dat er om je mening wordt gevraagd je op basis van een gebeurtenis op je pc. Die gebeurtenis is de trigger voor de feedback. Wil je niets delen of vind je het vervelend, dan zet je het uit. Ook kun je aangeven niet vaker dan eens per dag of week lastig gevallen te worden. Zet je dit net als ik uit, dan kun je toch feedback geven door de app Windows Feedback te starten.

Diagnose
Dit zijn gegevens die Microsoft wil verzamelen over de werking van Windows. Het is een monitorsysteem.
Basis is voldoende om Microsoft te laten weten hoe de essentiële functies van Windows werken. Er wordt beperkte informatie over fouten gedeeld. Wil je zelfs dit niet en ga je via het register of andere software aan de slag om dit uit te zetten, dan moet je beseffen dat er ook geen updates kunnen worden geleverd om Windows veilig en up-to-date te houden.



Zelf heb ik gekozen voor **Uitgebreid**. Dat omvat alle basisgegevens en daarnaast de wijze waarop je Windows en Microsoft-apps gebruikt.

Er worden zonodig uitgebreide foutrapportages verzonden. Naar mijn idee is dit de optie waarbij je zo min mogelijk van jezelf prijsgeeft en Microsoft en jezelf helpt het product te verbeteren en fouten op te lossen. Merk op dat, buiten veiligheidsproblemen, de problemen die het meest worden gemeld, het eerst worden aangepakt.
De optie **Volledig** geeft Microsoft het meeste inzicht in het gebruik van je systeem. Microsoft geeft aan dat het volledig anoniem is. Of je die uitspraak kan vertrouwen; ik kan je daarin niet raden. Wel denk ik dat Microsoft veel te verliezen heeft wanneer het ons vertrouwen zou beschamen.



1.9 Achtergrond-apps

Je geeft aan welke apps op de achtergrond actief mogen zijn. Los van het feit of apps je privacy mogelijk schenden, is het ook van belang om op apparaten die van een accu afhankelijk zijn het uitvoeren op de achtergrond te minimaliseren. De Store moet actief blijven om andere apps automatisch bij te werken.

2 Tot slot

De voornaamste zorg rond de privacy van de Windows 10-gebruiker richt zich op Cortana, de spraakassistent die in de Nederlandstalige Windows nog niet actief is. Cortana registreert alles wat je doet en zegt om je van dienst te kunnen zijn. Net als een goede secretaresse op de hoogte is van je (eigen)aardigheden, zal Cortana dat ook proberen te zijn. Feitelijk werkt het als een permanente luistervink met als doel je te dienen.

Er is een groot aantal tooltjes in omloop, zoals SHUTUP10, die aangeven je privacy onder Windows 10 goed te kunnen instellen. Naast de vraag of die tools zelf te vertrouwen zijn, zijn deze programma's zo ondoorzichtig en paranoïde in hun instellingen, dat je jezelf dient af te vragen of je zo rigoureus te werk moet gaan en je pc moet toevertrouwen aan dit soort dubieuze programma's. Bovendien zijn ze in het Engels en is de uitleg zó summier, dat moeilijk is te duiden wat de consequentie van een instelling is. Bovendien ben ik wars van hulpprogramma's wanneer het resultaat ook bereikt kan worden met Windows' eigen middelen zonder in het register te hoeven duiken.

Links:

1 Browser identificeren	http://bit.ly/r-potc
2 SmartScreen filter	http://bit.ly/r-ssf
MS Privacy Statement	http://bit.ly/r-msprivacy
MS Ierland vs USA	http://bit.ly/r-vs-ierl en
	http://bit.ly/r-vs-ierl2
Dataverzamelen Windows 10 geen privacyrisico	http://bit.ly/r-ms-datacol
Feedback en Diagnose FAQ	http://bit.ly/r-fb-diag
Apple weigert iMessage-data	http://bit.ly/r-iMess
Bits of Freedom - privacystorm	http://bit.ly/r-bof-priv