

HOE STA JIJ TEGENOVER

SLIMME TECHNOLOGIEËN IN JE HUIS ?

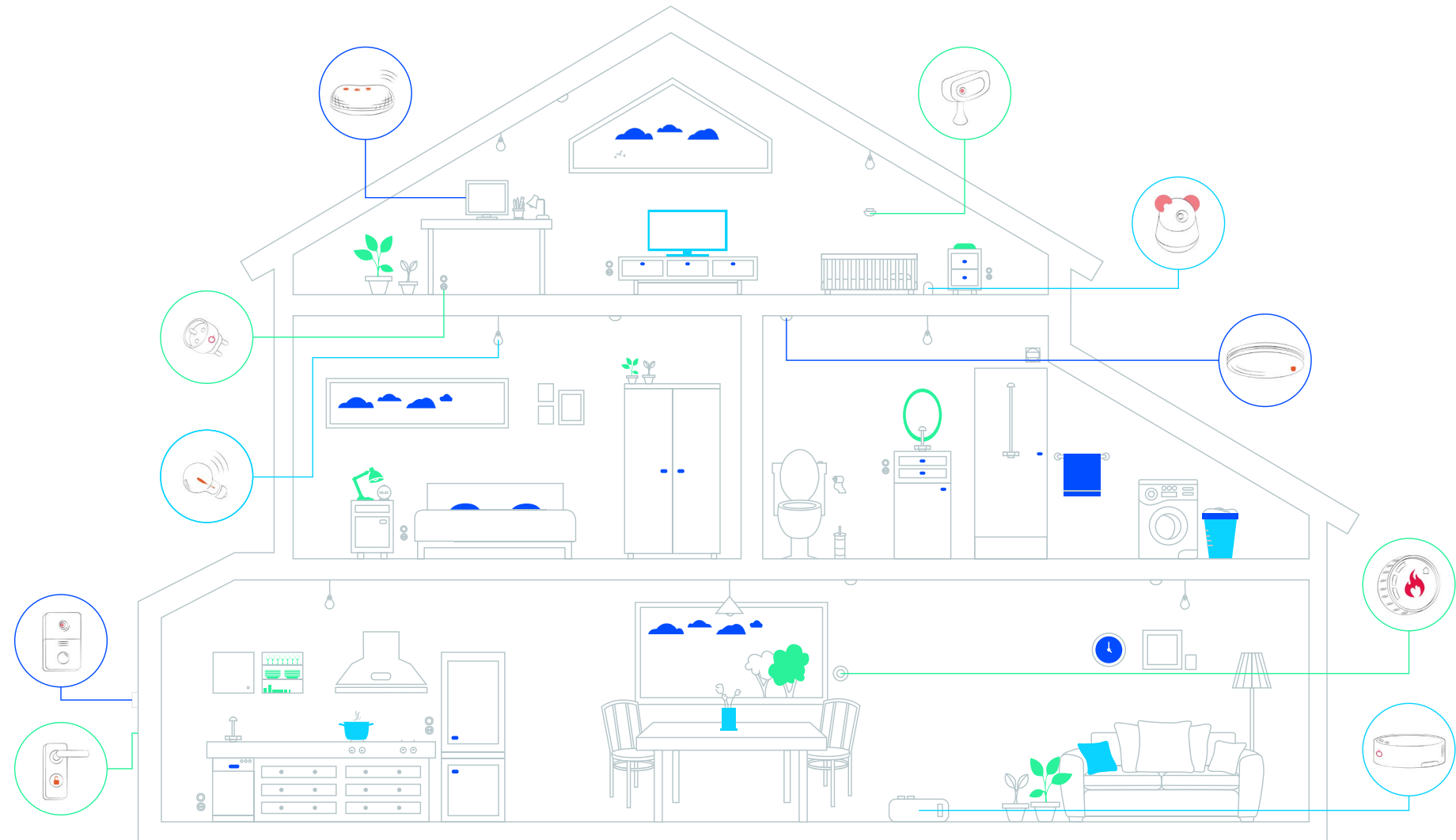
Smarthometechnologieën zijn talrijk aanwezig in onze huishoudens. Hoe werken deze technologieën juist, hoe gaan ze om met jouw data en wat betekent dat voor jouw privacy? Ontdek het in deze brAinfood, ontwikkeld door het Kenniscentrum Data & Maatschappij onder leiding van de onderzoeksgroep imec-MICT-UGent.

Wil je meer weten over smarthometechnologie, en hoe Vlamingen hier tegenover staan? Lees dan [deze studie](#) van het Kenniscentrum Data & Maatschappij, onder leiding van imec-MICT-UGent (publicatiedatum: februari 2023).



Kenniscentrum Data & Maatschappij (2023). Hoe sta jij tegenover slimme technologieën in je huis? Brussel: Kenniscentrum Data & Maatschappij.

Deze brAinfood is beschikbaar onder een CC by 4.0 licentie.



WAT IS SMARTHOMETECHNOLOGIE?

Smarthometechnologie maakt bepaalde aspecten van jouw huis 'slim'. De technologie zit in wat we smarthometoestellen noemen, zoals robotstofzuigers, slimme camera's, deurbellen en luidsprekers.

