RIJKSUNIVERSITEIT GRONINGEN

Privacystatements van zoekmachinebedrijven onder de loep

BACHELORSCRIPTIE
COMMUNICATIE- & INFORMATIEWETENSCHAPPEN

Wessel Poelman

(S2976129)

Begeleider:

dr. Wim Vuijk

16 januari 2020

SAMENVATTING

In dit onderzoek is gekeken naar privacystatements van zoekmachinebedrijven. Online privacy is een breed en relatief nieuw gebied waar steeds meer maatschappelijke aandacht voor is. Het bekijken van statements van zoekmachinebedrijven is een goed startpunt om hier meer grip op te krijgen; er kan buitengewoon veel afgeleid worden uit zoekopdrachten en dat maakt de statements van deze groep bedrijven extra interessant, als het gaat om hun communicatie daarover.

In het onderzoek is gekeken naar de statements vanuit een puur tekstueel oogpunt. Aan de hand van twee onderzoeksvragen zijn de statements getypeerd: *Wat staat er in de privacystatements van zoekmachinebedrijven?* en *Hoe verwoorden zoekmachinebedrijven de onderwerpen die aan bod komen in hun privacystatements?* Uit de analyses blijkt, onder andere, dat er veel verschillen zijn tussen de statements op verschillende vlakken: vorm, onderwerpen die aan bod komen, lengte, de manier van de onderwerpen verwoorden en de manier waarop het bedrijf zich in de tekst verhoudt tot online privacy. Dit is opvallend omdat de bedrijven in principe exact dezelfde soort dienst aanbieden.

Als vervolg op de *wat* en *hoe* vragen en om een *theory* te formuleren is een derde onderzoeksvraag opgesteld: *Hoe kan een privacystatement voor zoekmachinebedrijven eruit zien volgens experts?* Deze vraag is beantwoord in twee stappen; eerst is vakliteratuur over hoe bedrijven kunnen omgaan met online privacy vergeleken. Op basis hiervan is een *theory* geformuleerd in de vorm van 'aanbevelingen voor een goed privacystatement'. Deze aanbevelingen zijn vervolgens voorgelegd aan universitair hoofddocent IT-recht prof. dr. J. H. Hoepman, samen met algemenere vragen over privacystatements. De uitkomsten van dit interview zijn meegenomen in de aanbevelingen en ten slotte is deze *theory* toegepast op de bestaande statements. Het antwoord op de derde onderzoeksvraag zijn de uiteindelijke aanbevelingen:

Aanbevelingen voor onderwerpen die aan bod zouden kunnen komen in een privacystatements: 1. Hoe staat het bedrijf tegenover online privacy. 2. Welke data worden verzameld. 3. Hoe worden de data verzameld. 4. Waarom worden de data verzameld. 5. Waar worden de data voor gebruikt. 6. Wat is de impact van hetgeen waarvoor de data gebruikt worden op het bedrijf zelf en op de gebruikers.

Aanbevelingen voor hoe de onderwerpen verwoord zouden kunnen worden in een privacystatements: 1 Gebruik formuleringen en argumenten die de *relaties* met de *stakeholders* (gebruikers) bevorderen. 2. Bij het benaderen van de onderwerpen, houd rekening met het *vertrouwen* van de gebruikers in het bedrijf. 3. Toon *begrip & respect* voor de mogelijke zorgen van de gebruikers over online privacy. 4. Schets een beeld voor de *stakeholders* van hoe het bedrijf omgaat met online privacy in een *maatschappelijke setting*, dus breder dan de dienst zelf.

Naast de aanbevelingen en grote verschillen tussen de statements, laten de resultaten zien dat 'online privacy' een zeer breed veld is wat op veel verschillende gebieden doorwerkt.

INHOUDSOPGAVE

1 INLEIDING

> Steeds meer apparaten en diensten verzamelen persoonsgegevens waardoor ze steeds meer van ons weten.
>
> Dit gebeurt zonder dat we altijd precies weten wat er met die gegevens gebeurt en wie er toegang toe heeft. - *Autoriteit Persoonsgegevens*

1.1 ONDERWERP

Een internetzoekmachine is als een baliemedewerker in een lobby voor groot, onbekend en complex gebouw; als bezoeker (gebruiker) ben je op zoek naar iets, een bepaalde afdeling, een specifieke kamer van iemand, een bedrijf of een kantoor. Uiteraard is even vragen aan de balie de beste en makkelijkste manier om zo efficiënt mogelijk op je locatie te komen. Wat nou als de baliemedewerker jouw vraag en het antwoord daarop onthoudt voor een volgende keer? Je hoeft alleen maar een suggestie te doen en het oude antwoord of een soortgelijk antwoord komt direct naar voren. Aan de ene kant zorgt dit onthouden voor gemak, aan de andere kant is het de vraag of je als bezoeker (gebruiker) dit wel wilt. Wat als een gedeelte van het gebouw een zorginstelling is en de baliemedewerker na het zoveelste bezoek bijna zeker weet dat jij of iemand in jouw omgeving een beschamende kwaal heeft? Of dat een gedeelte van het gebouw een kantoor is van een politieke of religieuze organisatie? Of dat er 'relevante' advertentieposters worden opgehangen in de lobby voor de locaties waar jij bent geweest? Niet alle bezoekers zouden het prettig vinden als de baliemedewerker deze informatie van ze weet en gebruikt. Daarnaast is het de vraag wat er zou gebeuren als er een overval gepleegd wordt op de balie, wie heeft dan al die gevoelige informatie in handen? We kunnen niet verwachten dat iedereen die bij de balie komt een kijkje achter de schermen krijgt om te zien hoe hiermee wordt omgaan. We kunnen het vragen of de balie kan een flyer of document hebben waarin ze zeggen hoe ze dit aanpakken.

Dat laatste punt is het onderwerp van deze scriptie. Hoe zeggen zoekmachinebedrijven hoe ze omgaan met persoonlijk data? Hoe zien de 'privacystatements' van deze bedrijven eruit? De term 'privacystatements' is hier bewust gekozen. Het corpus voor dit onderzoek bestaat uit uitingen van zoekmachinebedrijven over hoe zij omgaan met gebruiksdata. Deze uitingen hebben vaak titels als: *About*, *Over ons*, *Privacyverklaring*, *Privacystatement* of *Privacy Policy*. Deze termen kunnen verwarrend zijn en daarom wordt gewerkt met de term 'privacystatements', in het kader van leesbaarheid, maar ook omdat bedrijven de eerdergenoemde termen inwisselbaar gebruiken om ongeveer hetzelfde te beschrijven. 'Privacystatements' is voor dit onderzoek de meest toepasbare term; een 'Privacy Policy' is een *juridisch* document over het omgaan met gebruikersdata en privacy. Een 'About' of 'Over ons' pagina gaat niet per definitie over privacy, maar vaak over het bedrijf zelf[1]. De term 'privacystatement' wordt gebruikt voor het omschrijven van een 'leesbaar' document over privacy; oftewel een document waar de eindgebruiker praktisch gezien iets mee kan en waar hij of zij geen juridisch

[1] Dit kan soms overlappen, zoals we verderop zullen zien.

kennis voor nodig heeft [2]. De betekenis en uitleg van 'privacystatement' die wordt aangehouden in dit onderzoek, is die van de Autoriteit Persoonsgegevens die, in het kader van *recht op informatie*, het als volgt omschrijft:

> Organisaties geven deze informatie [omgang met gebruikersdata & privacy] vaak via een online privacyverklaring (privacystatement). Die verklaring mag niet te lang en niet ingewikkeld zijn. Het moet voor u makkelijk te begrijpen zijn wat de organisatie met uw persoonsgegevens doet. Zodat u kunt beslissen of u uw persoonsgegevens wel met die organisatie wilt delen.
>
> Kunt u de privacyverklaring niet goed vinden? Mist er informatie? Of is de verklaring te lang en ingewikkeld? Vraagt u zich dan af of u met die organisatie wel uw persoonsgegevens wilt delen. Wellicht zijn er andere organisaties die hetzelfde product of dezelfde dienst leveren en die wél transparant zijn. - *Autoriteit Persoonsgegevens* [3]

1.2 Afbakening

Privacystatements van zoekmachinebedrijven zijn slechts een klein onderdeel van het doorlopende, maatschappelijke probleem van online privacy. Wekelijks komen artikelen voorbij over persoonsgegevens die 'op straat' zijn gekomen door datalekken, nieuwe wetten rondom online privacy of het wel of niet inperken van internetgiganten zoals Amazon, Facebook of Google.

Zoekmachinebedrijven zijn uiteraard niet de enige bedrijven die omgaan met gevoelige data, maar ze zijn voor praktisch alle internetgebruikers de 'ingang' tot het internet (om de analogie van de lobby aan te houden). Praktisch *alles* wat iemand wil opzoeken op het internet gebeurt door middel van een zoekmachine. Dat zorgt ervoor dat veel (gevoelige) informatie door de zoekmachines *kan* worden opgeslagen en gebruikt *kan* worden voor allerlei doeleinden. Er kan ongelofelijk veel afgeleid worden uit zoekopdrachten[4] en dat maakt van zoekmachinebedrijven een geschikte groep om naar hun privacystatements te kijken.

Dit 'bekijken' van de statements kan vanuit verschillende onderzoeksgebieden en invalshoeken gedaan worden; denk aan een bedrijfskundige insteek waarbij gekeken kan worden naar de voor- en nadelen van het verzamelen van persoonsgegevens. Of naar management strategieën binnen een bedrijf die zorgen dat de privacy van gebruikers gewaarborgd wordt en hoe dit in een statement verwerkt kan worden. Marketing is een andere insteek waarbij bijvoorbeeld gekeken kan worden naar hoe persoonsgegevens ingezet kunnen worden voor marketingdoeleinden. Aan privacystatements zit ook een groot juridisch aspect, hoe zorgt een zoekmachinebedrijf ervoor dat het binnen de privacywetten van bepaalde landen of gebieden opereert en hoe wordt dit gecommuniceerd naar de gebruiker? Verder is het technische

[2] Dit onderscheid wordt ook gemaakt op Wikipedia: https://en.wikipedia.org/wiki/Privacy_policy

[3] https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/gebruik-uw-privacyrechten/recht-op-informatie

[4] Een interactief voorbeeld hiervan is Google Trends https://trends.google.nl/trends/ waarin alle zoekopdrachten die Google verwerkt inzichtelijk gemaakt worden.

aspect van een zoekmachine ook een voor de hand liggende invalshoek, kan of moet een privacystatement gebruikt worden om gebruikers uit te leggen hoe de zoekmachine van binnen werkt en hoe privacy hierin een rol speelt? Dit zijn maar een paar invalshoeken die genomen kunnen worden als het gaat om de privacystatements. Deze invalshoeken beginnen echter met hetzelfde uitgangspunt: *Wat* staat er in de statements en vervolgens, *hoe* staat dit er? De onderzoeksvragen zijn daarom de volgende: 1. Wat staat er in de privacystatements van zoekmachinebedrijven? 2. Hoe verwoorden zoekmachinebedrijven de onderwerpen die aan bod komen in hun privacystatements? Om deze vragen te beantwoorden wordt de *grounded theory* methode toegepast. Deze methode wordt omschreven als:

> Bernard (2000) describes grounded theory as 'a set of techniques for (1) identifying categories and concepts that emerge from text, and (2) linking the concepts into substative and formal theories. (Kawulich, 2004, p. 97)

Deze methode is gekozen omdat het een basis geeft voor de analyses. Ook zorgt de methode voor inbedding in literatuur; de gepresenteerde analysemethoden kunnen getoetst worden aan de hand van bestaande maatstaven voor kwalitatief onderzoek[5]. In dit onderzoek wordt de methode op twee niveaus toegepast, ten eerste om de *wat* en *hoe* vragen te beantwoorden, de *set of techniques* wordt in het volgende gedeelte toegelicht, ten tweede worden de antwoorden op de *wat* en *hoe* vragen gebruikt als *technique* om de stap naar een *substative and formal theory* te maken. Deze tweede stap wordt gedaan aan de hand van de volgende onderzoeksvraag: Hoe kan een privacystatement voor zoekmachinebedrijven eruit zien volgens experts?

Zoals we straks zullen zien, verschillen de privacystatements behoorlijk van elkaar, niet alleen in de onderwerpen die besproken worden, maar ook in de formuleringen daarvan. Met een antwoord op de *wat* en *hoe* vraag zijn we nog niet bij een *substative and formal theory*; we hebben dan alleen nog maar een idee van het bestaande materiaal. De stap naar een *theory* wordt gedaan aan de hand van de bovengenoemde onderzoeksvraag; de antwoorden op de eerste twee onderzoeksvragen geven een inhoudelijk beeld van *wat er is te vinden* in de privacystatements van zoekmachinebedrijven en de derde onderzoeksvraag geeft hopelijk een basis voor een theorie over wat een 'goed' privacystatement *zou kunnen zijn*.

In het kort proberen we eerst grip te krijgen op de privacystatements aan de hand van de *wat* en *hoe* vragen. De antwoorden op deze vragen worden vervolgens zelf als *techniques* gebruikt om een theorie te formuleren aan de hand van de derde onderzoeksvraag. In het volgende gedeelte wordt uitgelegd hoe deze vragen beantwoord zullen worden. Samengevat zijn dit de onderzoeksvragen:

1. Wat staat er in de privacystatements van zoekmachinebedrijven?
2. Hoe verwoorden zoekmachinebedrijven de onderwerpen die aan bod komen in hun privacystatements?
3. Hoe kan een privacystatement voor zoekmachinebedrijven eruit zien volgens experts?

[5] Zoals: *Credibility, Transferability, Dependability, Conformability.*

2 THEORETISCH KADER

2.1 RAAMWERK

Het corpus voor dit onderzoek is behoorlijk specifiek en er is geen vooropgestelde manier om 'privacystatements van zoekmachinebedrijven' te analyseren. Om deze reden worden verschillende methoden samengevoegd om de statements op een systematische manier te analyseren en zo de onderzoeksvragen te beantwoorden. Het samenvoegen van de methoden wordt, zoals eerder genoemd, gedaan aan de hand van de *grounded theory* methode en in de volgende gedeeltes wordt de *set of techniques for identifying categories and concepts that emerge from text* (zie p. 3) gepresenteerd.

2.2 ARGUMENTATIEANALYSE

Om grip te krijgen op het materiaal en om voornamelijk de eerste onderzoeksvraag te beantwoorden, is gekozen om gebruik te maken van argumentatieanalyse. Deze keuze is gemaakt omdat de statements behoorlijk verschillende 'vormen' kunnen hebben; sommige bedrijven presenteren complexe juridische documenten, waar andere juist een lopend verhaal presenteren. Dit maakt het lastig om de statements op een universele manier te bekijken. Argumentatieanalyse biedt hier een uitkomst omdat het puur gericht is op de tekst. Er zijn raamwerken voor het analyseren van de *data ethics* of *privacy governance* binnen bedrijven, zoals we verderop ook zullen zien, maar deze vullen de onderwerpen die voor *zouden moeten* komen al in. De focus van de *wat* vraag komt daar nog voor; we weten niet wat er in de statements staat en dat is wat we willen weten. Dit maakt argumentatieanalyse op dat gebied een geschikte methode.

Aan privacystatements zit niet alleen een informatieve kant, maar ook een argumentatieve; binnen het onderwerp van online privacy is genoeg ruimte om een standpunt in te nemen, denk aan: het wel of niet verzamelen van persoonlijke gegevens, het wel of niet verwijderen van data wanneer iemand een account deactiveert, het wel of niet tonen van advertenties op basis van persoonlijke gegevens, enzovoorts. "[Een standpunt] betreft een kwestie waarover verschil van mening bestaat (of kan bestaan)." (Karreman en van Enschot, 2013) Naast inhoudelijke relevantie, biedt argumentatieanalyse ook een structureel raamwerk om te zien *wat* er in de statements staat. Dit wordt gedaan aan de hand van de volgende stappen (uit hoofdstuk 5 over argumentatieanalyse uit het boek van Karreman en van Enschot (2013)):

1. Identificeer de centrale stelling (het hoofdstandpunt) in het statement.
2. Identificeer de directe argumenten die gebruikt worden ter ondersteuning van deze stelling.

Argumentatieanalyse kan veel breder en dieper ingezet worden dan alleen deze twee punten. Hier is gekozen om alleen naar de centrale stelling en de bijbehorende argumenten te kijken, omdat dat voor dit onderzoek genoeg structuur geeft om te kijken naar *wat* er in de privacystatements staat. Daarnaast geeft dit voldoende houvast om de *hoe* vraag te benaderen.

Wanneer we de centrale stelling en de argumenten hebben, kunnen we kijken naar hoe deze verwoord worden en wat het mogelijke doel daarvan is.

2.3 Persuasieve Documenten & Corporate Social Responsibility

2.3.1 Persuasie

In het vorige gedeelte zagen we dat de privacystatements een argumentatieve kant hebben; er is immers ruimte om een standpunt in te nemen als het gaat om online privacy. De formulering van de standpunten en onderwerpen is de volgende stap om grip te krijgen op de statements. Om de *hoe* vraag, die in dit gedeelte centraal staat, systematisch te beantwoorden, worden privacystatements gezien als *persuasieve documenten*:

> Persuasieve documenten worden ontworpen met als doel de attitude van de lezer te beïnvloeden door middel van informatieoverdracht, waarbij de lezer een zekere mate van vrijheid heeft. (Hoeken, Hornikx en Hustinx, 2009, p. 14).

Het is belangrijk om hierbij op te merken dat Hoeken persuasieve documenten in het algemeen bedoelt, niet specifiek toegepast op een bepaald onderwerp. Privacystatements vallen binnen deze categorie van teksten omdat er argumenten gebruikt worden en omdat de lezer, in dit geval de gebruiker van de dienst, op veel vlakken 'een mate van vrijheid' heeft. Gaat de gebruiker deze zoekdienst gebruiken of een andere op basis van het statement[6]? Gelooft de gebruiker de intenties van het bedrijf die in het statement gepresenteerd worden (overtuigen)? Hier is het belangrijk om op te merken dat in dit onderzoek de focus puur op de tekst van de statements ligt en niet op, bijvoorbeeld, de persuasieve effecten van teksten op proefpersonen, iets waar Hoeken veel aandacht aan besteedt.

Hoeken geeft aanbevelingen en technieken die gebruikt kunnen worden bij het maken van persuasieve documenten. De privacystatements zijn echter al bestaande documenten en we kunnen niet in de hoofden van de makers kijken om te zien of zij die technieken bewust hebben toegepast. Daarom worden deze technieken alleen gebruikt om te kijken naar hoe de onderwerpen geformuleerd zijn *in de tekst op zich*. Dit brengt een zekere mate van subjectiviteit met zich mee wat nadelig is voor de *Credibility* van het onderzoek: een fenomeen [in dit geval het statement] kan verschillend geïnterpreteerd worden (Sikolia, Biros, Mason en Weiser, 2013). Om hier betrouwbaar en transparant mee om te gaan worden enkel aanbevelingen van Hoeken gebruikt die puur in de tekst te zien zijn. Dit zijn dus geen punten zoals 'begrijpelijkheid' (Hoeken e.a., 2009, p. 101) die grotendeels afhankelijk zijn van de interpretatie van proefpersonen, maar juist punten als:

- Worden argumenten overwegend gepresenteerd aan de hand van voor- of nadelen? (Hoeken e.a., 2009, p. 125)
- Worden bepaalde vuistregels toegepast in de argumenten? Voorbeelden hiervan zijn geloofwaardigheidsvuistregels (als een betrouwbaar iemand het zegt, dan zal het wel

[6] De uitleg van de Autoriteit Persoonsgegevens van het begrip *privacystatement* speelt hier ook op in, zie p. 2

waar zijn), consensusvuistregels (hoe meer mensen iets zeggen, hoe waarschijnlijker dat het waar is) en meer-argumentenvuistregels (hoe meer argumenten er voor het standpunt zijn, hoe waarschijnlijker dat het standpunt waar is) (Hoeken e.a., 2009, p. 167-169).

