

Achter de Schermen

S.R.W. van Kampen en R.A.J. Wacanno

11 mei 2019

1 Introductie

In onze infographic valt te zien wat er gebeurt met de data die *Facebook* vergaart. De toepassingen variëren, van het personaliseren van advertenties tot het beïnvloeden van verkiezingen. Zijn consumenten zich bewust van welke data *Facebook* van ze bijhoudt? En zo niet, kan dit bewustzijn (blijvend) verbeterd worden?

2 Zijn consumenten bewust van privacy-normen?

Allereerst de vraag: zijn consumenten zich bewust van welke data *Facebook* vergaart en verwerkt?

In sommige gevallen valt te verwachten dat consumenten zich bewust zijn van de datavergaring. Dit hangt onder andere af van de context waarin iets geplaatst wordt, iets wat Nissenbaum (2004) ook aanstipt als een cruciaal onderdeel van informatiedeling. Als je op *Facebook* een bericht op je tijdlijn plaatst over hoe erg je van katten houdt, is het redelijk logisch dat *Facebook* dat dan ook weet. Een bericht op de tijdlijn valt gevoelsmatig te vergelijken met een aankondiging, en daarvan verwacht men over het algemeen weinig privacy.

In het geval van het analyseren van privéberichten die via *Facebook Messenger* zijn gestuurd, zoals in Frier (2018) wordt onthuld, is de context heel anders. De *interface* van Facebook suggereert ook dat je hier deelneemt aan een een-op-een gesprek, waardoor gebruikers misschien niet verwachten dat Facebook op de achtergrond meeluistert.

Bij het *scrapen* van *Facebook*-profielen is vooral de koppeling van data een praktijk waar gebruikers over het algemeen niet bij stilstaan. Zoals beschreven in Madrigal (2018) worden e-mailadressen en telefoonnummers, waaraan vaak geen identiteit is gekoppeld, in grote getale verzameld door louche internettypes die hiermee vervolgens volledige profielen op *Facebook* kunnen bekijken. Als gebruiker weet je natuurlijk dat je profiel voor anderen zichtbaar is, maar je gaat er van uit dat iemand deze dan wel met jouw naam moet vinden, waar uit volgt dat deze persoon jou moet kennen. Ook gaan gebruikers er bij het invullen van je e-mailadres op een andere website niet van uit dat hiermee ongemerkt een koppeling gemaakt zou kunnen worden met data op hun *Facebook*-profiel.

In het geval van *tracking*-pixels, zoals beschreven in Schellevis and de Jong (2018), valt eigenlijk niet te verwachten dat consumenten zich er bewust van zijn. Aangezien de *tracking*-pixels onzichtbaar zijn en niet makkelijk te detecteren zonder *browser*-extensies of enige kennis van de *developer console*, is het gebruik ervan niet inzichtelijk voor de doorsnee gebruiker. Op platforms waarbij deze hulpmiddelen niet beschikbaar zijn, zoals veel van de mobiele browsers, is een *tracking*-pixel nog minder makkelijk te detecteren. Bij gebrek aan deze detectie is het moeilijk je bewust te zijn van de mogelijke datacollectie zonder paranoïde te worden: in Schellevis and de Jong (2018) gaat het om websites van zorgverzekeraars, dus de verwachting baseren op b.v. de gevoeligheid van het bezoeken van de site gaat niet op.

De casus *Cambridge Analytica*, zoals beschreven in Graham-Harrison and Cadwalladr (2018), is een gemengd geval. De *Facebook*-gebruikers die de data-verzamelande applicatie gebruikten hadden kunnen weten dat hun gegevens ten prooi vielen. De vrienden van deze gebruikers, wiens data ook verzameld werd, hadden hier echter geen weet van. Gezien het ontwerp van deze constructie zou het van deze vrienden ook niet verwacht kunnen worden dat zijn van deze praktijk op de hoogte waren.

3 Verbetering van het bewustzijn

Om het bewustzijn van mensen te verbeteren is het belangrijk om duidelijk kenbaar te maken wat met de data die mensen verstrekken gebeurt - een cyber-equivalent van de notie van *informed consent* in de medische wereld.

Dit verschilt op meerdere manieren met de wijze waarop men nu geïnformeerd wordt over datavergaring. Ten eerste hebben sites als Facebook wel pagina's waar ze hun gegevensbeleid uit de doeken doen, maar men kan zich gemakkelijk voor diensten als Facebook aanmelden zonder ook maar één blik te werpen op dit beleid.

Als we kijken naar softwarelicenties, waarbij het gebruikelijk is de licentietekst in een installatieprogramma weer te geven en om toestemming van de gebruiker te vragen, zien we dat die methode ook niet ideaal is. Zoals beschreven is in Van Kampen (2019) worden deze doorgaans ook niet door gebruikers gelezen, mede wegens de lengte en complexiteit. Het gegevensbeleid moet dus niet alleen weergegeven worden, maar ook behapbaar zijn voor de doorsnee persoon. Hierbij kan ook prominent gelinkt worden naar de stukken waarvan verwacht wordt dat ze minder vanzelfsprekend zijn, om de tijdsinvestering te minimaliseren en zo de hoeveelheid mensen die het beleid lezen te verhogen.

4 Zorgen voor een blijvend bewustzijn

Bij dit soort onderwerpen geldt vaak het devies: "*Out of sight, out of mind.*" Het is daarom belangrijk om in het geval van dataverzameling en -deling, de gebruiker op de juiste momenten aan deze praktijken te herinneren. In het

geval van het lezen van de berichten die men stuurt via *Messenger* zou er bijvoorbeeld om de zo veel tijd een melding kunnen worden weergegeven die de gebruiker verteld dat de gestuurde berichten voor bepaalde doeleinden door *Facebook* worden gelezen. Ook zou er daar waar men persoonlijke gegevens invoert en bewerkt duidelijk kunnen worden gemeld of dit publiek op het profiel vermeld gaat worden of niet. Hier is op dit moment vaak een losse privacy-pagina voor waar mensen niet vaak op kijken. Deze manier van duidelijk informeren wordt ondersteund door Nissenbaum (2004).

Referenties

- Frier, S. (2018). Revealed: Facebook scans what you send other people on messenger.
- Graham-Harrison, E. and Cadwalladr, C. (2018). Revealed: 50 million facebook profiles harvested for cambridge analytica in major data breach.
- Madrigal, A. C. (2018). 'most' people on facebook may have had their accounts scraped.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*.
- Schellevis, J. and de Jong, W. (2018). Verzekeraars sturen surfgedrag naar facebook, ook van medische pagina's.
- Van Kampen, S. (2019). Weekopdracht 1: EULA's.