Smarthometoestellen zijn vaak verbonden met het internet en kunnen hierdoor met elkaar communiceren. Een smarthometoestel is slim doordat het informatie uit de omgeving kan verzamelen en daarop kan reageren. Zo kan een slimme luidspreker door de toevoeging van een spraakassistent zoals Siri of Google Assistant, reageren op de commando's van de gebruiker. Of slimme verwarming schakelt zichzelf uit wanneer er geen mensen aanwezig zijn in de woning.

Iets meer dan de helft van de Vlamingen bezit één of meerdere smarthometoestellen. Over de laatste jaren is dit aantal steeds gegroeid.

SMARTHOMETECHNOLOGIE & SURVEILLANCE

Smarthometoestellen kunnen heel wat informatie over ons verzamelen binnen onze thuiscontext, iets wat velen als een private omgeving beschouwen. We kunnen op twee niveaus kijken naar de privacy van smarthometoestellen, zoals naar de

1. **hoeveelheid en soorten data** die deze slimme toestellen over ons verzamelen en delen met private bedrijven. Ook de beveiliging van de toestellen is hierbij van belang. Een smarthometoestel dat gehackt wordt, kan ongewenst informatie over gebruikers en hun huishouden vrijgeven, of
2. we kunnen deze toestellen zelf inzetten om **informatie over onze gezinsleden of huisgenoten** te verzamelen binnen ons huishouden.

1. JOUW DATA IS ONZE DATA

Bij het gebruik van smarthometoestellen worden data uitgewisseld tussen het toestel en de producent ervan. Inzichten die uit deze data voortvloeien, worden door de producent bijvoorbeeld gebruikt om productverbeteringen door te voeren. Afhankelijk van de beschikbare en gekozen privacyinstellingen worden deze data verzameld, verwerkt en zelfs verkocht. Voor welke doeleinden jouw data gebruikt worden en met welke partners deze precies worden gedeeld, is vaak niet eenvoudig te achterhalen. Naarmate deze dataprocessen intensiever en obscuurder worden, vinden gebruikers dit steeds minder gepast.

Smarthometoestellen zijn over het algemeen ook minder goed beveiligd dan ze lijken. Om de aankoopprijs laag te houden, gebruiken ze minder geavanceerde computerchips en/of is er een beperkte software-ondersteuning voor bijvoorbeeld het doorvoeren van beveiligingsupdates. Ook worden deze toestellen in de meeste gevallen geleverd met standaard wachtwoorden die niet altijd door de gebruiker veranderd worden in sterke wachtwoorden. Dit maakt dat smarthometoestellen vaak een relatief gemakkelijk toegangspunt zijn voor hackers om binnen te dringen in jouw netwerk en om zo mogelijks persoonlijke gegevens te stelen en te misbruiken.

2. EEN OOGJE IN HET ZEIL HOUDEN

Smarthometoestellen zoals slimme (beveiligings)camera's die binnen- en buitenshuis personen en objecten kunnen herkennen, een slimme deurbel die je toelaat om via je smartphone te kijken wie er voor de deur staat of een smart speaker die je handsfree kan bedienen, bieden verschillende mogelijkheden om (op afstand) een oogje in het zeil te houden. Deze producten hebben vaak ook bijkomende gebruiksmogelijkheden. Zo geeft een slimme deurbel gemakkelijk zicht op het tijdstip waarop gezinsleden of huisgenoten thuiskomen.

Ouders die smarthometechnologie gebruiken om gezinsleden in de gaten te houden, doen dit vaak met goede bedoelingen. Ondanks dat er bij ouderlijk toezicht via technologie gemakkelijk aan nieuwsgierigheid of wantrouwen gedacht wordt, zijn dit niet per se de belangrijkste drijfveren voor ouders. Vele ouders willen hun kinderen bijvoorbeeld beschermen tegen anderen met slechte intenties of willen zicht hebben op de activiteiten van hun kinderen. Zij zien het inzetten van smarthometechnologie dan ook als een hulpmiddel in het hedendaags ouderschap. Een voorbeeld kan zijn dat ouders via een slimme deurbel op afstand zien wanneer hun kinderen thuiskomen, maar ook aanwijzingen geven in het geval er iemand aanbelt terwijl zij zelf niet thuis zijn.

PRIVACY, TOEZICHT & DIALOOG

Vele gebruikers van smarthometoestellen geven aan dat ze privacy belangrijk vinden, maar niet voldoende op de hoogte zijn van welke data er nu juist verzameld, verwerkt en verkocht worden. Wel geven deze gebruikers aan nood te hebben aan een transparante en duidelijke manier om zichzelf te informeren over het (data)gebruik van hun smarthometoestel(len).

Gebruikers willen graag meer controle over het instellen van hun eigen (privacy-) wensen. Hiernaast gebruikt vandaag maar een minderheid van de ouders in Vlaanderen smarthometechnologie om een oogje in het zeil te houden.

Onderzoek toont aan dat er in Vlaanderen onder ouders een redelijk grote intentie is om smarthometechnologie te gebruiken om toe te zien op hun kinderen. In combinatie met de groeiende adoptie van smarthometechnologie in Vlaanderen, is het belangrijk om na te denken over de impact dat dit gebruik van smarthometechnologie op kinderen kan hebben. Het is daarom raadzaam om in samenspraak met kinderen goede afspraken te maken rond het gebruik van deze functionaliteiten.