- Worden *fear appeals* gebruikt in de argumenten? *Fear appeals* benadrukken nadelige gevolgen, er wordt schrik aangejaagd om iets juist wel of niet te doen (Hoeken e.a., 2009, p. 131).

Met deze punten krijgen we al een beter beeld van *hoe* de onderwerpen die aan bod komen verwoord worden in de privacystatements. De volgende stap is een methode kiezen die houvast biedt om persuasieve uitingen *van bedrijven* te analyseren. Dit dient als verlengstuk van van de punten van Hoeken: worden er bijvoorbeeld bepaalde tactieken of strategieën gebruikt? Schetst het bedrijf een bepaald beeld van zichzelf?

2.3.2 Corporate Social Responsibility

Dit brengt ons bij *Corporate Social Responsibility* (CSR). De persuasieve kant van de privacystatements van de zoekmachinebedrijven, in combinatie met het maatschappelijke aspect van online privacy, valt goed onder te brengen bij CSR, wat in Cornelissen (2014) omschreven wordt als:

> The continuing commitment by business to contribute to economic development while improving the quality of life of the workforce and their families as well as of the community and society at large. (p. 26)

Dit gebied wordt logischerwijs vaak in verband gebracht met duurzaamheid, milieu of werkomstandigheden. Online privacy is een nieuwkomer in dit rijtje, maar lijkt daar zeker thuis te horen gezien de toenemende maatschappelijke aandacht voor online privacy, meer bedrijven & organisaties die hierop inspelen[7] en nieuw onderzoek in dit gebied. In een onderzoek van Pollach (2011) naar CSR uitingen van technologiebedrijven, met de vraag of online privacy hierin voorkwam, concludeert ze het volgende:

> The findings suggest that information privacy is emerging as an element of CSR programs, but that there is a great deal of variety regarding the adoption of privacy as a CSR. (p. 89)

Pollach brengt echter een opvallend punt naar voren, namelijk dat zij geen *privacy policies* heeft opgenomen in haar corpus:

> Privacy policies, which are a standard element of every commercial website, were not collected, as their existence alone does not represent a commitment to social responsibility. (p. 92)

[7] Wat ook wordt aangekaart in de uitleg van de Autoriteit Persoonsgegevens, zie p. 2

In dit onderzoek is, zoals eerder aangegeven, de lijn tussen een *privacystatement*, een *privacy policy* en een *about page* niet zo zwart wit. Ook zullen we straks zien dat de statements wel degelijk voor uitingen van CSR gebruikt worden, zelfs als ze naar de meer juridische (*privacy policy*) kant neigen. Ik ben het hierdoor niet helemaal eens met de conclusie die getrokken wordt; de *privacy policies* op zich representeren inderdaad niet een *commitment to social responsibility*, maar er kunnen zeker elementen in voorkomen die dit wel communiceren. Als we vervolgens kijken naar de uitleg van het begrip *privacy policy* die Pollach aanhoudt, dan zien we dat zij praktisch gezien ook de uitleg gebruikt die in dit onderzoek aangehouden wordt:

> The original idea behind privacy policies on websites was that companies would disclose how they handle the data they collect from users, while users would carefully read through the explanation of the company's data handling practices, understand their consequences, and then make an informed decision about divulging personal data or not. In reality, privacy policies contain legalese, techspeak, and other obfuscating language patterns that obscure questionable data handling practices. (p. 90)

Dit zijn inderdaad aspecten die onderdeel kunnen zijn van *privacy policies*, maar dat wil nog niet zeggen dat daar geen CSR elementen in voor kunnen komen.

Uitingen van bedrijven rondom online privacy lijken qua vorm ook op meer traditionele CSR uitingen. Veel bedrijven produceren uitingen rondom CSR en gebruiken dit vaak als een PR instrument (Cornelissen, 2014, p. 366-367). Dit wordt ook gedaan door enkele bedrijven die in dit onderzoek zijn opgenomen, bijvoorbeeld in de vorm van blogs over online privacy[8]. Daarnaast hebben enkele bedrijven die zijn opgenomen in dit onderzoek zogenaamde *sustainability statements*[9], wat voor sommige bedrijven, qua vorm, in dezelfde lijn van *privacystatements* ligt.

CSR biedt in dit geval naast inhoudelijke relevantie ook theorie om onderwerpen en formuleringen binnen de privacystatements te typeren. Hier wordt het eerdergenoemde boek van Cornelissen (2014) voor gebruikt. Net als bij Hoeken worden *aanbevelingen* die gedaan worden gebruikt om de CSR technieken te typeren. Ook hier weer puur op de tekst gericht.

Cornelissen geeft lijst met punten die overwegend goed beoordeelde bedrijven, als het gaat om hun CSR uitingen, toepassen (p. 369-370). Op deze punten wordt ook gelet voor de analyse:

1. Set clear objectives: the company shows that it is serious about CSR by setting clear objectives for social and environmental performance annually, and by systematically reporting on the results achieved afterwards.
2. Set progressive objectives: objectives are progressive in bringing new aspi-

[8] https://www.startpage.com/blog/ & https://www.duckduckgo.com/blog/

[9] https://sustainability.google/ & https://www.gigabitmagazine.com/company/how-yandex-heating-finnish-city-its-data-centres-surplus-energy

rations and standards to bear upon business operations instead of a regurgitating of existing practices that may be seen as socially and environmentally viable.

3. Involve stakeholders: objectives and targets include issues that are relevant to stakeholders; and are linked to clear benchmarks and standards (at the industry and policy levels).
4. Report transparently: Reporting is an honest, transparent and full-scale self-assessment instead of a polishing of performance data.
5. Be accountable: Performance data are rigorously assessed and verified by credible auditors (accountants or consultants).

Deze punten worden gelinkt aan de manier waarop de onderwerpen die aan bod komen verwoord worden. Ze geven echter een beperkt beeld van *of* en *hoe* het bedrijf 'online privacy als CSR' verwoordt; een bedrijf kan alle punten perfect opvolgen, maar tegelijkertijd een dubieuze uitleg van 'online privacy als CSR' aanhouden. Een volgend interessant punt om te bekijken is daarom hoe de bedrijven online privacy als CSR uitleggen en of dit überhaupt gedaan wordt. Hiervoor wordt gekeken naar hoe het bedrijf zichzelf, in de privacystatements, verhoudt tot online privacy. Dit kan onder andere gedaan worden wanneer ze een *corporate identity* van zichzelf schetsen:

> (...) corporate identity, as the outward presentation of an organization through symbolism, communication and behaviour, should emerge from an understanding of the organization's core mission, strategic vision and the more general corporate culture of an organization. The mission and vision represent the basic who and what of an organization; what business the organization is in and what it wants to be known and appreciated for. An organization's mission often already includes a statement on the beliefs that constitute the organization's culture and underpin its strategy and suggests how the organization wants to be known by stakeholder groups outside the organization. (Cornelissen, 2014, p. 130)

Dit is nog niet per definitie direct zichtbaar in de tekst, daarom wordt gelet op uitingen die getypeerd kunnen worden als *strategic intent*:

> (...) strategic intent (...) is translated into themed messages that are designed to change or reinforce perceptions in line with the vision of how the organization wants to be known. (...) themed messages are strategic messages that relate to specific capabilities, strengths or values (as 'themes') of an organization. (Cornelissen, 2014, p. 169-171)

Samengevat worden de privacystatements bekeken aan de hand van *aanbevelingen voor CSR uitingen* en of dit in de statements doorgetrokken wordt naar *strategic intent* uitingen die een bepaald *corporate image* schetsen. Deze punten zorgen voor een wat meer toegespitste insteek wanneer we privacystatements niet alleen als *persuasieve* uitingen zien, maar ook als persuasieve uitingen *van bedrijven*.

2.4 EXPERTS

Voor de derde onderzoeksvraag en het formuleren van een *substative and formal theory* worden experts geraadpleegd op twee manieren. Eerst wordt bestaande vakliteratuur over communicatie over online privacy binnen bedrijven uit verschillende onderzoeksgebieden vergeleken. Aan de hand van de resultaten uit die analyse wordt een *theory* geformuleerd. Daarna is een kort interview afgenomen met universitair hoofddocent IT-recht, prof. dr. J.H. Hoepman waarin de *theory* aan hem is voorgelegd. Het interview had ruwweg de derde onderzoeksvraag als hoofdlijn, oftewel; hoe ziet een 'goed' privacystatement voor een zoekmachinebedrijf eruit? De uitwerking en bespreking van de experts staat in hoofdstuk 5 (p. 19), na de *wat* en *hoe* analyses van de privacystatements. Op deze manier kan direct een vergelijking gemaakt worden met de bestaande statements.

3 METHODE

3.1 MATERIAALVERZAMELING

Voor het verzamelen van de privacystatements zijn enkele methodologische voorwaarden opgesteld. Deze voorwaarden moeten voor een zo eerlijk en neutraal mogelijke analyse van de statements zorgen. In het kader van *grounded theory* moeten deze voorwaarden bijdragen aan *Credibility, Transferability, Dependability* en *Conformability*. De onderstaande voorwaarden kunnen gezien worden als een *thick description*; een uitgebreide uitleg van het materiaal met aandacht voor de situaties en context waarin dit voor kan komen (Shenton, 2004, p. 69, Kawulich, 2004, p. 98, Sikolia e.a., 2013, p. 3).

In de discussie worden de implicaties van deze voorwaarden nog extra belicht. De volgende voorwaarden zijn toegepast bij het verzamelen van de privacystatements:

- *De statements moeten afkomstig zijn van bedrijven.*

  In de onderzoeksopzet van deze scriptie waren eerst, naast bedrijven, twee zoekdiensten van *organisaties* opgenomen: Searx en Yacy. Hoewel dit zeker interessante diensten zijn, is de keuze gemaakt om deze niet mee te nemen in de analyse omdat het verschil te groot is tussen een open-source organisatie zonder winstoogmerk die onderhouden wordt door vrijwilligers en een commercieel bedrijf. De diensten zijn praktisch gezien hetzelfde, maar de contextuele verschillen waren toch te groot.

- *De statements moeten verzameld worden op dezelfde dag.*

  Dit zorgt voor een eerlijke vergelijking. Privacystatements worden zo nu en dan aangepast (zie bijvoorbeeld DuckDuckGo, p. 62 & Google, p. 66). Indien de statements over bijvoorbeeld een periode van een maand verzameld worden, dan is het risico dat nieuwe versies of aanpassingen uitgekomen zijn aanzienlijk groter vergeleken met het verzamelen van de statements op dezelfde dag. De statements voor dit onderzoek zijn allemaal verzameld op 4 november 2019.

- *De bedrijven of organisaties moeten een Nederlandse of Engelse variant van hun dienst hebben.*

  Dit punt is toegepast om het corpus toe te spitsen en om taalbarrières te voorkomen. Er zijn tal van populaire zoekmachines in andere talen gericht op specifieke landen: Baidu is bijvoorbeeld de grootste zoekmachine in China (70.26% marktaandeel in 2018[10]), maar heeft geen Engelse of Nederlands variant. Yandex is hier ook een voorbeeld van voor Rusland (51.08%), zij bieden echter wel een Engelse variant aan en zijn daarom ook opgenomen in het corpus voor dit onderzoek.

- *De eerste link die gerelateerd is aan 'privacy' op de hoofdpagina van de dienst wordt aangehouden als 'privacystatement'.*

  Dit ook in het kader van een eerlijke vergelijking. Sommige bedrijven (bijvoorbeeld Startpage of Qwant) hebben informatie rondom privacy verspreid over hun website staan, bijvoorbeeld een gedeelte op een *About us* of *About the company* pagina en een gedeelte op een specifieke privacy pagina. Om de vergelijking eerlijk en gelijk te houden wordt de specifieke privacy pagina daarom gekozen boven de *About* pagina. Praktisch gezien houdt dit in dat bijvoorbeeld naar qwant.com gegaan is en daar gezocht is naar een link met 'privacy' in de naam op de landingspagina (deze bevinden zich vaak helemaal onderaan de pagina).

- *De bedrijven moeten actief zijn op het moment dat de privacystatements verzameld worden.*

  Dit heeft te maken met de relevantie en beschikbaarheid van de statements. In dit onderzoek is de keuze gemaakt om geen 'historische' statements mee te nemen in de vergelijking en analyse.

- *De bedrijven moeten een publiek toegankelijk zoekdienst aanbieden.*

  Dit is een essentiële voorwaarde voor het onderzoek. Wanneer een zoekdienst niet publiekelijk aangeboden wordt of niet publiekelijk toegankelijk is (bijvoorbeeld een interne zoekmachine binnen een bedrijf), dan zegt een privacystatement in de context van Corporate Social Responsibility niet veel. Essentieel in CSR is het *social* (maatschappelijk) gedeelte; oftewel de relatie met de *community and society at large* (Cornelissen, 2014, p. 26). Een werkgerelateerde, interne zoekdienst zal daarnaast waarschijnlijk minder over het persoonlijke leven van een gebruiker zeggen en daardoor minder privacygevoelig zijn. Zoals eerder aangegeven, is een zoekdienst de 'ingang' tot het internet voor praktisch alle internetgebruikers. De informatie die dit oplevert is vele malen persoonlijker dan een 'ingang' naar een interne zoekdienst.

[10] https://medium.com/@SearchDecoder/global-search-engine-market-share-for-2018-in-the-top-15-gdp-nations-2cf65c11e5f5

3.2 LIJST VAN ZOEKMACHINEBEDRIJVEN

Aan de hand van de voorwaarden uit het vorige gedeelte zijn de volgende bedrijven geselecteerd:

- Ask
- Bing
- DuckDuckGo
- Google
- Qwant
- Startpage
- Wolfram Alpha
- Yahoo
- Yandex (Engelse variant)

4 ANALYSE MATERIAAL

4.1 EERSTE INDRUKKEN

Tot nu toe zijn privacystatements nog een behoorlijk abstract begrip gebleven, daarom worden nu enkele eerste indrukken gepresenteerd. Zoals in de methode beschreven staat, wordt de eerste link die met privacy te maken heeft op de hoofdpagina van de zoekmachine gebruikt om naar het privacystatement te komen.

De privacystatements verschillen op het eerste gezicht enorm van elkaar. Bedrijven als Aks, Bing en Google linken naar lange en grote pagina's met privacy informatie over hun complete bedrijf. De gebruiker moet zelf op zoek naar het relevante gedeelte over de zoekmachinedienst van deze bedrijven. Deze informatie wordt vervolgens, met een korte introductie, als een opsomming gepresenteerd, soms met tussenstukken. Yahoo is hierbij een uitzondering, zoals we straks ook zullen zien, zij presenteren enkel een lijst met opsommingen zonder introductie en zonder tussenstukken. Aan de andere kant maken DuckDuckGo, Qwant, Startpage en Yandex een doorlopend verhaal van hun privacystatements met toelichtingen over technische details. Ook de lengte van de statements loopt behoorlijk uiteen; Aks en Google hebben bijvoorbeeld bijna negen pagina's tellende statements, terwijl DuckDuckGo en Yandex maar twee tot drie pagina's hebben.

4.2 WAT WORDT GEZEGD?

In dit gedeelte worden de meest opvallende en bevindingen besproken die uit de argumentatieanalyse naar voren zijn gekomen. In op pagina 38, in de bijlagen, zijn de uitgebreide uitwerkingen hiervan te vinden.

De centrale stellingen worden in bijna alle statements in de eerste paragraaf, meestal de inleiding, gegeven. De 'conclusie' wordt direct gepresenteerd en de argumenten worden verderop in de statements uitgewerkt. Yahoo is hier een uitzondering, in het statement van Yahoo worden enkel feiten opgesomd zonder een standpunt te formuleren. Verder valt op dat bedrijven

uiteenlopende centrale stellingen innemen. Ten eerste is een duidelijke splitsing te zien bij wie het 'probleem' (of verantwoordelijkheid) van 'privacy' ligt. Dit 'probleem' slaat in de statements op 'privacy' in het algemeen of 'persoonlijke informatie'. In tabel 1 is te zien dat een groep bedrijven zichzelf als 'verantwoordelijke partij' neerzet; zij nemen het 'probleem' van privacy op zich: *we are commited* of *we begrijpen dat dit een grote verantwoordelijkheid is*. De andere groep suggereert dat deze verantwoordelijkheid bij de gebruiker ligt met stellingen als: *Wolfram Alpha understands your concerns about how your information is used and shared*. Ask en Wolfram Alpha formuleren hun stellingen op dezelfde manier; ze geven aan dat ze snappen dat gebruikers hun eigen privacy belangrijk vinden en vervolgens wat zij als aanbieder van de dienst daaraan kunnen bijdragen. Deze bedrijven refereren wel naar zichzelf, maar leggen 'het probleem' bij de gebruiker neer.

Een andere duidelijke tweedeling is te zien in de manier en plaats van vermelden of het bedrijf juist *wel* of *niet* persoonlijke gegevens van hun gebruikers verzamelt. Enkele bedrijven kaarten dit punt direct aan in hun centrale stelling. Bij anderen komt dit pas verderop naar voren. Wat hier opvalt is dat bedrijven die juist *wel* persoonlijke informatie verzamelen, dit niet in de centrale stelling noemen. De centrale stellingen van deze bedrijven nemen altijd twee insteken: benadrukken dat de privacy van de gebruiker belangrijk is voor hen of benadrukken dat ze begrijpen dat de gebruiker zijn of haar privacy belangrijk vindt. Dit sluit aan op het vorige verschijnsel bij wie de 'verantwoordelijkheid' ligt (zie tabel 1). Aan de andere kant vermelden bedrijven als DuckDuckGo, Startpage en Qwant, die juist geen persoonlijke informatie verzamelen, dit punt direct in hun centrale stelling. Mogelijke inhoudelijke verklaringen hiervoor worden besproken in sectie 4.3. Omdat het wel of niet verzamelen van persoonsgegevens een belangrijk punt is, zoals we straks zullen zien, staat in tabel 2 een overzicht van deze splitsing. Het is belangrijk om te benadrukken dat deze tabel puur gebaseerd is op *de tekst* van de statements; er worden geen uitspraken gedaan over het punt of deze bedrijven ook navolgen wat ze claimen in de statements.

Wel	**Niet**
Ask	DuckDuckGo
Bing	Qwant
Google	Startpage
Wolfram Alpha	
Yahoo	
Yandex	

Tabel 2: Bedrijven die wel of niet persoonsgegevens verzamelen.

