STRATEGIEËN OM JE PRIVACY TE BESCHERMEN

De meeste apps en digitale diensten die we dagelijks gebruiken, verzamelen persoonlijke gegevens over ons. Met die gegevens maken deze bedrijven een omvattend profiel van ons op.

In het geval een bedrijf gehackt wordt of het niet nauw neemt met de privacyregels kan het gebeuren dat in één klap al deze persoonlijke data openbaar beschikbaar zijn.

Één van de manieren om ervoor te zorgen dat in het geval van een datalek 'slechts' een deel van je data openbaar wordt gemaakt, is door gebruik te maken van alternatieve toepassingen en diensten.

In deze brAInfood geven we je tips om je gegevens beter te beveiligen tegen allesomvattende *surveillance* door bedrijven of overheden en/of het openbaar beschikbaar worden van al jouw data door één enkel datalek.

Kenniscentrum Data & Maatschappij (2021). Strategieën om je privacy te beschermen. brAInfood van het Kenniscentrum Data & Maatschappij. Brussel: Kenniscentrum Data & Maatschappij.

1. Leg niet al je eieren in één mand.

Grote technologiebedrijven bieden vaak voor elke dienst die je je maar kan inbeelden een app aan: e-mail, (online) presentatie en tekstverwerking, (navigatie)kaarten, foto-opslag... Vaak zijn deze **diensten met elkaar verbonden** zodat je er makkelijk tussen kan schakelen en gegevens kan delen. Hoewel dit handig is voor de gebruiker, is het voor deze bedrijven ook een manier om de data die ze over je verzamelen te diversifiëren. Op deze manier kunnen ze een heel **gedetailleerd profiel van je opmaken**.

Dit altijd up-to-date profiel kan voor bedrijven handig zijn om **gerichter te adverteren**. Het kan ook gebruikt worden als middel om **bevolkingsgroepen te volgen** en **(sociale) controle uit te oefenen** op burgers. Op verschillende plaatsen in de wereld delen bedrijven, al dan niet verplicht, de data die ze verzamelen met hun overheden en inlichtingendiensten. Bovendien, als een hacker toeslaat bij het bedrijf waar je je profiel bij hebt, kan alle data in je profiel ook voor cybercriminelen toegankelijk worden.

Een manier om ervoor te zorgen dat één bedrijf niet de mogelijkheid heeft om een totaalprofiel van je op te stellen is door **apps en diensten van verschillende bedrijven te gebruiken voor verschillende functies** (bijv. e-mail via Outlook, cloudopslag via Google,...). Kortom, om je persoonlijke privacy beter te beschermen: leg al je 'data-eieren' niet in één 'bedrijfsmand'.

2. Wees je bewust van de ommuurde tuin.

Door verschillende diensten aan te bieden verdwijnt de noodzaak om voor elke dienst een aparte account aan te maken bij verschillende bedrijven. Op deze manier kan het bedrijf uit de data van de ene dienst gepaste aanbevelingen maken in een andere dienst, wat heel handig kan zijn. Zo kan bijvoorbeeld het adres van een afspraak in je agenda automatisch worden geïmporteerd in de navigatiesoftware van hetzelfde bedrijf.

Deze bedrijven weten dat dit een significante meerwaarde kan zijn voor de gebruiker. Ze zullen daarom niet snel data die ze over je hebben in een toegankelijk bestandsformaat beschikbaar maken. Zo is het moeilijk voor andere bedrijven om die info op eenzelfde manier te integreren in hun software. Bedrijven vergroten je **gebruiksgemak** door een grote diversiteit van data te integreren en vergroten zo de kans dat je de verschillende diensten van één bedrijf blijft gebruiken. Maar tegelijkertijd verhogen ze het risico dat in het geval van een **datalek**, al deze persoonlijke informatie in één keer openbaar kan worden gemaakt.

3. Doe je eigen onderzoek.

Als je ervoor kiest om apps of diensten van een bepaalde aanbieder te gebruiken, loont het de moeite om de **data- en privacypraktijken van het bedrijf** te bekijken. Deze documenten zijn vaak zeer uitgebreid en bevatten veel juridische termen die niet voor iedereen even toegankelijk zijn. Ook zijn de teksten vaak op een misleidende manier opgesteld, waardoor ze door het verbloemen van de waarheid vertrouwen wekken.

Een andere manier om zelf onderzoek te doen is door te zoeken naar de naam van het bedrijf of de dienst gevolgd door termen als "hacked", "privacy" of "data-protection". Op deze manier kan je meer te weten komen over problemen of lof rond data- en privacypraktijken van het bedrijf. Dit is natuurlijk geen waterdichte oplossing. Zoals bij alles wat je leest op het internet: **blijf kritisch**.

Nog enkele algemene tips & tricks:

1. Gebruik indien mogelijk apps die **open-source** zijn i.p.v. apps waarvan de broncode geheim is. In open-source software is de broncode openbaar toegankelijk. Dit geeft mensen (o.a. gebruikers, beveiligings- en privacy-experten) de mogelijkheid om de werking van de app te controleren en na te gaan of de app veilig en privacyvriendelijk is of niet.
2. Niet alles hoeft digitaal te zijn. Je kan je privacy ook beschermen door bepaalde functionaliteiten **analoog** te houden.
3. Zorg voor je eigen privacy by default: de Algemene Verordening Gegevensbescherming (AVG) verplicht verwerkingsverantwoordelijken om hun processen zo te organiseren dat de meest privacyvriendelijke opties van in het begin worden ingesteld. Dit is niet altijd het geval. Wil je niet dat bepaalde gegevens verwerkt worden, raadpleeg zeker de **privacy-instellingen** van de dienst en zet, indien mogelijk, deze gegevensverwerking uit.
4. Gebruik **niet overal dezelfde identiteit**. Veel apps of diensten maken gebruik van 'inloggen met je Google/Facebook-account', waardoor je met één klik een account kan aanmaken en kan inloggen. Zo geef je (impliciet) de toestemming voor het uitwisselen van je data tussen het bedrijf waar je je registreert en Google/Facebook. Zo kunnen beide bedrijven gebruik maken van je data. Als je een account aanmaakt met je e-mailadres, kan je dit (in veel gevallen in bepaalde mate) voorkomen.

brAInfood van het
Kenniscentrum Data
& Maatschappij