Qua onderwerpen die aan bod komen, zijn er verrassend weinig die in alle statements voorkomen. De meest duidelijke die in alle genoemd worden zijn: het verzamelen van persoonsgegevens (onder andere: wel of niet verzamelen) en een technische 'uitleg' van cookies, zoekopdrachten of HTTPS. Die uitleg kan weer erg verschillen in lengte, DuckDuckGo wijdt hier een complete, zeer gedetailleerde pagina aan, Google noemt het in tussenzinnen bij relevante onderwerpen en Yandex noemt alleen de termen zonder echte uitleg. Als de splitsing

Wij zijn verantwoordelijk	**De gebruiker is verantwoordelijk**
Uw privacy is *belangrijk voor ons*. In deze privacyverklaring wordt uitgelegd welke persoons-gegevens Microsoft verwerkt, hoe Microsoft deze verwerkt en voor welke doeleinden het bedrijf deze verwerkt. (**Bing**)	We understand that *your privacy is important to you*, and we are committed to being transparent about the information we collect and process upon your use of our websites. (**Ask**)
Wanneer u onze services gebruikt, *vertrouwt u ons* uw gegevens toe. We begrijpen dat dit een grote verantwoordelijkheid is en werken er hard aan om uw gegevens te beschermen en u erde controle over te geven. (**Google**)	DuckDuckGo does not collect or share personal information. That is our privacy policy in a nutshell. The rest of this page tries to explain *why you should care*. (**DuckDuckGo**)
Qwant ensures that your privacy is protected, and this is *the cornerstone of our philosophy*. (**Qwant**)	Wolfram understands *your concerns about how your information is used and shared*, and we endeavor to use such information carefully and sensibly. This policy explains how the information you provide is collected and used. (**Wolfram Alpha**)
Startpage.com doesn't log or share your personal information. *We don't track you. We don't profile you.* Period. (**Startpage**)	
For over twenty years, Yandex has served millions of users, working to maintain their trust through *our commitment to protecting their privacy and freedom of expression online. Our commitment to users* is rooted in Yandex's wider responsibility to respecting human rights. Data privacy and security is an important part of this commitment. (**Yandex**)	

Tabel 1: Verantwoordelijkheid in centrale stellingen.

van *wel* en *niet* verzamelen van persoonsgegevens weer gemaakt wordt, dan zijn er wel overeenkomstige onderwerpen en argumenten te zien binnen de groepen. Binnen de groep die *wel* persoonsgegevens verzameld komt het argument dat *gebruikers keuzes hebben als het gaat om de data die verzameld worden [waardoor u goed zit bij ons]* vaak terug, waarbij de centrale stelling van deze bedrijven, zoals eerder genoemd, in de trend is van *wij snappen dat u zich zorgen maakt over uw data* of *wij nemen de verantwoordelijkheid van het omgaan met uw data serieus*.

In de statements van de bedrijven die *wel* of *geen* persoonsgegevens verzamelen, worden regelmatig dezelfde argumenten gebruikt, maar dan voor tegenovergestelde centrale stellingen:

> Our commitment to users is rooted in Yandex's wider responsibility to respecting human rights. - *Yandex* (verzamelen wel persoonsgegevens)
>
> We believe privacy is a fundamental human right. With Startpage.com you can search and browse the internet privately. - *Startpage* (verzamelen geen persoonsgegevens)

Yandex zegt dat ze persoonsgegevens verzamelen omdat dat ervoor zorgt dat ze een goede dienst kunnen leveren, wat weer zorgt voor een bijdrage aan *respecting human rights*. Startpage geeft precies hetzelfde argument, maar dan met de insteek dat ze een goede dienst leveren die *human rights* respecteert door geen persoonsgegevens te verzamelen. Dit soort patronen zijn vaker te zien: bijvoorbeeld als het gaat om technische innovatie; 'wij leveren een meer innovatie dienst *omdat* we persoonsgegevens verzamelen' bij Bing, Google en Yandex. Hetzelfde argument, maar dan 'omdat we *geen* persoonsgegevens verzamelen' bij DuckDuckGo, Startpage en Qwant.

In het kort zijn hier nog enkele opvallende verschijnselen rondom de *wat* vraag:

- Qwant noemt als enige de omgang met persoonlijke informatie rondom sollicitaties in hun statement.
- DuckDuckGo & Yahoo zijn de enigen die de GDPR (Europese Privacywet) *niet* noemen.
- DuckDuckGo, Qwant en Startpage geven alle drie tips voor gebruikers om hun online privacy te verbeteren in het algemeen, oftewel, ook buiten hun eigen dienst.

4.3 Hoe wordt het gezegd?

Zoals we in het vorige gedeelte zagen zijn er veel verschillen tussen de onderwerpen en argumenten die aan bod komen in de statements. Zoals we zullen zien is dit niet anders als het gaat om de manier waarop de statements verwoord worden.

4.3.1 VOORDELEN EN NADELEN

De framing van de argumenten verschilt weer sterk tussen de bedrijven die *wel* of *niet* persoonsgegevens verzamelen. Zoals eerder genoemd maakt Hoeken een splitsing tussen het presenteren van argumenten op basis van voordelen of nadelen. De bedrijven die *wel* persoonsgegevens verzamelen presenteren hun argumenten voornamelijk op basis van voordelen:

- Wij bieden innovatieve diensten door de informatie die we verzamelen. (Google, Bing, Yandex)
- U heeft veel overzichtelijke opties waarmee u controle heeft over de informatie die wij verzamelen. (Ask, Google, Bing, Wolfram Alpha, Yandex)
- Doordat we persoonsgegevens verzamelen zijn we in staat belangrijke en positieve dingen te doen zoals: klanten beschermen, relevante aanbevelingen doen, levens te beschermen, de veiligheid van onze producten te garanderen en onze diensten in stand te houden. (Google, Bing, Wolfram Alpha, Yandex)

Deze bedrijven presenteren bijna geen argumenten op basis van nadelen. De enige duidelijke 'nadelige' insteek komt impliciet naar boven wanneer het gaat om het beschermen van de verzamelde persoonsgegevens: 'wij doen ons best om uw persoonsgegevens zo goed mogelijk te beveiligen [zodat er niet iets negatiefs mee kan gebeuren]'. De bedrijven die geen persoonsgegevens verzamelen presenteren daarentegen juist meer argumenten op basis van nadelen:

- We nemen maatregelen die zorgen dat de privacy van gebruikers gewaarborgt blijft, in tegenstelling tot andere zoekmachinebedrijven. (DuckDuckGo, Startpage)
- Op veel plekken op het internet worden uw persoonsgegevens verkocht, bij ons niet. (DuckDuckGo, Startpage, Qwant)

Wat hierbij opvalt is dat het nadeel in bijna alle gevallen gebracht wordt als een *fear appeal* en niet als een vervelend nadeel in het algemeen. Dit gebeurt door de link die steeds gelegd wordt met andere internet diensten, waaronder andere zoekmachinediensten. Deze worden nooit met naam genoemd, wat misschien nog meer inspeelt op de 'angst' dat 'het internet een slechte plek is voor privacy', wat vervolgens weer inspeelt op het idee, 'maar bij ons zit u goed':

> At other search engines, when you do a search and then click on a link, your search terms are sent to that site you clicked on (in the HTTP referrer header). We call this sharing of personal information 'search leakage.' For example, when you search for something private, you are sharing that private search not only with your search engine, but also with all the sites that you clicked on (for that search). - *DuckDuckGo*
>
> We never try to find out who you are or what you are personally doing when you use our search engine. When we do need to collect data, we do not disclose nor

> sell it for commercial or other uses. - *Qwant*
>
> We don't serve any tracking or identifying cookies. This is about 'good' and 'bad' cookies. Cookies are small pieces of data that are sent to your hard drive by websites you visit. 'Bad' cookies have unique elements that can track all kinds of personal information. We don't serve any of those. Startpage.com uses just one 'good' cookie called 'preferences' in order to remember the search preferences you choose. It's completely anonymous and expires after not visiting Startpage.com for 90 days. - *Startpage*

4.3.2 STRATEGIE

Bing (Microsoft), Google en Yandex benoemen alle drie hoe 'belangrijk' en 'invloedrijk' hun bedrijf is voordat relevante informatie over privacy aan bod komt.

> Microsoft biedt een breed scala aan producten, waaronder serverproducten die wereldwijd worden gebruikt om ondernemingen te ondersteunen, apparaten die u thuis gebruikt, software die studenten op school gebruiken en services die ontwikkelaars gebruiken voor het maken en uitvoeren van wat er komen gaat. - *Bing (Microsoft)*
>
> We bouwen een reeks services waarmee miljoenen mensen dagelijks de wereld op nieuwe manieren kunnen verkennen en er interactie mee kunnen hebben. - *Google*
>
> For over twenty years, Yandex has served millions of users, working to maintain their trust through our commitment to protecting their privacy and freedom of expression online. - *Yandex*

Bing, Google en Yandex verzamelen alle drie persoonlijke gegevens van hun gebruikers en deze tacktiek lijkt gebruik te maken van het eerdergenoemde punt van Cornelissen dat bedrijven CSR uitingen ook als PR instrument zien en gebruiken. In dit geval om duidelijk te maken dat 'wij als bedrijf deugen [als het gaat om uw privacy]'. Ook lijkt de vuistregel aanbeveling van Hoeken hier te zijn toegepast: 'wij deugen als bedrijf, omdat we veel gebruikers hebben en we veel diensten aanbieden'. Dit lijkt bij alle drie een combinatie te zijn van de *meer-argumentenvuistregel* (veel diensten) en de *consensusvuistregel* (veel mensen gebruiken de diensten).

Zoekmachinediensten die juist geen persoonlijke gegevens verzamelen lijken gebrand op het 'opvoeden' of 'opleiden' van hun gebruikers. In de statements van deze bedrijven wordt bijvoorbeeld een gedetailleerde, technische uitleg gegeven over hoe zij de privacy van hun gebruikers respecteren, om vervolgens te benoemen of suggereren hoe *andere* zoekmachines deze technieken niet toepassen en daarom de privacy van hun gebruikers niet respecteren:

> When you access DuckDuckGo (or any Web site), your Web browser automatically sends information about your computer (...). Because this information

> could be used to link you to your searches, we do not log (store) it at all. This is a very unusual practice, but we feel it is an important step to protect your privacy. It is unusual for a few reasons. First, most server software auto-stores this information, so you have to go out of your way not to store it. Second, most businesses want to keep as much information as possible because they don't know when it will be useful. Third, many search engines actively use this information, for example to show you more targeted advertising. - *DuckDuckGo*
>
> We don't serve any tracking or identifying cookies. This is about 'good' and 'bad' cookies. (...) We don't serve any of those [bad cookies]. - *Qwant*
>
> It's a myth that search engines need to profile you in order to earn decent money. Startpage.com serves strictly non-personalized ads. Sure, our ads make only a fraction of what other search engine ads make, but they pay all our bills. - *Startpage*

DuckDuckGo, Qwant en Startpage laten hier duidelijk merken dat zij online privacy als CSR uitdragen. Cornelissen noemt, in de eerdergenoemde lijst voor het evalueren van CSR communicatie, het volgende punt wanneer het gaat om *involving stakeholders*: "objectives and targets include issues that are relevant to stakeholders" (p. 370). *Stakeholders* zijn in dit geval gebruikers van de dienst. De *objectives and targets* zijn in dit voorbeeld niet alleen dat online privacy belangrijk is binnen hun dienst, maar ook daarbuiten. Om gebruikers daarbij te betrekken (*involving stakeholders*) worden tips gegeven om bewuster om te gaan met online privacy in het algemeen op het internet. De gebruikers die deze statements lezen zijn per definitie al internetgebruikers en de tips bevatten daarom *issues that are relevant to stakeholders*. Het 'opleiden' komt ook naar voren in de toon van DuckDuckGo met tussenkopjes als *"Why you should care - Search History"*.

We zagen al dat de bedrijven die geen persoonlijke informatie verzamelen, dit direct in hun centrale stelling vermelden. Wat opvalt aan de manier waarop ze dit doen is dat ze alle drie dit als een soort *one-liner* verwoorden:

> We don't collect or share personal information. That's our privacy policy in a nutshell. - *DuckDuckGo*
>
> Qwant ensures that your privacy is protected, and this is the cornerstone of our philosophy. - *Qwant*
>
> Startpage.com doesn't log or share your personal information. We don't track you. We don't profile you. Period. - *Startpage*

Dit laat mooi de persuasieve kant van de statements zien. De bedrijven in het voorbeeld presenteren online privacy als een essentieel onderdeel van hun dienst en bedrijf. Cornelissen omschrijft dit als *strategic intent*:

> (...) strategic intent (...) is translated into themed messages that are designed to change or reinforce perceptions in line with the vision of how the organization wants to be known. (...) themed messages are strategic messages that relate

> to specific capabilities, strengths or values (as 'themes') of an organization. (p. 169-171)

Deze bedrijven laten merken dat online privacy een kracht (*strength*) van hen is. Specifiek is het 'niet verzamelen van persoonsgegevens' een essentiele kracht volgens deze bedrijven. Dit werkt niet alleen door in de statements zelf, maar ook in andere uitingen van de bedrijven. Deze uitingen zijn niet de focus van deze analyse, maar helpen wel met het typeren van deze bedrijven en de context waarin de statements zich begeven. De eerdergenoemde blogs over privacy (p. 7) zijn hier een goed voorbeeld van. De manier waarop deze bedrijven communiceren suggereert sterk dat online privacy en 'geen persoonsgegeven verzamelen' onderdeel is van hun *corporate identity*. Zonder de context en puur gericht op de statements is dit ook zeker zichtbaar. Cornelissen vat dit fenomeen samen als:

> (...) corporate identity, as the outward presentation of an organization through symbolism, communication and behaviour, should emerge from an understanding of the organization's core mission, strategic vision and the more general corporate culture of an organization. The mission and vision represent the basic who and what of an organization; what business the organization is in and what it wants to be known and appreciated for. An organization's mission often already includes a statement on the beliefs that constitute the organization's culture and underpin its strategy and suggests how the organization wants to be known by stakeholder groups outside the organization. (p. 130)

4.4 VOORLOPIGE CONCLUSIE

We hebben nu een beeld van *wat* er in de statements staat en *hoe* dit verwoord wordt. In het volgende hoofdstuk worden de resultaten voor de derde onderzoeksvraag gepresenteerd. Om straks een duidelijke vergelijking te maken volgt hieronder een korte lijst met de belangrijkste punten uit de vorige analyses.

Meest opvallende onderwerpen die aan bod komen in de statements:

- Welke data worden verzameld.
- Keuzes die de gebruiker heeft rondom het verzamelen van zijn of haar data.
- Waar de verzamelde data voor gebruikt worden.
- Hoe de data verzameld worden.
- Uitleg van technische begrippen rondom het verzamelen van data.

Meest opvallende verwoordingen in de statements:

- Wanneer een bedrijf geen data verzamelt, is dit een vooraanstaand en centraal thema wat zich uit in *strategic messages* die de *corporate identity*, van het niet verzamelen en privacybewust zijn, ondersteunen.

- Wanneer een bedrijf wel data verzamelt, wordt in drie van de zes statements benadrukt door het bedrijf zelf hoe invloedrijk en belangrijk het bedrijf is.
- Bedrijven die data verzamelen presenteren bijna alleen argumenten op basis van voordelen, terwijl bedrijven die geen data verzamelen meer argumenten gebruiken op basis van nadelen.
- Bedrijven die geen data verzamelen gebruiken *fear appeals* in hun op nadelen gebasseerde argumenten.
- De bedrijven die wel en niet data verzamelen gebruiken regelmatig dezelfde argumenten voor tegenovergestelde punten.

5 Analyse experts

We hebben nu een beeld van wat gezegd wordt in de bestaande privacystatements en hoe dit verwoord wordt. De volgende vraag is hoe een 'goed' statement eruit kan zien. Daarvoor wordt eerst een beknopte literatuurreview gedaan in paragraaf 5.1 om te kijken wat experts en wetenschappers vinden als het gaat om online privacy, in het bijzonder: communiceren als bedrijf over eigen online privacy activiteiten. Aan de hand hiervan wordt een *substantive and formal theory* geformuleerd in de vorm van aanbevelingen voor een 'goed' statement. Deze *theory* is vervolgens voorgelegd aan prof. dr. J. H. Hoepman in een interview. De belangrijkste punten daaruit worden in paragraaf 5.2 besproken, ten slotte wordt kort teruggeblikt op de geanalyseerde statements uit het vorige hoofdstuk met de *theory* en het interview in het achterhoofd, in paragraaf 5.3.

5.1 Vakliteratuur

De vakliteratuur bestaat uit onderzoeksartikelen en een boek over hoe bedrijven om kunnen gaan met online privacy. De auteurs benaderen dit vanuit verschillende gebieden die allemaal toepasbaar zijn voor het formuleren van een 'goed' privacystatement en die aansluiten op CSR. Het is belangrijk om vooraf op te merken dat niet alle auteurs letterlijke aanbevelingen doen. Als er echter onderwerpen worden besproken zoals *key issues* (belangrijke aandachtspunten, problemen) binnen het gebied van online privacy of bijvoorbeeld onderwerpen die *stakeholder relations* bevorderen, dan wordt de aanname gedaan dat de zoekmachinebedrijven deze positieve punten willen nastreven. De volgende aanname is dan dat ze dit in hun privacystatement willen verwerken om naar hun gebruikers (*stakeholders*) te communiceren. Als we deze twee aannames vasthouden, dan kunnen we de door de experts genoemde punten als aanbevelingen zien. Zonder deze aannames zijn de punten van de experts nog steeds te vertalen naar de statements. Het is goed om de aannames expliciet te maken in het kader van *credibility*, oftewel; binnen het onderzoek consistent 'meten' en *transferability*, oftewel; wat hier gepresenteerd wordt, moet generaliseerbaar en voor herhaling vatbaar zijn, (Sikolia e.a., 2013, Kawulich, 2004 & Shenton, 2004).

Activity	Description of activity	Ethical consideration
What data to collect?	Personal data and its sensitivity	Proper use of computing technology to protect the data
How it is collected?	Directly (primary data), using existing databases (secondary data)	Must be collected at the consent of the individual
How it is processed?	Logic used in processing data	Proper use of algorithm, i.e. should not be any bias that would favor one over the other individual
How it is presented?	Printed form, computer screen, distribution	Must be presented and distributed with the consent of individual
What purpose it is used for?	Use for marketing, used for performance evaluation, for credit purpose, determining eligibility of some sort	Should be used for the purpose for which the data was created and should not be harmful to anyone
The extent of its impact?	Determine the consequence of its used such as credit approval, legal consequence, health impact	If the impact is severe that would hurt someone's life or if it is going to impact a large number of individuals

Tabel 3: 'Framework for assessing major electronic information activities', overgenomen uit Desai en von der Embse (2008), p. 24.

5.1.1 ACTIVITIES

In het onderzoek van Desai en von der Embse (2008) werden de ethische en organisationele implicaties van online privacy bekeken. Het onderzoek resulteerde in *'A framework for assessing major electronic information activities'*. Privacystatements zijn niet het hoofdonderwerp in dit onderzoek, maar de aanbevelingen voor ethisch en verantwoord omgaan met persoonlijke data van medewerkers en klanten (gebruikers van de zoekmachinediensten in dit geval) kunnen zo vertaald worden naar een privacystatement. Het uiteindelijke raamwerk staat in tabel 3. In het vorige hoofdstuk hebben we gezien dat de meeste bedrijven de ernst van online privacy inzien, benadrukken dit belangrijk te vinden en zeggen hiermee verantwoord om te gaan. Als we aannemen, op basis van die uitingen in de statements, dat 'belangrijk' en 'verantwoord' in dezelfde lijn ligt als 'ethisch', dan is het raamwerk zeker toepasbaar als maatstaf voor een 'goed' statement. Veel van de *activities* worden ook al behandeld in de bekeken statements.

5.1.2 KEY ISSUES

Een tweede raamwerk is opgesteld door Shantz (2018) in een onderzoek naar de implicaties die *data-based business models* hebben voor bedrijven en de maatschappij. Zoals we hebben gezien verkopen de bedrijven die data verzamelen vaak die data met een winstoogmerk in de vorm van gerichte advertenties, wat zeker onder een *data-based business model* valt. In het onderzoek wordt CSR niet letterlijk genoemd, maar de manier van analyseren komt sterk overeen: *stakeholders* worden getypeerd en vergeleken, sociale implicaties worden uitvoerig besproken en de manier waarop een bedrijf met online privacy om zou kunnen gaan wordt besproken aan de hand van *key issues*. Deze *issues* kunnen als maatstaf gebruikt worden om te kijken of de privacystatements deze onderwerpen aankaarten:

> In what follows I outline the issues considered to be central to this organizational field [data goverence]; that is, issues related to ownership, privacy, tracking and discrimination, and power and democracy. (Shantz, 2018, p. 311)

De *issues* worden vervolgens uitgewerkt met voorbeelden uit andere onderzoeken, met de insteek aanbeveling doen voor bedrijven en organisaties om goed en transparant om te gaan met persoonsgegevens. In het bijzonder, de persoonsgegevens verkregen door de *data-driven* dienst die ze aanbieden. Hieronder staan haar aanbevelingen kort samengevat:

- *Ownership:* Wees transparant over hoe het bedrijf waarde toekent aan de data en wie daar winst uit haalt. Weet als bedrijf wat voor type data je verzamelt (medisch, financieel, gebruikersstatistieken, etc.).
- *Privacy:* Wees transparant wanneer het gaat om 'gratis' diensten tegenover je gebruikers, zij zijn niet de klant, zij zijn het product voor de echte klanten (vaak adverteerders).
- *Tracking and discrimination:* Bedrijven moeten goed doorhebben hoe ze data inzetten. Het typeren en targeten van gedetailleerde 'groepen' mensen aan de hand van hun online kenmerken kan verstrekkende gevolgen hebben (bijvoorbeeld het targeten op basis van zwaktes van een groep).
- *Power and democracy:* Bedrijven moeten goed doorhebben hoe ver data ingezet kunnen worden. Hierbij gaat het niet alleen om het targeten van gebruikers, maar ook het voorspellen van het gedrag van gebruikers en daarmee gedrag gepland beïnvloeden.

5.1.3 SENSE MAKING

Eerder werd het onderzoek van Pollach (2011) al besproken waarin CSR uitingen van technologiebedrijven werden bekeken, om te zien of online privacy als een centraal onderwerp (of überhaupt) naar voren kwam. Hiervoor werd het volgende raamwerk gebruikt:

> The starting point for the analysis are the three processes of CSR included in Basu & Palazzo's (2008) process model of sense-making: (1) the reasons a company

> states for engaging in specific CSR activities, (2) the kind of behavior a company displays to live up to its CSR commitments, and (3) the way in which a company regards its relationships with its stakeholders. (Pollach, 2011, p. 91)

Als we weer aannnemen dat bedrijven online privacy als CSR verwerken in hun privacystatements, dan kunnen deze punten gebruikt worden voor het formuleren van een 'goed' statement. Het is belangrijk om op te merken dat hier geen onderscheid gemaakt hoeft te worden tussen het wel en niet verzamelen van persoonsgegevens. Zoals we eerder ook hebben gezien, verwoorden beide groepen online privacy als CSR. De bovenstaande punten van Pollach kunnen vertaald worden naar aanbevelingen voor een statement als volgt:

1. Vermeld waarom online privacy belangrijk is voor het bedrijf, oftewel waarom ze het zien als een CSR.
2. Vermeld wat het bedrijf doet om te onderbouwen dat ze online privacy zien als CSR.
3. Vermeld hoe de bovenstaande punten van invloed zijn op de gebruikers van de dienst.

Pollach zag in haar onderzoek dat bedrijven dit op verschillende manieren aanpakten, maar dat de punten voornamelijk aan de hand van drie *motives* gecommuniceerd werden in de CSR uitingen (p. 94):

1. *Moral:* Three companies acknowledge that people have a right to privacy. Four companies hold that they have a responsibility to protect the data they gather from Internet users.
2. *Relational:* Two companies recognize that customers have a desire for privacy that needs to be met. Four companies view privacy protection as a means to winning customer trust.
3. *Instrumental:* One company states that it expects to gain a reputational advantage from its privacy program.

In het vorige hoofdstuk hebben we dit allemaal voorbij zien komen, waaronder; de argumenten waarin privacy als een *human right* gezien wordt (*moral*), de verantwoordelijk in de centrale stellingen (*moral* & *relational*) en online privacy presenteren als CSR en onderdeel van een *corporate image* (*relational* & *instrumental*). De onderwerpen die Pollach gevonden heeft hoeven natuurlijk niet altijd in een statemen verwerkt te worden, maar ze kunnen gebruikt worden om aanbevelingen te doen over hoe de onderwerpen verwoord kunnen worden.

5.1.4 Ethical information management

Ten slotte zijn enkle punten uit het boek *Ethical Data and Information Management: Concepts, Tools and Methods* van O'Keefe en O Brien (2018) gehaald. Punten die communicatie belichten van bedrijven als het gaat om online privacy. O'Keefe en O Brien beginnen met de noodzaak van ethisch verantwoord omgaan met data:

> Ethical information management and ethical decision making are increasingly

> being recognized as a competitive advantage in a competitive global market. Virtues and values such as trustworthiness, beneficence, fairness or justice, respect for privacy, and accountability promote good relationships between the organization and its stakeholders and sustainable business models. (O'Keefe en O Brien, 2018, p. 49)

Deze *virtues and values* zijn we al tegengekomen in de statements in het vorige hoofdstuk:

- *Trustworthiness:* u vertrouwt ons toe met uw data en wij gaan daar goed mee om omdat ....
- *Beneficence:* het wel of niet verzamelen van persoonsgegevens is goed voor onze bijdrage aan de samenleving omdat ...
- *Fairness or justice:* wij zien online privacy als een *human right*.
- *Respect for privacy:* wij begrijpen dat u zich zorgen maakt als het gaat om uw online privacy en wij gaan hier goed mee om omdat ...
- *Accountability:* wij zullen nooit persoonsgegevens verzamelen gezien deze technische maatregelen ...

Deze punten zijn al te vertalen naar onderwerpen die aan bod komen in privacystatements en kunnen daardoor gebruikt worden als aanbevelingen om een 'goed' statement te formuleren. Dit kan aangevuld worden met directe aanbevelingen die O'Keefe en O Brien doen als het gaat om communicatie over een *ethical framework* binnen een bedrijf (p. 164):

> The following steps are necessary to clearly determine and communicate the ethical framework for your organization:
>
> - Identify the priorities of the organization and desired behaviour in the organization.
> - Identify how the organizational ethic or priorities align with the larger societal ethical expectations.
> - Determine the desired outcomes and desired behaviour.
> - Ensure you have the tools to promote that outcome.

Uitwerkingen van de eerste drie punten zijn we al tegengekomen in de statements en het laatste punt is inherent aan het bestaan van de statements, het is immers een tool om met *stakeholders* te communiceren.

5.1.5 Een 'goed' privacystatement

Als we de aanbevelingen van de vakliteratuur samenvoegen, dan kunnen we de splitsing maken tussen *wat* er gezegd zou kunnen worden en *hoe* dat gezegd zou kunnen worden. Alles samen kan gezien worden als de *substantive and formal theory* uit de analyses:

Aanbevelingen voor onderwerpen die aan bod zouden kunnen komen in een privacystatements:

1. Hoe staat het bedrijf tegenover online privacy.
2. Welke data worden verzameld.
3. Hoe worden de data verzameld.
4. Waarom worden de data verzameld.
5. Waar worden de data voor gebruikt.
6. Wat is de impact van hetgeen waarvoor de data gebruikt worden op het bedrijf zelf en op de gebruikers.

Aanbevelingen voor hoe de onderwerpen verwoord zouden kunnen worden in een privacystatements:

1. Gebruik formuleringen en argumenten die de *relaties* met de *stakeholders* (gebruikers) bevorderen.
2. Bij het benaderen van de onderwerpen, houd rekening met het *vertrouwen* van de gebruikers in het bedrijf.
3. Toon *begrip & respect* voor de mogelijke zorgen van de gebruikers over online privacy.
4. Schets een beeld voor de *stakeholders* van hoe het bedrijf omgaat met online privacy in een *maatschappelijke setting*, dus breder dan de dienst zelf.

5.2 Interview

De *theory*, samen met algemene vragen over privacystatements, zijn voorgelegd aan universitair hoofddocent IT-recht prof. dr. J. H. Hoepman. Meneer Hoepman is, onder andere, gespecialiseerd in *privacy by design*, *privacy enhancing technologies* en *computer beveiliging*[11]. Er is toestemming gevraagd of het gesprek opgenomen mocht worden en of met naam geciteerd mocht worden, voor beide is toestemming gegeven. In dit geval was een formulier niet nodig, omdat meneer Hoepman in deze context geen proefpersoon is, dit punt is ook overlegd met de begeleider van deze scriptie. Op pagina 31 van de bijlagen is een transcript van het gesprek te vinden. Hier verwijzen de paginanummers achter de citaten ook naar. Voordat het interview plaatsvond, is nog mailcontact geweest waarin, onder andere, vermeld is welke uitleg van de term 'privacystatement' in deze scriptie wordt aangehouden.

Het interview begon met een algemene vraag of meneer Hoepman vindt dat een online dienst altijd een privacystatement zou moeten hebben, naast een privacy policy. Hier kwam een interessant punt naar voren dat meneer Hoepman het onderscheid maakt tussen een privacy policy en een privacystatement, als het gaat om wat naar buiten toe gecommuniceerd wordt. Een privacy policy is in dat geval een intern, juridisch document en wat naar buiten gebracht

[11] https://www.rug.nl/staff/j.h.hoepman/

wordt, wordt getypeerd als een privacystatement. Meneer Hoepman geeft ook aan dat die terminologie verschillend wordt toegepast, in de AVG wordt bijvoorbeeld geen onderscheid gemaakt tussen wat hier uitgelegd wordt als een privacystatement en privacy policy. Daar wordt dit allemaal aangeduid als privacy policy. In de rest van het gesprek zijn we echter uitgegaan van de uitleg van de Autoriteit Persoonsgegevens, die in dit onderzoek wordt aangehouden. Als het gaat om het hebben van een (leesbaar) privacystatement, naast een privacy policy, dan zegt meneer Hoepman:

> Ik denk dat je uiteindelijk allebei nodig hebt, dat je voor die mensen die het in detail willen weten dat uitgebreide document moet hebben en voor die mensen die grofweg willen kunnen inschatten wat er aan de hand is, dat er voor die mensen ook een document is. (p. 31)

Dit hoeven echter niet per se twee losse documenten te zijn:

> (...) dat kan ook in een gelaagde vorm zijn. Je kunt dus een privacystatement hebben wat heel begrijpelijk geschreven is, waarbij je dan door kunt klikken naar uiteindelijk de echte achterliggende lap tekst waar het volledige juridische ding in zit. (p. 31)

Ook de eerdergenoemde 'kritiek' die de Autoriteit Persoonsgegevens, Pollach (2011) en Shantz (2018) geven komt terug in het interview, namelijk dat "de gemiddelde gebruiker nooit, wat je dan een privacy policy noemt, [zal] doorlezen" (p. 32). Dit is ook een reden waarom meneer Hoepman het hebben van beide onderschrijft.

Qua onderwerpen die aan bod zouden moeten komen in een privacystatement vindt meneer Hoepman dat er "in moet staan welke gegevens je verzamelt, voor welk doel, voor hoe lang en met wie je ze deelt" (p. 32). Deze zijn we al tegengekomen in de statements, alleen voor hoe lang de gegevens bewaard worden is niet vaak genoemd. De bedrijven noemen dit hier en daar wel, maar bijna altijd met de vage formulering 'zo lang het nodig is', zie bijvoorbeeld pagina 80 of pagina 92.

Meneer Hoepman beaamde de bevinding uit dit onderzoek dat er veel verschillen bestaan tussen privacystatements:

> Ja dat is zo, er is een wereld van verschil in privacystatements, dat weet ik wel, ik heb wel eens gevraagd om een paar goede voorbeelden, maar daar heb ik nooit echt goede voorbeelden van gekregen. (p. 32)

Met het presenteren van de *theory* kwam het punt van 'het maatschappelijke aspect van online privacy benadrukken' naar voren, samen met het vermelden van hoe het bedrijf tegenover online privacy staat. Oftewel het 'online privacy als CSR' gedeelte:

> Ik kan me er wel iets bij voorstellen, als je daarmee begint in je privacystatement, dat je aangeeft hoe je er instaat. (...) Maar uiteindelijk gaat het er om dat, als er beslissingen beschreven staan, dat je die navolgt (...) Dat je die implementeert aan de hand van een bepaalde grondhouding, daar kan ik me iets bij voorstellen.

> Het zou niet bij mij opkomen als het belangrijkste van wat er in moet staan, maar, ja, ik snap het. (p. 33)

Wanner het gaat om het benadrukken van de relatie tussen het bedrijf en de gebruiker in het statement en het vertrouwen proberen te winnen, zegt meneer Hoepman het volgende:

> (...) het is niet bedoelt als reclame he. (...) Ja ik moet zeggen dat ik daar wel moeite mee heb hoor, het is zo'n grens, juist omdat je dat op twee manieren kunt gebruiken. Weet je, ik kan het me heel goed voorstellen (...), stel dat je op een landingspage zelf heel erg veel, als je dat belangrijk vindt, dat je zegt van 'wij vinden privacy belangrijk' of 'we zijn sustainable' of noem maar op. Maar dat als je uiteindelijk klikt op de link 'privacystatement' dat het dan toch vrij zakelijk en helder wordt uitgelegd wat je doet en waarom je het doet en wat nodig is en niet. Dat je probeert dat in zekere zin in neutrale termen te brengen (...) Ja het gaat twee kanten op (...) Laat ik het zo zeggen, bijvoorbeeld kan Shell wel claimen dat ze sustainable zijn, maar dat geloof ik niet. En weet je, een willekeurig ander bedrijf wat ik niet ken dat claimt dat het sustainable is, dan wil ik eerst wel zien waarom ze dat dan zijn. Met alleen roepen dat je het bent kom je er niet, dus dan kun je beter in zo'n statement helder maken 'waarom je het zo doet en waarom je het zo doet', in plaats van alleen maar van die meer marketing-achtige begrippen (...) Ik kan me heel goed voorstellen dat je dat in allerlei andere publicaties daar omheen doet, maar in het privacystatement zou ik dat niet doen eerlijk gezegd. (p. 35)

Meneer Hoepman geeft dus een soort waarschuwing dat te veel CSR uitingen (het roepen van de marketing begrippen) in de statements averechts kan werken, bijvoorbeeld als het gaat om het vertrouwen van de gebruikers. In Cornelissen komt dit ook terug:

> (...) if companies put too much spin on their CSR or communicate aggressively or excessively about their CSR, they may achieve the opposite from what they intended and be negatively perceived and evaluated by stakeholders. (Cornelissen, 2014, p. 367)

In de statements die we gezien hebben kan dit zeker een rol spelen, dit is echter buiten de scope van dit onderzoek, omdat het niet direct in de tekst te vinden is. Dit wordt in de discussie verder besproken.

Ten slotte kwam nog een voorbeeld van 'het benadrukken van de bredere context van online privacy' ter sprake; de bredere tips voor gebruikers om beter met hun privacy om te gaan. In de eerdere hoofdstukken zagen we dat dit vooral gedaan wordt door de bedrijven die geen gegevens verzamelen. De link tussen deze tips en het voorkomen in de statements werd uitgelegd vanwege het feit dat het, zelfbenoemde, 'privacybewuste' bedrijven zijn. Meneer Hoepman gaf hier nog een andere mogelijk oorzaak voor:

> (...) dat [voorkomen van die tips] heeft misschien ook te maken omdat je specifiek naar zoekmachines kijkt. (...) Want kijk, de grap is natuurlijk wel dat, een zoekmachine (...) is een toegang naar andere webdiensten en webpagina's. Ik

> kan me nog best wel voorstellen dat als je een zoekmachine hebt en je wilt een privacyvriendelijke zoekmachine maken, dat je je dan bewust bent van het feit van 'ja ik maak mijn eigen dienst wel privacyvriendelijk, maar op het moment dat je hier op een link klikt, die ik jou aanbied, dan kom je in het wilde westen terecht waar cookies worden geplaatst, dus daar moet ik je misschien voor waarschuwen'. Dus (...) in deze hele specifieke context kan ik me dat wel voorstellen (...) (p. 36)

Deze nieuwe insteek is mooie brug voor vervolgonderzoek, wat meneer Hoepman ook aanraadt. Bijvoorbeeld om te onderzoeken "of je dat verschil ook ziet [tussen] de privacystatements van zoekmachinebedrijven en de niet doorgeef-achtige diensten" (p. 36). Dit wordt in de dicussie verder toegelicht.

5.3 Terugblik

Met de *substantive and formal theory*, oftewel de aanbevelingen, geformuleerd aan de hand van experts en met de aanvulling van meneer Hoepman, kunnen we nu terugblikken op de statements uit hoofdstuk 4 (p. 11). We kunnen de aanbevelingen als maatstaf nemen en kijken wat de statements goed en niet goed doen. Dit zal niet een gedetailleerde analyse zijn, meer een *proof of concept*, waarbij de statements van de bedrijven kort worden beoordeeld. Op pagina 36 is de uitwerking hiervan te vinden.

6 Conclusies

De onderzoeksvragen voor dit onderzoek waren:

1. Wat staat er in de privacystatements van zoekmachinebedrijven?
2. Hoe verwoorden zoekmachinebedrijven de onderwerpen die aan bod komen in hun privacystatements?
3. Hoe kan een privacystatement voor zoekmachinebedrijven eruit zien volgens experts?

Voor de eerste onderzoeksvraag is door middel van argumentatieanalyse geprobeerd te typeren welke centrale stellingen en argumenten aan bod komen in de privacystatements. Hieruit kan geconcludeerd worden dat er veel verschillende onderwerpen genoemd worden in de verschillende statements. Twee onderwerpen kwamen in alle statements voor: het wel of niet verzamelen van persoonsgegevens en een technische uitleg over hoe persoonsgegens wel of niet verzameld worden.

De resultaten voor de tweede vraag zijn door een analyse op basis van persuasie- en *corporate social responsibility* theorie verkregen. Hier kan ook geconcludeerd worden dat er veel verschillen bestaan tussen de manier waarop de onderwerpen in de statements verwoord worden. Een duidelijk verschil in de statements is te zien tussen bedrijven die wel en geen

persoonsgegevens verzamelen. De bedrijven die geen persoonsgegevens verzamelen verwoorden dit allemaal als een essentieel onderdeel van hun bedrijf en doen dit door middel van *strategic messaging* om zo een duidelijk *corporate image* te schetsen waar online privacy een kernpunt van is. Van de bedrijven die wel persoonsgegeven verzamelen, vermelden drie van de zes aan het begin van hun statement hoe invloedrijk en belangrijk hun bedrijf is, de bedrijven die geen persoonsgegevens verzamelen doen dit niet. Bedrijven die geen persoonsgegevens verzamelen gebruiken relatief veel argumenten op basis van nadelen waar *fear appeals* in verwerkt zitten, terwijl de bedrijven die wel persoonsgegevens verzamelen bijna geen argumenten op basis van nadelen presenteren.

Voor de derde vraag is verschillende vakliteratuur geraadpleegd, wat gebruikt is om een *substantive and formal theory* te formuleren. Deze *theory* heeft de vorm van 'aanbevelingen voor een goed statement' gekregen. Deze aanbevelingen zijn voorgelegd aan universitair hoofddocent IT-recht prof. dr. J. H. Hoepman, samen met algemenere vragen over privacystatements.

Ten slotte zijn de bestaande statements vergeleken met de aanbevelingen om te kijken wat goede en minder goede punten zijn in de statements. De aanbevelingen, zie pagina 23, kunnen gezien worden als het antwoord op de derde onderzoeksvraag

7 Discussie

Er is geprobeerd zo goed en duidelijk mogelijk te verantwoorden waarom voor bepaalde methoden of insteken gekozen is, om de interne validiteit te waarborgen. Toch zit hier bij kwalitatief onderzoek altijd een mate van interpretatie en subjectiviteit bij, vooral bij de toegepaste methoden. De bestaande analysemethoden zijn niet een op een overgenomen, hier zit de interpretatie van de onderzoeker tussen om de methoden toepasbaar te maken op het materiaal. Dit maakt de generaliseerbaarheid van de conclusies en resultaten niet optimaal, de vraag hierbij is wel in hoeverre iets specifieks als 'een uitspraak over een privacystatement van een zoekmachinebedrijf' überhaupt generaliseerbaar is.

Het interview met meneer Hoepman is naast interesse, ook gehouden om de validiteit te verbeteren. Meneer Hoepman noemde veel dezelfde punten rondom 'wat er in de statements zou moeten staan', maar was sceptischer over 'online privacy als CSR'. De vakliteratuur en zijn mening kwamen niet altijd overeen, wat wijst op een noodzaak voor vervolgonderzoek.

Meneer Hoepman bracht ook waardevol punt naar voren in het interview, namelijk dat het mogelijk interessant is om in vervolgonderzoek te kijken naar de verschillen tussen de privacystatements van 'doorgeef-achtige diensten' (p. 36), zoals zoekmachinebedrijven en meer op zichzelf staande diensten, zoals webshops. Meneer Hoepman gaf als mogelijke uitleg voor de privacytips die de bedrijven gaven, dat ze links aanbieden van andere diensten en daarmee het 'wilde westen' openzetten voor de gebruiker. Dit is een interessante link die nog meer openingen biedt voor vervolgonderzoek. Wat valt er te ontdekken als privacystatements van verschillende soorten online diensten vergeleken worden?

De aanbevelingen zijn zo veel mogelijk los van de zoekmachinebedrijven opgezet, deze be-

drijven waren vooral een, in mijn ogen, geschikte groep om te bekijken. Dit omdat, zoals eerder gezegd, zoekopdrachten veel gevoelige informatie kunnen bevatten. In die zin zouden de zoekmachinebedrijven als een soort *worst case scenario* gezien kunnen worden en zijn de aanbevelingen juist goed toe te passen op privacystatements van andere online bedrijven. Dit is uiteraard speculatie en mogelijk vervolgonderzoek zou ook hier op zijn plaats zijn. Ook het testen van de aanbevelingen door een andere student of onderzoeker zou goed zijn om te zien of deze nog aangevuld en verbeterd kunnen worden.

Zoals we hebben gezien zijn er verrassend veel verschillen tussen de uitingen van de bedrijven, die in principe dezelfde soort dienst aanbieden. Het idee voor deze scriptie is ontstaan nadat ik de twee tegenovergestelde *human rights* argumenten van Startpage en Yandex had gelezen en ik verwachtte dat dat soort verschijnselen de grootste verschillen zouden zijn. Dat, onder andere, de complete opbouw, argumenten, onderwerpen en manier van verwoorden zo van elkaar zouden verschillen, had ik niet verwacht.

Naast de verschillen laten de resultaten zien dat 'online privacy' een zeer breed veld is wat op veel verschillende gebieden doorwerkt. Onderzoek in dit gebied zal naar mijn verwachting alleen maar in maatschappelijk relevantie toenemen, gezien de technische vooruitgangen die in rap tempo geboekt worden. Ik hoop dat dit onderzoek als een soort *case study* kan dienen om te laten zien wat er allemaal voor materiaal is.

REFERENTIES

Cornelissen, J. (2014). *Corporate Communication: A Guide to Theory & Practice*. Erasmus University: Sage Publications.

Desai, M. & von der Embse, T. (2008). Managing electronic information: an ethics perspective. *Information Management & Computer Security*, *16*(1), 20–27.

Hoeken, H., Hornikx, J. & Hustinx, L. (2009). *Overtuigende teksten: Onderzoek en ontwerp*. Bussum: Coutinho.

Karreman, J. & van Enschot, R. (2013). *Tekstanalyse: Methoden & Toepassingen*. Gorcum B.V., Koninklijke van.

Kawulich, B. B. (2004). Data Analysis Techniques in Qualitative Research. *Journal of Research in Education*, *14*(1), 96–113.

O'Keefe, K. & O Brien, D. (2018). *Ethical Data and Information Management: Concepts, Tools and Methods*. London: Kogan Page.

Pollach, I. (2011). Online Privacy as a Corporate Social Responsibility: An Empirical Study. *Business Ethics: A European Review*, *20*, 88–102.

Shantz, A. (2018). Big Data, Bigger Questions: Data-based Business Models and Their Implications for Organizational Boundaries, Data Governance, and Society, Toward Permeable Boundaries of Organizations? *Research in the Sociology of Organizations*, *57*, 305–329.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*, 63–75.

Sikolia, D., Biros, D., Mason, M. & Weiser, M. (2013). Trustworthiness of Grounded Theory Methodology Research in Information Systems. *MWAIS 2013 Proceedings*, *16*.

BIJLAGEN

TRANSCRIPT INTERVIEW

Transcript van het interview met prof. dr. J. H. Hoepman op 15 januari 2020. Voor het opnemen van het gesprek en het citeren met naam, is van tevoren toestemming gevraagd en deze is ook gegeven.

(Begin gesprek)

Wessel: Ik had u dat mailtje gestuurd over de privacystatements en wat ik versta onder de term privacystatements en dat ik heb gekeken naar wat er wordt gezegd en hoe dat wordt gezegd. Ik heb toen gekeken naar de literatuur om te kijken hoe een 'goed' privacystatement er misschien uit zou kunnen zien volgens expert literatuur en ik wil u eigenlijk mijn bevindingen daaruit voorleggen en dan kijken wat u daarvan vindt, of u dat ook een 'goed' statement vindt. Maar eerst een wat algemenere vraag; vindt u dat, als we weer het onderscheid maken tussen een privacystatement, dus het 'leesbare' document over privacy waar de gebruiker echt iets mee kan en een privacy policy echt als juridisch document, vindt u dan dat een online dienst, en dat hoeft niet in het bijzonder voor zoekmachines te zijn, maar vindt u dat een online dienst altijd een privacystatement zou moeten hebben, naast die privacy policy? Die privacy policy is eigenlijk altijd wel verplicht en ...

Meneer Hoepman: Ja, dat is wel grappig, het is een kwestie van terminologie. Ik zou, ja en AVG en dergelijke houdt daar ook niet echt rekening mee omdat zij ook de term 'privacy policy' gebruiken om naar buiten toe te communiceren ... Ik maak altijd onderscheid tussen datgene wat je aan privacybeleid hebt en daarmee de privacy policy binnen een bedrijf, dat kan heel erg uitgebreid zijn, waar je vervolgens over moet communiceren naar buiten toe, en dat noem ik dan een privacystatement, maar dat kan nog best een heel juridisch document zijn, maar ik noem dat nog steeds een privacystatement. En dat is dan wat in de context van de AVG dan een privacy policy genoemd wordt. Maar ik vind meer, het gaat om datgene wat gecommuniceerd wordt en dat kun je op een hele juridiche manier doen of een heel begrijpelijke manier doen. Ik denk dat je uiteindelijk allebei nodig hebt, dat je voor die mensen die het in detail willen weten, dat uitgebreide document moet hebben en voor die mensen die grofweg willen kunnen inschatten wat er aan de hand is, dat er voor die mensen ook een document is.

Wessel: Dus eigenlijk gewoon naast elkaar.

Meneer Hoepman: Ja, dat kan ook in een gelaagde vorm zijn. Je kunt dus een privacystatement hebben wat heel begrijpelijk geschreven is waarbij je dan door kunt klikken naar, uiteindelijk, het echte achterliggende lap tekst waar het volledige juridische ding in zit.

Wessel: O ja, want ik zag bij de ... in de scriptie heb ik aangehouden dat op de landingspagina van de zoekmachinebedrijven, dus gewoon de zoekdienst die ze aanbieden, dat ik daar dan de eerste beste link gewoon heb gepakt en dan zeg, dat neem ik als privacystatement, wat daar dan staat. Dus dat is dan zo'n link helemaal onderaan de pagina naar 'privacy' of 'privacyverklaring' of 'privacystatement' en dat dat dan een eerlijke vergelijking is, maar daar

zit dus nog wel ...

Meneer Hoepman: Daar kunnen dus twee links staan, als je pech hebt dan heb je er twee ...

Wessel: O ja, dat ben ik niet tegengekomen ...

Meneer Hoepman: Nee dat zal niet, maar het is wel mogelijk.

Wessel: ... er zat wel heel veel verschil in, van wat daar dan wordt gepresenteerd. Sommige hebben wel echt een heel lopend verhaal en andere een wat meer, nou, zoals de Autoriteit Persoonsgegevens zegt, dat hele leesbare document. Anderen hebben juist weer, nou, de vorm van een privacy policy. Maar u zou zeggen dat het wel goed is om beide wel te laten zien.

Meneer Hoepman: Nou kijk, uiteindelijk, een meer leesbaar privacystatement is natuurlijk niet juridisch bindend, maar legt wel uit wat er gebeurt, dus dat een bedrijf zich wel gaat houden aan wat ze beloven in een meer gedetailleerd juridisch document, een strikter beschreven document natuurlijk. Dus dat is dan een meer juridische privacystatement. Ik denk dat je uiteindelijk allebei nodig hebt, de gemiddelde gebruiker zal nooit, wat je dan een privacy policy noemt, doorlezen.

Wessel: Ja, en als we dan het 'leesbare' privacystatement, die term aanhouden, welke onderwerpen vindt u die daar dan in ieder geval in voor zouden moeten komen. Dus echt het leesbare document waar de gebruiker iets mee kan.

Meneer Hoepman: Ja weet je, ik kan er van alles over zeggen, maar het is niet mijn focus van dingen waar ik veel naar kijk, privacystatements en dat soort dingen, maar grofgezegd vind ik dat er in moet staan welke gegevens je verzamelt, voor welk doel, voor hoe lang en met wie je ze deelt.

Wessel: Ja, dat ben ik ook tegengekomen inderdaad, dat zijn wel de hoofdonderwerpen die voorbij komen. Maar er zijn ook, ik kwam bijvoorbeeld een bedrijf tegen die in het privacystatement waar ze naar linken bijvoorbeeld zeggen hoe ze omgaan met gegevens voor een sollicitatie en dat ze dat dan ook vermelden in dezelfde tekst van hoe ze met de gegevens uit de zoekdienst omgaan, maar dat ...

Meneer Hoepman: Ja dat zijn verschillende dingen.

Wessel: Ja, maar dus gewoon op de dienst zelf?

Meneer Hoepman: Ja, die informatie zou dan juist weer moeten staan op die plek waar je mensen gaat uitnodigen om te solliciteren, weet je wel, daar heb je dan een los privacystatement voor en daar staat dat dan weer in.

Wessel: Ja dat is ... ik vond ook een hele boel verschillende manieren ...

Meneer Hoepman: Ja dat is zo, er is een wereld van verschil in privacystatements, dat weet ik wel, ik heb wel eens gevraagd om een paar goede voorbeelden, maar daar heb ik nooit echt goede voorbeelden van gekregen. Volgens mij vinden mensen die van Coolblue wel redelijk, duidelijk in ieder geval, misschien een beetje popiopie.

Wessel: Ja, bij die zoekmachinebedrijven zijn inderdaad ook een paar die dat doen, die zetten dan ook helemaal vooraan van, 'nou wij zijn heel privacybewust' en dan, ja, 'we don't track you', 'it's your data not big data', ja zulke dingen.

Meneer Hoepman: Als dat dan uiteindelijk ook maar gesubstantieerd wordt in een privacy policy, dat moeten we dan zien.

Wessel: En of ze dat dan ook navolgen ...

Meneer Hoepman: Ja dat hoop je dan ook ...

Wessel: Ja en toen heb ik wat expert literatuur erbij gehaald en gekeken naar ... en dat was meer op de, ja ik schrijf mijn scriptie bij meer de Corporate Social Responsibility kant, dus meer het communiceren daarover, en ik heb dus meer literatuur gevonden op basis van data ethics en business ethics en in ieder geval hoe ze ermee om kunnen gaan. Niet heel erg de juridische kant, laat ik het zo zeggen, meer de aanbevelingen van hoe je dat als bedrijf kunt aanpakken. Die heb ik samengevoegd tot een soort 'aanbevelingen', zo noem ik het maar, wat er dan in een, tussen haakjes, goed statement zou kunnen staan. Dat wilde ik eigenlijk aan u voorleggen. Nou ja, wat u ook al zei van dat wat er in moet staan; dat er in elk geval staat welke data verzameld worden, hoe deze worden verzameld, waarom ze worden verzameld, waar worden ze voor gebruikt en dan wat meer specifiek, echt voor de bedrijven zelf ... ik vond in veel van de literatuur dat het goed is voor de bedrijven om zelf te omschrijven hoe zij tegenover online privacy in het algemeen staan. Ik was benieuwd of u denkt dat dat ook wel eentje is die, ja misschien niet per se nodig, maar wel eentje is die wel goed is om er in te noemen. Dus dat het wat breder getrokken wordt dan alleen privacy in de dienst zelf, maar ook dat het een meer maatschappelijk ...

Meneer Hoepman: Ja, dat is interessant, de vraag is 'wat betekent dat', want is dat 'wij vinden privacy belangrijk' zo'n soort statement?

Wessel: Bijvoorbeeld, ja, en dan uitgewerkt aan de hand van voorbeelden van 'wij vinden privacy belangrijk omdat we ...', nou bijvoorbeeld, die privacygerichte bedrijven zeggen dan 'wij vinden privacy belangrijk omdat wij dus geen persoonsgegevens verzamelen en geen data verzamelen', en die geven dan vaak ook nog een soort tips van hoe je verder op het internet en bij andere diensten het beter kunt doen. Dus meer dat het zo ook buiten die dienst zelf nog wordt toegelicht.

Meneer Hoepman: Ik kan me er wel iets bij voorstellen, als je daarmee begint in je privacystatement, dat je aangeeft hoe je er instaat. Uiteindelijk wordt het, ja, ik denk dat dat kan helpen. Maar uiteindelijk gaat het er om dat, als er beslissingen beschreven staan, dat je die navolgt, wat de dienst doet en dat je die navolgt. Dat je die implementeerd aan de hand van een bepaalde grondhouding, daar kan ik me iets bij voorstellen. Het zou niet bij mijn opkomen als het belangrijkste van wat er in moet staan, maar, ja, ik snap het.

Wessel: Ja ik ben het ook niet in alle tegengekomen, maar sommigen, die laten het wel heel duidelijk merken van, ja ...

Meneer Hoepman: Ja, Apple is bijvoorbeeld een goed voorbeeld van een bedrijf die daar heel duidelijk over communiceert, van 'privacy is belangrijk en daarom doen we dit en dit' en 'ons

business model is dit en dit', ja dat legt wat uit en dat doet ook wat.

Wessel: Ja, en dan dat dat niet alleen voor de gebruiker wordt uigelegd wat daar tegenover-staat, maar ook wat voor impact dat heeft voor het bedrijf zelf, dus wat u ook noemde, 'zo verdienen wij ons geld' of 'zo zorgen wij ervoor dat privacy gewaarborgt wordt'.

Meneer Hoepman: Ja, dat helpt natuurlijk, omdat je anders denkt 'ja hoe kunnen zij nou hun geld verdienen met' of weet ik veel, dus 'ze zeggen nu wel dit, maar', dus dat je wel op die manier aannemelijk maakt dat ze in hun privacystatement ook zeggen dat dat kan of hoe dat aan wordt gepakt, ja.

Wessel: Dus ook meer het vertrouwen wel ...

Meneer Hoepman: Ja. Ja, precies.

Wessel: Ja en het volgende van wat ik in die expert literatuur had gevonden, waren een soort aanbevelingen van hoe je het dan kunt verwoorden, ja de onderwerpen, dus meer hoe dat geformuleerd kan worden. Die benadrukten allemaal dat het ook belangrijk is om de relatie tussen de gebruiker en de dienst zelf dan op zo'n manier te verwoorden dat dat ook duidelijk is en een soort vertrouwen opwekt ...

Meneer Hoepman: Nou noem eens een voorbeeld dan, wat zou dat concreet betekenen als ze dat beschrijven, een goede manier van het beschrijven?

Wessel: Nou dat verschilt ook weer, ik zag echt een duidelijk verschil tussen de statements van bedrijven die wel gegevens verzamelen en niet. Voor bedrijven die gegevens verzamelen zou dat bijvoorbeeld 'doordat wij gegevens verzamelen kunnen wij een innovatieve dienst leveren' en aan de hand daarvan geven ze dan weer argumenten 'we maken levens beter van mensen, we zorgen hier en daarvoor' en allemaal zulke onderwerpen die daar dan bij worden gehaald. Maar die dus wel een soort van het vertrouwen van de gebruiker proberen te winnen. En die bedrijven die dus geen gegevens verzamelen, die deden dat vooral aan de hand van echt het uitleggen van hoe ze dan gedetailleerd die data niet verzamelen, dus van 'we doen extra ons best om dingen op die en die server uit te zetten op die en die manier' en sommigen gaan dan erg in detail en sommigen doen het meer met van die one-liners, popiopie, van 'we vezamelen niks' op die manier, maar wel ja, eigenlijk proberen ze allemaal, als het echt dat statement, dat leesbare document is, dan proberen ze vaak het vertrouwen te winnen van de gebruiker. En dat stond in die expert literatuur ook, maar ik dacht van, nou ja, wat vindt u daarvan? Is dat nog een, ook zo'n onderwerp wat nog wel, vindt u dat het echt een op een moet zijn van 'dit is de informatie en that's it', of mag daar, een beetje 'kneden van het publiek' wel bij zitten?

Meneer Hoepman: Ja precies, daar zat ik ook een beetje naar te kijken, het is niet bedoelt als reclame he.

Wessel: Nee, maar dat komt ook uit het onderzoek dat dat wel, als je dan vergelijkt met dat corporate social repsonsibility, dat wordt ook wel ingezet als een soort PR-achtig middel of een soort reclame en dat komt ook wel naar voren in die statements.

Meneer Hoepman: Ja ik moet zeggen dat ik daar wel moeite mee heb hoor, het is zo'n grens,

juist omdat je dat op twee manieren kunt gebruiken. Weet je, ik kan het me heel goed voorstellen dat je, stel dat je op een landingspage zelf heel erg veel, als je dat belangrijk vindt, dat je zegt van 'wij vinden privacy belangrijk' of 'we zijn sustainable' of noem maar op. Maar dat als je uiteindelijk klikt op de link 'privacystatement' dat het dan toch vrij zakelijk en helder wordt uitgelegd wat je doet en waarom je het doet en wat nodig is en niet. Dat je probeert dat, in zekere zin, in neutrale termen te brengen, ik zou daar niet . . . Ja het gaat twee kanten op, in het geval van een bedrijf als Facebook dan zeggen ze 'we gebruiken dat want we willen iedereen verbinden met elkaar', ja het verbinen is hartstikke mooi, maar het wekt aan de andere kant ook niet eens altijd vertrouwen op, zeker een privacyvriendelijk bedrijf, zeker als je het niet goed kent en zeker als niet goed beargumenteerd wordt waarom ze het op die manier doen, behalve dan met mooie termen. Laat ik het zo zeggen, bijvoorbeeld kan Shell wel claimen dat ze sustainable zijn, maar dat geloof ik niet. En weet je, een willekeurig ander bedrijf wat ik niet ken dat claimt dat het sustainable is, dan wil ik eerst wel zien waarom ze dat dan zijn. Met alleen roepen dat je het bent kom je er niet, dus dan kun je beter in zo'n statement helder maken 'waarom je het zo doet en waarom je het zo doet' in plaats van alleen maar van die meer marketing-achtige begrippen of, te vergrijpen, zou ik zeggen. Dus ik zou dat niet het belangrijkste, althans niet in het privacystatement zelf. Ik kan me heel goed voorstellen dat je dat in allerlei andere publicaties daar omheen doet, maar in het privacystatement zou ik dat niet doen eerlijk gezegd.

Wessel: Ja dus de manier van verwoorden moet echt wat meer informatief, neutraal . . .

Meneer Hoepman: Ja, informatief, neutraal, zou ik zeggen.

Wessel: En dit sluit daar wel op aan, dit is niet heel erg marketing, ik zag het niet erg als een marketing manier of marketing gestuurd, maar het was meer dat in die expert literatuur, maar ook statements zelf stond dat sommige bedrijven een heel beeld schetsen van, ja, dat het hele internet erbij wordt gehaald. Dus 'dit kun je doen om je privacy in het algemeen te verbeteren' en dat is niet zo zeer als marketing voor henzelf bedoeld, maar ik was benieuwd wat u daar van vindt, van dat dat ook in zo'n statement naar voren komt. Dat heeft in principe niet echt met de dienst zelf te maken en het wordt ook niet echt ingezet als een soort PR, marketing middel. Maar wat vindt u daarvan?

Meneer Hoepman: Nou ik ben dat eigenlijk nog nooit tegengekomen, heb je een concreet voorbeeld van een privacystatement waarin dat heel specifiek gebeurt, dat er echt andere dingen bij worden gehaald? Dat vind ik eigenlijk wel frappant.

Wessel: Nou ook weer vooral bij die privacybewuste zoekmachines dus Startpage, DuckDuckGo en Qwant die hadden dat vooral er in en Yandex had dat ook, maar dat is dan weer eentje die juist wel persoonsgegevens verzamelt, maar die geven van die tips van 'je kunt je cookies uitzetten' en allemaal zulke dingen komen daar nog in voor.

Meneer Hoepman: Ja, maar dat heeft misschien ook te maken met omdat je specifiek naar kijkt naar zoekmachines.

Wessel: Dat zou zeker kunnen.

Meneer Hoepman: Want kijk, de grap is natuurlijk wel dat, een zoekmachine geeft uitein-

delijk . . . is een toegang naar andere webdiensten en webpagina's. Ik kan me nog best wel voorstellen dat als je een zoekmachine hebt en je wilt een privacyvriendelijke zoekmachine maken, dat je je dan bewust bent van het feit van 'ja ik maak mijn eigen dienst wel privacyvriendelijk, maar op het moment dat je hier op een link klikt die ik jou aanbied, dan kom je in het wilde westen terecht waar cookies worden geplaatst, dus daar moet ik je misschien voor waarschuwen'. Dus dat kan in deze hele specifieke context kan ik me dat wel voorstellen dat dat gebeurt. Terwijl in een meer . . . in een andere context van laten we zeggen Facebook of iets dergelijks, een afgesloten dienst, dan ligt het minder voor de hand eigenlijk. Laten we zeggen, een willekeurige webshop of zo, dat is heel vreemd als daar nog weer dat soort dingen worden gezegd, dus dat kan daaraan liggen. Daar zou je naar kunnen kijken of je dat verschil ook ziet, de privacystatements van zoekmachinebedrijven en de niet doorgeef-achtige diensten. Dat lijkt me een verschil. In deze specifieke context kan ik het plaatsten, ja dat vind ik wel logisch, net zoals dat TOR ook, als je TOR installeert dan krijg je ook allemaal adviezen over wat je moet doen buiten TOR om 'ja weet je, je kunt TOR gebruiken maar als je dat en dat dan niet doet, dan ben je als nog fucked'. Dat hoort er dan een beetje bij, dat kan ik me in deze context ook wel voorstellen.

Wessel: Ja dat is een mooie insteek, die was bij mij nog niet opgekomen. Ik heb ook niet gekeken naar andere statements . . .

Meneer Hoepman: Zou je voor de grap eens naar kunnen kijken, of dat uitmaakt, eerlijk gezegd.

Wessel: Ja dat is wel een goeie, ergens voelt het ook wel wat misplaatst als je het dan, of als je het leest, of voor mij dan, niet op basis van die analyse, dat je dan denkt van ja, en ook dat gesuggereerd wordt dat andere diensten en zelfs ook andere zoekmachinediensten, die worden dan niet met naam en toenaam genoemd, maar wel van 'wij doen het zo en zo en wij gaan hier goed mee om, maar andere diensten die doen dat wel' of 'maar uw gegevens worden wel verkocht daar en daar'. Maar ik had meer de link gelegd tussen het privacybewust zijn, dat ze het daarom zeggen, maar het is inderdaad omdat het zoekmachines zijn, dat is inderdaad ook een logische verklaring.

Meneer Hoepman: Ja want anders is het niet logisch en ja dan nog, ja het zijn wel privacystatements.

(Afsluiting gesprek)

VOORBEELD TOEPASSING *theory*

- Ask
  - Goede punten: benoemt bijna alle onderwerpen die aan bod zouden moeten komen, behalve de impact die hun dataverzamelpraktijken hebben op gebruikers.
  - Minder goede punten: alleen in de centrale stelling is een van aanbevelingen over hoe de onderwerpen verwoord zouden kunnen worden verwerkt. De rest is opsommend en juridisch geformuleerd zonder de aanbevelingen.

- Bing
  - Goede punten: bijna alle punten die aan bod moeten komen worden genoemd. De beschrijving van de directe impact van de dataverzamelpraktijken voor de *stakeholders* is gedetailleerd.
  - Minder goede punten: hoewel de impact voor de *stakeholders* goed beschreven wordt, gaat deze alleen uit van de *stakeholders* als 'gebruikers van Bing'; het bredere maatschappelijke aspect komt nergens terug.
- DuckDuckGo
  - Goede punten: benoemt alle punten die aan bod zouden moeten komen en houdt ook rekening met manieren waarop deze verwoord zouden moeten worden.
  - Minder goede punten: het inspelen op het vertrouwen van de gebruiker wordt veel gedaan, maar hier worden veel technische details voor gebruikt, wat wellicht averechts werkt voor gebruikers die hier minder van af weten (dit is een aanname).
- Google
  - Goede punten: benoemt zeer gedetailleerd alle punten die aan bod zouden moeten komen, ook met veel aandacht voor de impact die de onderwerpen hebben op Google zelf en de gebruiker.
  - Minder goede punten: er worden veel redenen gegeven waar de verschillende persoonsgegevens voor gebruikt worden, dit kan ervoor zorgen dat het niet altijd duidelijk is waar wat voor gebruikt wordt.
- Qwant
  - Goede punten: benoemt alle punten die voor zouden moeten komen en schetst het bredere maatschappelijke aspect van online privacy vanuit verschillende oogpunten: juridisch, persoonlijk voor de gebruiker, andere online bedrijven en het internet in het algemeen. Ook de impact voor henzelf wordt vanuit veel punten belicht: waar halen ze hun inkomsten vandaan en wat voor gevolgen hebben hun keuzes voor hun bedrijfsvoering.
  - Minder goede punten: **geen duidelijke gevonden aan de hand van de aanbevelingen**.
- Startpage
  - Goede punten: noemt alle punten die genoemd zouden moeten worden. Ze geven veel details wanneer ze uitleggen hoe ze online privacy zien als bedrijf. Alle aanbevelingen voor het verwoorden komen ook naar voren, er is veel aandacht voor de *stakeholder relation* met de gebuiker.
  - Minder goede punten: sommige onderwerpen worden maar kort en oppervlakkig besproken, zoals de maatschappelijke impact van hun omgang met online

privacy of hoe ze precies sommige data verzamelen.

- Wolfram Alpha
  - Goede punten: benoemt in detail wat er gebeurt met de data die ze verzamelen.
  - Minder goede punten: niet alle onderwerpen die aan bod moeten komen worden genoemd; hoe het bedrijf tegenover online privacy staat ontbreekt. Ook wordt nergens aandacht besteed aan de impact van hun praktijken op zichzelf of op de gebruiker. Alleen de aanbeveling om te benadrukken begrip te hebben voor de zorgen die de gebruiker heeft rondom online privacy wordt gebruikt. Er wordt niets gedaan met de *stakeholder relation* tussen het bedrijf en de gebuikers. Ook wordt nergens online privacy breder getrokken buiten het bedrijf
- Yahoo
  - Goede punten: **geen duidelijke gevonden aan de hand van de aanbevelingen**.
  - Minder goede punten: welke persoonsgegevens worden verzameld en waar deze voor gebruikt worden zijn de enige onderwerpen die zeer kort naar voren komen uit de aanbevelingen. Niks uit de aanbevelingen over het verwoorden komt voor in het statement.
- Yandex
  - Goede punten: alle onderwerpen die opgenomen zouden moeten worden zijn in een lopende tekst, gedetailleerd opgenomen. Er is veel aandacht voor het maatschappelijke aspect van online privacy en hoe het bedrijf hier een rol in speelt. Er wordt veel gebruik gemaakt van het inspelen op het vertrouwen van de gebruikers en daarmee wordt de relatie tussen het bedrijf en de *stakeholders* ook vanuit verschillende punten benaderd.
  - Minder goede punten: **geen duidelijke gevonden aan de hand van de aanbevelingen**.

CENTRALE TELLINGEN EN ARGUMENTEN

ASK

Centrale stelling: We understand that your privacy is important to you, and we are committed to being transparent about the information we collect and process upon your use of our websites.

Argument: We laten onze gebruikers weten wanneer iets veranderd aan de manier waarop we informatie verzamelen.

Voorbeelden uit statement:

- We will provide notice in advance of the effective date with regard to any updates that materially change the ways in which we process your personal information.

- (...) advertiser and advertising networks, as well as data analytics companies who service them, may participate in online behavioral advertising and track your activity acrossvarious sites and/or devices where they display ads and record your activities, so they can show ads that they consider relevant to you. Where necessary, we will obtain your consent for these activities.

Argument: We geven onze gebruikers adviezen over verantwoord omgaan met persoonlijke gegevens.

Voorbeelden uit statement:

- There is no need to provide to us, and we strongly discourage you from, providing any perso-nally identifiable or sensitive information about you or anyone else including, details about your exact location, physical or mailing address, telephone number, race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership or information about your health.
- Our search results list and link to content that exits on web pages that are most likely not owned or controlled by us and the same or similar results are likely available through other search engines (e.g., Google, Yahoo! etc.). If content about you is included in search results displayed on our Sites, it only means that the information exists on the Internet and it doesn't mean that we endorse it or have the ability to remove content available on any other site and/or block such sites. To remove the content from the site linked to in the search results you should contact the owner of that site.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- Do Not Track (DNT) is an optional browser setting that allows you to express your preferencesregarding tracking by advertisers and other third-parties. However, we do not recognize or respond to browser-initiated DNT signals, as the Internet industry is currently still workingtoward defining exactly what DNT means, what it means to comply with DNT, and a common approach to responding to DNT.
- Lange lijst met voorbeelden, zie p. 52.
- Noemt het volgen van de regels van de GDPR.

Argument: De gebruiker heeft keuzes rondom zijn / haar data die wij verzamelen.

Voorbeelden uit statement:

- We only enable behavioral targeting with your consent where such consent is required.
- You can opt-out of third-party advertising-related cookies, pixel tags and web beacons, in which case our advertising partners should not deliver Interest/behavioral/targeted –based ads to you.
- You may opt out of tracking and receiving tailored advertisements on your mobile de-

vice by some mobile advertising companies and other similar entities by downloading the App Choices app

Argument: We nemen de beveiliging van de data van gebruikers serieus.

Voorbeelden uit statement:

- We use appropriate technical and organizational measures to protect your information against unauthorized or unlawful processing and against accidental loss, destruction or damage.
- We also limit access to information about you to employees who reasonably need access to it to provide products or services to you, or in order to do their jobs.

BING (MICROSOFT)

Centrale stelling: Uw privacy is belangrijk voor ons.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- Microsoft hanteert de principes van de Privacy Shield-raamwerken tussen de EU en de VS en Zwitserland en de VS.
- Microsoft verzamelt gegevens van u, via onze interacties met u en via onze producten. U verstrekt een aantal van deze gegevens rechtstreeks, terwijl sommige gegevens worden verkregen via het verzamelen van gegevens over uw interacties, gebruik en ervaringen met onze producten. Welke gegevens we verzamelen, is afhankelijk van de context van uw interacties met Microsoft en de opties die u kiest, zoals uw privacyinstellingen en de producten en functies die u gebruikt. We krijgen ook gegevens over u van derden.
- Lange lijst met voorbeelden: 60
- Noemt het volgen van de regels van de GDPR.

Argument: De gebruiker heeft keuzes rondom zijn / haar data die wij verzamelen.

Voorbeelden uit statement:

- U hebt keuzes wat betreft de technologie die u gebruikt en de gegevens die u deelt. Wanneer we u vragen om persoonsgegevens te verstrekken, kunt u dit weigeren.
- U kunt ook keuzes maken over het verzamelen en gebruiken van uw gegevens door Microsoft. U kunt uw persoonsgegevens die Microsoft heeft verkregen beheren en uw rechten met betrekking tot gegevensbescherming uitoefenen, door contact op te nemen met Microsoft of met behulp van verschillende hulpprogramma's die we bieden.
- Lijst met voorbeelden over de keuzes / controle die een gebruiker heeft: 61

DUCKDUCKGO

Centrale stelling: We don't collect or share personal information. That's our privacy policy in a nutshell.

Argument: We nemen maatregelen die zorgen dat de privacy van gebruikers gewaarborgt blijft (in tegenstelling tot andere zoekmachinebedrijven).

Voorbeelden uit statement:

- At other search engines, when you do a search and then click on a link, your search terms are sent to that site you clicked on (...). We call this sharing of personal information "search leakage."DuckDuckGo prevents search leakage by default. Instead, when you click on a link on our site, we route (redirect) that request in such a way so that it does not send your search terms to other sites. The other sites will still know that you visited them, but they will not know what search you entered beforehand.
- At some other search engines (including us), you can also use an encrypted version (HTTPS), which as a byproduct doesn't usually send your search terms to sites.
- At DuckDuckGo, our encrypted version goes even further and automatically changes links from a number of major Web sites to point to the encrypted versions of those sites.
- DuckDuckGo actually operates a Tor exit enclave, which means you can get end to end anonymous and encrypted searching using Tor & DDG together.
- Other search engines save your search history. & Also, note that with this information your searches can be tied together. This means someone can see everything you've been searching, not just one isolated search. You can usually find out a lot about a person from their search history.

GOOGLE

Centrale stelling: Wanneer u onze services gebruikt, vertrouwt u ons uw gegevens toe. We begrijpen dat dit een grote verantwoordelijkheid is en werken er hard aan om uw gegevens te beschermen en u er de controle over te geven.

Argument: De gebruiker heeft keuzes rondom zijn / haar data die wij verzamelen.

Voorbeelden uit statement:

- U kunt onze services op vele verschillende manieren gebruiken om uw privacy te beheren. U kunt zich bijvoorbeeld aanmelden voor een Google-account als u content (zoals e-mails en foto's) wilt maken en beheren of als u relevantere zoekresultaten wilt krijgen. U kunt veel Google-services ook gebruiken als u bent uitgelogd of zonder überhaupt een account te maken, zoals zoeken op Google of YouTube-video's bekijken. U kunt er ook voor kiezen privé te browsen op het web via Chrome in de incognitomodus. In al onze services kunt u uw privacyinstellingen aanpassen om te beheren wat we

verzamelen en hoe uw gegevens worden gebruikt.

- We hebben ook een plek ingebouwd waar u gegevens kunt bekijken en controleren die u heeft opgeslagen in uw Google-account. Uw Google-account bevat onder meer: Privacyopties Activiteitsopties
- Beheer uw voorkeuren over advertenties die aan u worden weergegeven op Google en op sites en apps die samenwerken met Google om advertenties weer te geven. U kunt uw interesses aanpassen, kiezen of uw persoonlijke gegevens worden gebruikt om advertenties relevanter voor u te maken en bepaalde advertentieservices in- en uitschakelen.
- Specifieke voorbeelden per dienst: 72
- Indien de gegevensbeschermingswetgeving van de Europese Unie (EU) van toepassing is op uw gegevens, bieden we de in dit beleid beschreven opties, zodat u gebruik kunt maken van het recht op inzage om uw gegevens te updaten, te wissen en de verwerking ervan te beperken. U heeft ook het recht om bezwaar te maken tegen de verwerking van uw gegevens of om de gegevens te exporteren naar een andere service.

Argument: We vertellen wat we doen met uw persoonlijke gegevens.

Voorbeelden uit statement:

- We delen persoonlijke informatie buiten Google als we uw toestemming hebben. Als u bijvoorbeeld een Google Home gebruikt om een reservering te maken via een boekingsservice, krijgen we uw toestemming voordat we uw naam of telefoonnummer delen met het restaurant. We vragen om uw uitdrukkelijke toestemming voordat we gevoelige persoonlijke informatie delen.
- Als u student bent of werkt voor een organisatie die gebruikmaakt van Google-services (zoals G Suite), hebben uw domeinbeheerder en resellers die uw account beheren toegang tot uw Google-account.
- We leveren persoonlijke gegevens aan onze partners en andere vertrouwde bedrijven of individuen zodat ze de gegevens voor ons kunnen verwerken, op basis van onze instructies en in overeenstemming met ons privacybeleid en andere passende vertrouwelijkheids- en beveiligingsmaatregelen. We maken bijvoorbeeld gebruik van dienstverleners om ons te helpen met klantenondersteuning.
- We delen persoonlijke gegevens buiten Google als we te goeder trouw van mening zijn dat toegang, gebruik, behoud of openbaarmaking van de gegevens redelijkerwijs nodig is (...)
- We kunnen niet-persoonlijke gegevens openbaar delen en met onze partners, zoals uitgevers, adverteerders, ontwikkelaars of houders van rechten. We delen gegevens bijvoorbeeld openbaar om trends te laten zien voor het algemene gebruik van onze services.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij

volgen.

Voorbeelden uit statement:

- Lange lijst met voorbeelden: p. 70 tot p. 70.
- We staan ook specifieke partners toe gegevens te verzamelen uit uw browser of van uw apparaat voor advertentie- en meetdoeleinden via hun eigen cookies of soortgelijke technologieën.
- Noemt het volgen van de regels van de GDPR.

Argument: We beschermen de informatie die we verzamelen goed.

Voorbeelden uit statement:

- We gebruiken versleuteling om uw gegevens privé te houden tijdens de overdracht. We bieden een reeks beveiligingsfuncties, zoals Safe Browsing, Beveiligingscheck en authenticatie in twee stappen om u te helpen uw account te beschermen.
- We evalueren onze handelswijzen op het gebied van verzameling, opslag en verwerking van gegevens, waaronder fysieke beveiligingsmaatregelen, om ongeautoriseerde toegang tot systemen te voorkomen.
- We beperken de toegang tot persoonlijke gegevens tot medewerkers van Google, contractanten en vertegenwoordigers die deze gegevens moeten kennen om ze te verwerken. Iedereen met deze toegang is onderworpen aan strenge contractuele vertrouwelijkheidsverplichtingen en kan worden bestraft of ontslagen als hij of zij niet aan deze verplichtingen voldoet.

QWANT

Centrale stelling: Qwant ensures that your privacy is protected, and this is the cornerstone of our philosophy.

Argument: We nemen maatregelen die zorgen dat de privacy van gebruikers gewaarborgt blijft.

Voorbeelden uit statement:

- We don't use any cookie nor any tracking device that may allow us to track your browsing habits or to establish your profile.
- We forbid ourselves from collecting an important amount of data that others collect, which are useless to provide you with the services you need. We never try to find out who you are or what you are personally doing when you use our search engine. When we do need to collect data, we do not disclose nor sell it for commercial or other uses. We use it exclusively to provide you with the services offered by Qwant.
- When you use Qwant as a search engine, we don't put any cookie on your browser that may allow us or others to recognize you or to follow you everywhere on the Internet. We

don't use any tracking device (pixel, fingerprinting...). We don't collect and we don't store any history or your searches. When you search, your query is instantly anonymized by being dissociated from your IP address, in accordance with what the French data controller advices. Long story short, what you are doing with Qwant is part of your privacy and we don't want to know.

- Qwant has a Privacy office dedicated to protecting your privacy. It also has a Data Protection Officer (DPO).
- We commit to do anything we can to ensure the security and confidentiality of our users personal data, including by preventing data damage, loss, or access by unauthorized third parties. Qwant's URL has the HTTPS header that shows users they communicate with Qwant through a secure channel using the TLS protocol. Technically, TLS ensures users that their data can't be intercepted by fraud. Moreover, the green lock that you see on most browsers when using Qwant certifies that you are browsing a secure website.
- (...) every ad that Qwant displays fully adheres to the values we defend and our quality standards. When you use Qwant, no personal information whatsoever is neither captured or transmitted to advertisers.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- Noemt het volgen van de regels van de GDPR.
- Qwant does not require any registration to use its search engine. However, you may want to register an account to sign-in and enjoy advanced functionalities such as the possibility to save search results in favorites, or create Boards. In such cases, we collect some personal data such as your name, firstname and email address.
- Qwant also collects connection data, not associated with your search queries, only to ensure the security of its information system and, if you create or modify Boards, to respect the obligation to identify content creators mandated by law.
- Even when you are connected with an ID, we don't use any cookie nor any other tracking device when you browse the site. The only technology that may be installed on your browser, called "local storage", is used to locally save your settings (language, activation or deactivation of options...). You can delete personal data stored in your "local storage" by deactivating cookies in your browser.
- Lijst met redenen: p. 79.
- For connection data, we do not collect directly identifiying information (we do not store your IP address). The information we process for user queries are a hashed IP address and approximate geolocation.

Argument: We zijn open over wat we doen met de gegevens die we verzamelen.

Voorbeelden uit statement:

- Personal data that you transmit are never disclosed or sold by Qwant to third parties, except for job applications that may be shared with recruiting partners, unless you ask us not to. Your data is stored on servers that belong to us and is never send to third-party technical parteners. Our host (as identified in our Terms) only provides a secure location for our servers, and can't access it.
- Users personal data is kept as long as you use the services provided by the site.

STARTPAGE

Centrale stelling: Startpage.com doesn't log or share your personal information. We don't track you. We don't profile you. Period.

Argument: We nemen maatregelen die zorgen dat de privacy van gebruikers gewaarborgt blijft.

Voorbeelden uit statement:

- Protecting your privacy is all about having control over your data. At Startpage.com, we help you control and protect what's yours: It's Your Data. Not Big Data! Why we don't collect any "personal data"? It's the best way to safeguard your privacy.
- Our definition of personal data is based on the privacy laws and regulations of the EU, including the General Data Protection Regulation (GDPR). These are widely regarded as the strongest privacy protections in the world. We consider any information about you or your behavior that can be traced back to you as personal data.
- We don't record your IP address.
- We don't serve any tracking or identifying cookies. This is about "good" and "bad" cookies. Cookies are small pieces of data that are sent to your hard drive by websites you visit. "Bad" cookies have unique elements that can track all kinds of personal information. We don't serve any of those. Startpage.com uses just one "good"cookie called "preferences" in order to remember the search preferences you choose. It's completely anonymous and expires after not visiting Startpage.com for 90 days.
- We don't record your search queries.
- Most online advertising today is personalized, meaning that online advertising services track what you do online and profile you in order to serve tailored ads. We don't do that at Startpage.com. No tracking. No profiling!
- We don't disclose or sell your contact information. When you contact us via email or through our support center, we'll use your contact information to respond to you. We won't sell or share this info with anyone else. You'll have the option to subscribe to our newsletter, from which you can unsubscribe at any time.

WOLFRAM ALPHA

Centrale stelling: Wolfram understands your concerns about how your information is used and shared, and we endeavor to use such information carefully and sensibly.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- We may collect both personally identifiable information about you and non-personally-identifiable information through your experience on our websites, from your use of our services and products, and via other voluntary contact with you (collectively "Services").
- The personally identifiable information we collect through our Services primarily consists of information you submit to us, including your name, email address and other personal information that you willingly provide. Because participation in our Services is voluntary, you have a choice of whether or not to disclose such information.
- In addition to information that you provide to us voluntarily, we receive some additional personally identifiable information and non-personally-identifiable information whenever you interact with our Services online, including your Internet Protocol (IP) address, browser type and version, referral URLs and other data automatically supplied by most common web browsers.
- We may also collect information from third-party sites (...)
- When you use our Services to connect to or access data from a third-party site ("TPS"), including but not limited to social networking sites, we may collect personally identifiable information about you from any TPS profile for which you give our Services access credentials. By authorizing these Services to access your TPS profile, you are authorizing us, in accordance with this Privacy Policy, to collect, store and use any and all information that your privacy settings at the TPS allow our Services to access through the TPS application programming interface ("API").
- Using Wolfram|Alpha, or utilizing the Wolfram|Alpha functionality within other Services, will trigger the collection of information about the specific query. Some queries may require collecting additional information.

Argument: We zijn open over wat we doen met de gegevens die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- Your IP address is used to determine, when possible, your approximate geographical location, which affects the computations or outputs provided by our Services for such things as default currency and units of measure based on what country you are in. Your browser type may be used to optimize your display, for example on mobile devices or to work around limitations of a particular browser. Referrer URLs may be used to generate

usage statistics and analyze usage patterns.

- If you provide your email address to us, we may email you in response, as well as notify you of other offers or services that may be of interest.
- We do not sell, rent, trade or lease your information to third parties. Any information we share shall be subject to the parameters associated with your requested Services and preferences.
- When we share personal information, we require the recipient to protect your personal information in compliance with the law. Wolfram may share information with affiliates, partners, service providers, authorized resellers and distributors and relevant third parties.
- Any collected information (personal and non-personal) associated with your use of our Services may also be subject to disclosure to government authorities or other authorized third parties pursuant to a lawful request, subpoena or other process that legally compels disclosure of that information.
- Noemt het volgen van de regels van de GDPR.

Argument: De gebruiker heeft keuzes rondom zijn / haar data die wij verzamelen.

Voorbeelden uit statement:

- To opt out of cookies that allow information to be delivered to you, such as targeted (or ïnterest-based") advertising, via third-party ad groups we may work with, there are options for controlling the ads you receive. Please note, however, that opting out does not prevent you from seeing the ads; it only makes them less relevant or tailored to your interests.

YAHOO

Centrale stelling: Niet aanwezig.

Omdat Yahoo geen centrale stelling heeft, worden alleen de onderwerpen besproken.

Onderwerp: Informatie de verzameld wordt.

Voorbeelden uit statement:

- When you conduct a search on a product or service that uses our search technology, we collect information from your experience, such as your search queries.
- Some advertising you receive may be customized based on your searches or related terms at Verizon Media.
- We may share your search query, IP address, and other depersonalized information from your web browser or app, such as a unique identifier for your web browser, with these search partners.

Onderwerp: Controle die de gebruiker heeft over verzameling van persoonlijke gegevens.

Voorbeelden uit statement:

- Please visit our Opt-Out page to learn more about the information used to personalize your search experience. If you opt-out, you will continue to see ads Verizon Media serves on these websites, but they won't be customized to your interests or search history.
- Visit the Search Preferences page to manage your Yahoo Search experience, including Safe Search, Search History, and Private Results.

YANDEX

Centrale stelling: For over twenty years, Yandex has served millions of users, working to maintain their trust through our commitment to protecting their privacy and freedom of expression online. Our commitment to users is rooted in Yandex's wider responsibility to respecting human rights.

Argument: We zijn open over de informatie die we verzamelen en de regels die we daarbij volgen.

Voorbeelden uit statement:

- Users are different, and data such as their preferences, location, and online history is critical to provide them with the best possible services. To that end, our services take into account various types of relevant data to personalise the experience for each user.
- Similarly, a user's search history helps Yandex choose the most relevant search results specifically for that user.
- We collect user data in two main ways – through Yandex profiles that users create and through users' interactions and activities on Yandex services.
- Yandex services automatically collect technical information such as cookie files, IP addresses, and geographic location to better understand users' preferences and settings.

Argument: We zijn open over wat we doen met de gegevens die we verzamelen.

Voorbeelden uit statement:

- Personalising a user's experience using historical data improves both the current experience and helps Yandex to develop new products and services. And the more data we utilize, the better the experience we can provide to our users.

Argument: We beschermen de informatie die we verzamelen goed.

Voorbeelden uit statement:

- Yandex takes your data security very seriously and follows rigorous data protection rules to ensure our users' data is secure and their privacy is protected. All data is processed automatically in our system, and we prohibit access to the data by any individual

other than in times of necessity such as for Yandex customer support or other obligatory administrative and technical help. We also always encrypt all stored confidential information, such as passwords.

- Our technological infrastructure securely protects the data that we handle. We implemented a secure HTTPS protocol for all Yandex services, meaning all data is encrypted as it moves between the user and Yandex.

Argument: De gebruiker heeft keuzes rondom zijn / haar data die wij verzamelen.

Voorbeelden uit statement:

- It's vital to Yandex to provide our users with information about how they can control and manage their personal data. Users can view part of the data, including personal information, available to Yandex and its services on Yandex.Passport. You can edit or delete this information, or change the settings of your personal Yandex account, at any point.

PRIVACYSTATEMENTS

Verzameld op: 4 november 2019. Toegevoegd in alfabetische volgorde. De link naar het statement staat bovenaan vermeld.

ASK

Bron: https://nl.ask.com/privacy

Ask Media Group Privacy Policy

Last Updated On: August 9, 2019

Ask Media Group LLC, ("AMG"), directly or indirectly operates Ask.com, as well as Reference.com, Life123.com, Consumersearch.com, Shop411.com, and many other sites offering search services and everyday useful content (click here for more info about other AMG sites). We understand that your privacy is important to you, and we are committed to being transparent about the information we collect and process upon your use of our websites. This Privacy Policy describes our practices concerning the personal information collected, processed and stored by AMG when you visit and use websites operated by AMG ("Sites").

If you are accessing the ask.com site via a downloadable application, you are using a service offered by AMG's affiliated business Ask Applications and this privacy policy is applicable.

Below we describe what information we collect when you use our Sites, how we protect that information, how long we retain it, with whom we share it, and what your privacy options are. By using the Sites, you consent to our collection and use of your information as described in this Privacy Policy. Information about our use of cookies and how you can change your cookie settings can be found here.

- Introduction and Scope
- Information Collected and Means of Collection
- How we Use your Information
- How we Share your Information
- Your Privacy Choices
- Security
- Retention
- Access, Review, Revision & Deletion Rights
- International Transfer
- Privacy Shield Participation
- Your California Privacy Rights
- Nevada Privacy Rights
- Contact Information

1) INTRODUCTION AND SCOPE

AMG operates the Site from the United States of America and, regardless of your place of residence or access location, your use of the Sites is governed by the laws of the State of California, USA. Users who access or use the Sites from other locations consent to the transfer and processing of their data in the United States of America and any other jurisdiction throughout the world.

This Privacy Policy is provided in English. Translations to certain other languages may be available and can be requested by contacting us here.

Our Sites are intended for general audiences over the age of 16 years old. We do not knowingly collect information from children under the age of 16 years old. IF YOU ARE NOT AT LEAST 16 YEARS OLD, DO NOT USE THE SERVICES.

We will continue to evaluate this Privacy Policy against new technologies, applicable laws, business practices, and our user's needs, and may make changes accordingly. Please check this page periodically for updates. If we make any material changes, we will post the updated Privacy Policy here, along with its effective date, and notify you by email or by means of a notice on the Sites. Except in connection with updates that materially change the ways in which we process your information, your continued use of the Services after our posting of changes to this Privacy Policy means that you agree to be bound by such changes. We will provide notice in advance of the effective date with regard to any updates that materially change the ways in which we process your personal information.

The Sites may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data

about you. We do not control these third-party websites and are not responsible for their privacy practices.

2) INFORMATION COLLECTED AND MEANS OF COLLECTION

We collect information about you from you directly providing it to us (e.g., when you contact us), from cookies and other tracking technologies that automatically collect information in the course of your use of the Sites (Learn more about these trackers in our Cookie Policy) and we may also collect information about you from third parties with whom we contract.

Information you provide directly to us. Access to web search results or other general content on our Sites does not require you to provide us any identification (e.g., name, date of birth), contact (e.g., email address, phone number) and/or account (username and password) information.

You may provide personal information to us, if you choose to request to receive certain communications from us, submit a help request, a customer service inquiry or other inquiry to us, or contact us about employment opportunities posted on the Sites.

There is no need to provide to us, and we strongly discourage you from, providing any personally identifiable or sensitive information about you or anyone else including, details about your exact location, physical or mailing address, telephone number, race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership or information about your health.

Information collected via automated technologies and interactions. As you interact with the Sites, we may collect information via automated means about your browser, you computer or device, your preference settings, your location and your activities, including:

IP address of your computer (which helps us identify your general location); Technical information about your computer or mobile device such as type of device, mobile device ID number, screen resolution, web browser information and operating system or platform; Your preferences and settings (time zone, language, etc.); Internet provider or mobile carrier name; The URL of the webpage you were visiting when clicking to our Site; Information about your activity on the Services (e.g., your search queries, mis-formatted DNS entries, search results selected, clicks, pages viewed, search history, comments, time spent on our Sites, return visits).

Third-parties who provide us with products and services may also place cookies, ad tags and/or beacons that collect the information outlined above in order to provide us with products and services including:

Analytics tools (e.g., Google Analytics) allowing us to analyze the performance of our Services; Service features and functionalities such as those that enable videos to be played and you to connect to your social media accounts; Advertisers and ad networks allowing the delivery of targeted advertisements.

These third parties may also collect information about you from other sources and combine it with other information collected about you from third party websites not affiliated with us.

For example, advertiser and advertising networks, as well as data analytics companies who service them, may participate in online behavioral advertising and track your activity across various sites and/or devices where they display ads and record your activities, so they can show ads that they consider relevant to you. Where necessary, we will obtain your consent for these activities.

Do Not Track (DNT) is an optional browser setting that allows you to express your preferences regarding tracking by advertisers and other third-parties. However, we do not recognize or respond to browser-initiated DNT signals, as the Internet industry is currently still working toward defining exactly what DNT means, what it means to comply with DNT, and a common approach to responding to DNT. However, our Cookie Policy provides information and opt-out links to help you can control the collection of information about you on our Sites.

3) HOW WE USE YOUR INFORMATION

We may use information relating to you for the following purposes:

Provide our services: we process your personal information to provide our web search and content services. This is so we can comply with our contractual obligations to you. We also use your browser information to recognize you as a returning visitor, or as the same user using other sites operated by AMG.

Improving our services: we analyze information about how you use our Sites to provide an improved experience for our users, including product testing and site analytics. It is in our legitimate business interests to use the information provided to us for this purpose, so we can understand any issues with our Sites and improve them.

Compensating our partners: we process your personal information for purposes of calculating compensation to be paid to our third party product/service providers and distributors and to analyze usage across products, services and distribution partner/channel. It is in our legitimate interest to appropriately determine amounts to be paid to our partners and inform our product roadmap and distribution strategy;

Communicating with you: we may use your personal information when we communicate with you, for example if we are providing information about changes to the terms and conditions or if you contact us with questions. It is in our legitimate interests that we are able to provide you with appropriate responses and provide you with notices about our Sites and services.

Marketing: we may use your personal information to deliver relevant advertisements to you to promote our Sites, and measure the effectiveness of our marketing campaigns. It is in our legitimate interest to analyse interests of our users to craft more relevant advertising messages and inform our marketing strategy. We may use automated decision-making to deliver tailored advertisements based on your personal information. In most cases, we use cookies and trackers placed on your browsers by our marketing network partners, such as Facebook.

Exercising our rights: we may use your personal information to exercise our legal rights where it is necessary to do so, for example to detect, prevent and respond to fraud claims, intellectual property infringement claims or violations of law or our Terms of Service.

Complying with our obligations: we may process your personal information to, for example, carry out fraud prevention checks or comply with other legal or regulatory requirements, where this is explicitly required by law, such as responding to your request for data access or deletion.

Customizing your experience, including ads: when you use the Sites, we may use information about your use of the Sites (queries you submitted, content you viewed) to customize your experience, such as by providing personalized elements and showing you content based on your recent interests. We may use automated decision-making for these activities. Upon your affirmative consent or request, we may use your browser information to send you notifications about content on our site via your browser. Where necessary, we will obtain your consent for these activities.

We may also aggregate your information with information of our other users, in such a way that you may not reasonably be identified by us or anyone else, and we may use any such aggregate information for any purpose.

4) HOW WE SHARE YOUR INFORMATION

We share your information in the following ways:

Our suppliers, subcontractors and business partners ("service providers"): we may share your information with our service providers who process your personal information to provide us with products and services as described above. Group Companies: we may share your information with our affiliates, which are entities under common ownership or control of our ultimate parent company, IAC/InterActive Corp for security, internal reporting and regulatory compliance, and to help our affiliates improve their products and services. Fraud prevention: we may disclose your information when we believe disclosure is necessary to investigate, prevent, or respond to suspected illegal or fraudulent activity or to protect the safety, rights, or property of us, our users, or others. Law enforcement purposes and public safety: if requested or required by government authorities, such as law enforcement authorities, courts, or regulators, or otherwise to comply with the law, we may disclose any information we have about our users. We may disclose information collected about you in order to exercise or protect legal rights or defend against legal claims. We also may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. Sale or merger of our business: we may transfer your information to a third party if we or any of our affiliates are involved in a corporate restructuring (e.g., a sale, merger, or other transfer of assets). Advertisers and advertising networks: advertisers and advertising networks place ads (including sponsored links in search results) on our Sites. These companies may collect information, such as your computer's IP address, browser information, mobile device ID, and search queries, as you use our Sites. They also may use cookies and other technologies to collect this information when you visit our site as described in our Cookie Policy. Social Media Platforms. The social media features in the Sites (like the Facebook "Like" or "Share" button) may allow the third-party social media providers to collect your IP address, which page of the Sites you're visiting, and other information relating to your use of our Sites, and to set a cookie to enable such social

sharing feature. Your interactions with these features are governed by the privacy policy of the social sharing platform.

We require all third parties to respect your privacy and to treat your information in accordance with the law. We only permit third parties to process your personal data for specified purposes and in accordance with our agreements with them.

In cases of onward transfer to third parties of data of EU or Swiss individuals received pursuant to the EU-US or the Swiss-US Privacy Shield, AMG is potentially liable.

5) YOUR PRIVACY CHOICES

You have choices when it comes to the privacy practices described in this Privacy Policy. A few of those choices are set forth below and others are available in our Cookie Policy.

Choices relating to information we collect. We may be required by law to collect certain personal information about you or as a consequence of any contractual relationship we have with you. Failure to provide this information may prevent us from providing certain Services or all of the Services to you. Online Behavioral Advertising. We only enable behavioral targeting with your consent where such consent is required. You can opt-out of third-party advertising-related cookies, pixel tags and web beacons, in which case our advertising partners should not deliver Interest/behavioral/targeted –based ads to you. You will continue to see advertisements on our Sites, but they will not be tailored to you based on any past behavior on the internet. You can choose to opt-out through these (and other) resources: Network Advertising Initiative (http://www.networkadvertising.org/) Digital Advertising Alliance (http://www.aboutads.info/consumers) Your Online Choices (http://www.youronlinechoices.com/) You may however still receive customized content and/or ads based on the search queries you submitted or the content of the pages you are visiting. Advertising on Mobile Devices. You may opt out of tracking and receiving tailored advertisements on your mobile device by some mobile advertising companies and other similar entities by downloading the App Choices app at https://youradchoices.com/appchoices.

6) SECURITY

We take the security of your information seriously and use appropriate technical and organizational measures to protect your information against unauthorized or unlawful processing and against accidental loss, destruction or damage. We also limit access to information about you to employees who reasonably need access to it to provide products or services to you, or in order to do their jobs. However, because no security system can be 100% effective, we cannot completely guarantee the security of any information we may have collected from or about you.

7) RETENTION

We retain the information we collect about and from you for as long as necessary to fulfill the purpose we collected it for and for the purpose of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal information we process, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your information, the purposes for

which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, accounting, or reporting requirements.

In some circumstances we may aggregate and de-identify your information in such a way that you may not reasonably be re-identified by us or any other company in which case we may use this information indefinitely without further notice to you.

In some circumstances you can ask us to delete your data: see ACCESS, REVIEW, REVISION & DELETION RIGHTS below for further information.

8) ACCESS, REVIEW, REVISION & DELETION RIGHTS

If you would like to access, review, revise or delete personal information we have collected from you, please contact us here.Your specific rights regarding access, review, revision or deletion your information is prescribed by local laws. Specific applicable local laws may be outlined below.

Note regarding Search Results. Our search results list and link to content that exits on web pages that are most likely not owned or controlled by us and the same or similar results are likely available through other search engines (e.g., Google, Yahoo! etc.). If content about you is included in search results displayed on our Sites, it only means that the information exists on the Internet and it doesn't mean that we endorse it or have the ability to remove content available on any other site and/or block such sites. To remove the content from the site linked to in the search results you should contact the owner of that site.

Legal rights applicable to personal data collected in the EEA. Pursuant to the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR") natural persons (called data subjects) are afforded certain rights regarding their personal data, including the right to access, correct, delete, restrict or object to our use of, and receive a portable copy in a usable electronic format of your personal information. You also have the right to withdraw any consent that you have previously provided to us.

If you would like to exercise any of the rights described above, and the law of your jurisdiction requires us to honor that request, please please make your request here. To assist us in processing your request in a timely manner, please make your request in English if you are able to do so. Unless you have voluntarily provided to us any other information about you, the only information we collect and store is linked to a unique user identification number we have assigned to you via a cookie placed on your browser. Please click the button below to get your unique user identification ("User ID") number.

Upon submitting your request to access or delete information we store about you, please provide your User ID number. This will enable us to process your request.

To help us prevent fraudulent removal requests, please also include a legible copy of a document that verifies your identity. You need not provide a government-issued document; a utility bill or similar mailing will suffice. Please also obscure parts of the document such as identifying numbers so long as the document continues to clearly identify you. If you are requesting the removal of search results that contain photographs of you, please ensure that the identifying document includes your photograph. If you are making the request on behalf

of another person, please indicate your relationship to that person and provide evidence of your authority to make such request. All requests for removal will be reviewed by AMG's legal and compliance team and we reserve the right, in compliance with applicable laws, to accept or reject, or make further inquiries regarding, any requests.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

We are committed to working with you to obtain a fair resolution of any complaint or concern about privacy. If, however, you believe that we have not been able to assist with your complaint or concern, you may have the right to make a complaint to the data protection authority of your country of residence.

9) INTERNATIONAL TRANSFER

If you are receiving the Services from outside the United States, your data will be transferred to and stored in our servers in the U.S. By using the Services, you consent to our collection and use of your data as described in this Privacy Policy.

Further, if you are receiving the Services from the European Economic Area (the "EEA") your information may be transferred to, stored, and processed in a country that is not regarded as providing the same level of protection for personal information as the laws of your home country, and may be available to the government of those countries under a lawful order made in those countries. However, whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

Model Contracts. Where appropriate, we put in place specific contractual commitments in accordance with applicable legal requirements to provide adequate protections for your information. For further details, see European Commission: Model contracts for the transfer of personal data to third countries. Privacy Shield. We may also transfer data to the U.S. under the Privacy Shield framework which requires them to provide similar protection to personal data shared between the EU and the US.

10) PRIVACY SHIELD PARTICIPATION

We comply with the EU-US Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union and Switzerland to the United States, respectively. Ask Media Group has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms of this Privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view Ask Media Group, LLC please visit

https://www.privacyshield.gov/

In compliance with the EU-US and Swiss-US Privacy Shield Principles, we commit to resolve complaints about your privacy and our collection or use of your personal information. European Union or Swiss individuals with inquiries or complaints regarding this privacy policy should first contact us at the address set forth here.

We have further committed to refer unresolved privacy complaints regarding the Site or mobile applications under the EU- US and Swiss-US Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, a non-profit alternative dispute resolution provider located in the United States and operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed by us, please visit the BBB EU PRIVACY SHIELD website at www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Please note that if your complaint is not resolved through the channels listed in this Privacy Policy, under limited circumstances, a binding arbitration option may be available before a Privacy Shield Panel.

Ask Media Group, LLC is further subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

11) CALIFORNIA PRIVACY RIGHTS

Under the California Civil Code, California residents have the right to request a list of all third parties to which a company conducting business in California has disclosed personal information during the preceding year for direct marketing purposes. Alternatively, the law provides that, if a company has a privacy policy that gives either an opt-out (which we may sometimes refer to as ünsubscribe") or opt-in choice for use of your Personal Information by third parties (such as advertisers or affiliated companies) for marketing purposes, the company may instead provide you with information on how to exercise your disclosure choice options. If you are a California resident and request information about how to exercise your third party disclosure choices you must send a request to the following address with a preference on how our response to your request should be sent (email or postal mail). Contact us here, or you may contact us via regular mail at: Ask Media Group, LLC, 555 12th Street, Suite 300, Oakland, CA 94607, Attn: Your California Privacy Rights c/o Data Protection Office. All requests sent via regular mail must be labeled IJour California Privacy Rightsön the envelope or postcard and clearly stated on the actual request. For all requests, please include your name, street address, city, state, and zip code (your street address is optional if you wish to receive a response to your request via email. Please include your zip code for our own recordkeeping).

12) NEVADA PRIVACY RIGHTS

Under Nevada law, Nevada residents may opt out of the sale of certain “covered information” collected by operators of websites or online services. We currently do not sell covered information, as “sale” is defined by such law, and we don’t have plans to sell this information.

13) CONTACT INFORMATION

If you have any questions or concerns about this Privacy Policy or the manner in which your information is processed (or if you are an EEA resident, how your data is transferred outside of the EEA), or if you would like to submit a request to us, please contact our Data Protection Officer here or via mail at: Ask Media Group, LLC Data Protection Officer 555 12th Street, Suite 300 Oakland, CA 94607

BING

Bron: https://privacy.microsoft.com/nl-nl/privacystatement

Uw privacy is belangrijk voor ons. In deze privacyverklaring wordt uitgelegd welke persoonsgegevens Microsoft verwerkt, hoe Microsoft deze verwerkt en voor welke doeleinden het bedrijf deze verwerkt.

Microsoft biedt een breed scala aan producten, waaronder serverproducten die wereldwijd worden gebruikt om ondernemingen te ondersteunen, apparaten die u thuis gebruikt, software die studenten op school gebruiken en services die ontwikkelaars gebruiken voor het maken en uitvoeren van wat er komen gaat. Verwijzingen naar Microsoft-producten in deze verklaring hebben betrekking op services, websites, apps, software, servers en apparaten van Microsoft.

Lees de productspecifieke informatie in deze privacyverklaring, met aanvullende relevante informatie. Deze verklaring heeft betrekking op de communicatie tussen u en Microsoft, de hieronder vermelde Microsoft-producten en op andere Microsoft-producten waarvoor deze verklaring wordt weergegeven.

- Persoonsgegevens die we verzamelen
- Hoe we persoonsgegevens gebruiken
- Redenen waarom we persoonsgegevens delen
- Toegang krijgen tot uw persoonsgegevens en deze beheren
- Cookies en soortgelijke technologieën
- Producten die worden geleverd door uw organisatie – kennisgeving aan eindgebruikers
- Microsoft-account
- Andere belangrijke privacyinformatie
- Productspecifieke details:
- Producten voor ondernemingen en ontwikkelaars
- Productiviteits- en communicatieproducten
- Zoeken en kunstmatige intelligentie
- Windows

- Entertainment en verwante services
- Microsoft Health-services
- Cookies

De meeste websites van Microsoft gebruiken cookies, kleine tekstbestanden die op uw apparaat worden geplaatst en die later kunnen worden opgehaald door webservers in het domein dat de cookie heeft geplaatst. We gebruiken cookies om uw voorkeuren en instellingen op te slaan, hulp te bieden bij het inloggen, doelgerichte reclame te bieden en de activiteiten op de site te analyseren. Raadpleeg voor meer informatie de sectie Cookies en soortgelijke technologieën van deze privacyverklaring. Privacy Shield tussen EU en VS en tussen Zwitserland en VS

Microsoft hanteert de principes van de Privacy Shield-raamwerken tussen de EU en de VS en Zwitserland en de VS. Voor meer informatie: ga naar de Privacy Shield-website van het Amerikaanse ministerie van handel.

Contact opnemen

Als u een vraag of klacht over privacy hebt voor de Chief Privacy Officer van Microsoft of de Functionaris Gegevensbescherming van de EU, neemt u contact met ons op via ons webformulier. Voor meer informatie over hoe u contact opneemt met Microsoft, waaronder Microsoft Ireland Operations Limited, leest u de sectie Contact met ons opnemen van deze privacyverklaring.

Persoonsgegevens die wij verzamelen

Microsoft verzamelt gegevens van u, via onze interacties met u en via onze producten. U verstrekt een aantal van deze gegevens rechtstreeks, terwijl sommige gegevens worden verkregen via het verzamelen van gegevens over uw interacties, gebruik en ervaringen met onze producten. Welke gegevens we verzamelen, is afhankelijk van de context van uw interacties met Microsoft en de opties die u kiest, zoals uw privacyinstellingen en de producten en functies die u gebruikt. We krijgen ook gegevens over u van derden.

Als u een organisatie vertegenwoordigt, zoals een bedrijf of school, die gebruikmaakt van de Producten voor ondernemingen en ontwikkelaars van Microsoft, raadpleegt u de sectie Producten voor ondernemingen en ontwikkelaars van deze privacyverklaring om uit te vinden hoe we uw gegevens verwerken. Als u eindgebruiker bent van een Microsoft-product of een Microsoft-account dat wordt verstrekt door uw organisatie, raadpleegt u de secties Producten die worden geleverd door uw organisatie en Microsoft-account voor meer informatie.

U hebt keuzes wat betreft de technologie die u gebruikt en de gegevens die u deelt. Wanneer we u vragen om persoonsgegevens te verstrekken, kunt u dit weigeren. Veel van onze producten vereisen bepaalde persoonsgegevens om u een service te kunnen leveren. Als u ervoor kiest om gegevens die vereist zijn om een product of service aan u te leveren niet te verstrekken, kunt u dat product of die service niet gebruiken. Evenzo geldt dat, als u persoonsgegevens die we moeten verzamelen omdat de wet dit eist of voor het aangaan of uitvoeren van een overeenkomst niet verstrekt, we de overeenkomst niet kunnen aangaan of,

als dit betrekking heeft op een bestaand product dat u gebruikt, het moeten opschorten of annuleren. We informeren u hierover op het moment dat dit gebeurt. Als het verstrekken van de gegevens optioneel is en u ervoor kiest persoonsgegevens niet te delen, werken functies zoals personalisatie waarbij gebruik wordt gemaakt van dergelijke gegevens niet voor u.

Hoe we persoonsgegevens gebruiken

Microsoft gebruikt de gegevens die we verzamelen om u te voorzien van rijke, interactieve ervaringen. Wij gebruiken gegevens in het bijzonder voor:

Het leveren van onze producten, waaronder het verstrekken van updates, het bieden van beveiliging en het oplossen van problemen, evenals het leveren van ondersteuning. Het omvat ook het delen van gegevens, wanneer dat is vereist om de service te leveren of de transacties uit te voeren waarom u vraagt. Het verbeteren en ontwikkelen van onze producten. Het personaliseren van onze producten en het doen van aanbevelingen. Het maken van reclame en het uitvoeren van marketingactiviteiten, zoals het verzenden van promotionele berichten, het leveren van gerichte advertenties en het presenteren van relevante aanbiedingen.

Wij gebruiken de gegevens ook voor onze bedrijfsvoering, waaronder het analyseren van onze prestaties, het voldoen aan onze wettelijke verplichtingen, het ontwikkelen van ons personeel en het doen van onderzoek.

Bij het realiseren van deze doeleinden combineren we gegevens die we verzamelen uit verschillende contexten (bijvoorbeeld van uw gebruik van twee Microsoft-producten) of die we van derden verkrijgen om u een meer naadloze, consistente en gepersonaliseerde ervaring te bieden, geïnformeerde zakelijke beslissingen te nemen en voor andere gerechtvaardigde doeleinden.

Onze verwerking van persoonsgegevens voor deze doeleinden omvat zowel geautomatiseerde als handmatige (menselijke) verwerkingsmethoden. Onze geautomatiseerde methoden zijn vaak gerelateerd aan en ondersteund door onze handmatige methoden. Onze geautomatiseerde methoden omvatten bijvoorbeeld kunstmatige intelligentie (AI), wat we beschouwen als een set technologieën waarmee computers kunnen nadenken, leren, beredeneren en helpen bij de beslissingen om problemen op te lossen op manieren die vergelijkbaar zijn met wat mensen doen. Om de nauwkeurigheid van onze geautomatiseerde verwerkingsmethoden (inclusief AI) op te bouwen, te trainen en te verbeteren, controleren we handmatig enkele van de voorspellingen en conclusies die door de geautomatiseerde methoden worden geproduceerd aan de hand van de onderliggende gegevens op basis waarvan de voorspellingen en de conclusies zijn gemaakt. We bekijken bijvoorbeeld handmatig korte fragmenten van een kleine steekproef van spraakgegevens om onze spraakservices te verbeteren, zoals herkenning en vertaling. We hebben stappen genomen om deze gegevens niet-identificeerbaar te maken.

Redenen waarom we persoonsgegevens delen

We delen uw persoonsgegevens met uw toestemming of om een transactie te voltooien of een door u gevraagd of geautoriseerd product te leveren. We delen ook gegevens met door Microsoft aangestuurde filialen en dochterondernemingen; met leveranciers die namens ons

werken; wanneer vereist door de wet of om te reageren op juridische procedures; om onze klanten te beschermen; om levens te beschermen; om de veiligheid van onze producten te garanderen; en om de rechten en eigendommen van Microsoft en haar klanten te beschermen.

Toegang krijgen tot uw persoonsgegevens en deze beheren

U kunt ook keuzes maken over het verzamelen en gebruiken van uw gegevens door Microsoft. U kunt uw persoonsgegevens die Microsoft heeft verkregen beheren en uw rechten met betrekking tot gegevensbescherming uitoefenen, door contact op te nemen met Microsoft of met behulp van verschillende hulpprogramma's die we bieden. In sommige gevallen zal uw vermogen om toegang te krijgen tot of om de controle uit te oeferen over uw persoonsgegevens beperkt zijn indien het toepasselijk recht dit vereist of toestaat. Hoe u toegang kunt krijgen tot uw persoonsgegevens of ze kunt beheren, is tevens afhankelijk van de producten die u gebruikt. U kunt bijvoorbeeld:

Het gebruik van uw gegevens voor op interesses gebaseerde advertenties van Microsoft beheren door een bezoek te brengen aan onze 'opt-out'-pagina. Kiezen of u promotionele e-mails, sms-berichten, telefoontjes en post van Microsoft wilt ontvangen. Bepaalde gegevens inzien en wissen via het Microsoft-privacydashboard.

Niet alle persoonsgegevens die zijn verwerkt door Microsoft kunnen worden geopend of beheerd via de bovenstaande hulpprogramma's. Als u toegang wilt krijgen tot of de controle wilt hebben over persoonsgegevens die door Microsoft zijn verwerkt maar niet beschikbaar zijn via de bovenstaande hulpprogramma's of rechtstreeks via de Microsoft-producten die u gebruikt, kunt u altijd contact opnemen met Microsoft op het adres in de sectie Contact met ons opnemen of via ons webformulier.

Cookies en soortgelijke technologieën

Cookies zijn kleine tekstbestanden die op uw apparaat worden geplaatst om gegevens op te slaan die kunnen worden opgehaald door een webserver in het domein dat de cookie heeft geplaatst. We gebruiken cookies en soortgelijke technologieën voor het opslaan en instandhouden van uw voorkeuren en instellingen om u in staat te stellen zich aan te melden, op interesses gebaseerde reclame aan te bieden, fraude te bestrijden, te analyseren hoe onze producten presteren en aan andere gerechtvaardigde doeleinden te voldoen. Microsoft-apps maken voor soortgelijke doeleinden gebruik van aanvullende id's, zoals de reclame-id in Windows die wordt beschreven in de sectie Reclame-id van deze privacyverklaring.

We maken ook gebruik van 'webbakens' om te helpen cookies te leveren, en gebruiks- en prestatiegegevens te verzamelen. Onze websites kunnen webbakens, cookies of vergelijkbare technologieën van andere serviceproviders omvatten.

U beschikt over tal van hulpprogramma's voor het beheren van de gegevens die worden verzameld door cookies, webbakens en soortgelijke technologieën. Zo kunt u bijvoorbeeld besturingselementen in uw internetbrowser gebruiken om te beperken hoe de websites die u bezoekt cookies kunnen gebruiken en uw toestemming intrekken door cookies te wissen of te blokkeren.

DUCKDUCKGO

Bron: https://duckduckgo.com/privacy

We don't collect or share personal information. That's our privacy policy in a nutshell.

DuckDuckGo does not collect or share personal information. That is our privacy policy in a nutshell. The rest of this page tries to explain why you should care.

- Why You Should Care - Search Leakage
- Why You Should Care - Search History
- Information Not Collected
- Information Collected
- Information Shared

- Last updated on 04/11/12. Removed ", which gets sent to my personal email.ïn last paragraph as our feedback is now
- handled by multiple team members via desk.com.
- Before that, on 03/11/12. Removed dead link (Scroogle) and added a missing 'to'.
- Before that, on 11/16/10. This paragraph was added.
- Before that, on 9/25/10. This paragraph was added.
- Before that, on 9/16/10. This paragraph was added.

Why You Should Care Search Leakage

At other search engines, when you do a search and then click on a link, your search terms are sent to that site you clicked on (in the HTTP referrer header). We call this sharing of personal information "search leakage."

For example, when you search for something private, you are sharing that private search not only with your search engine, but also with all the sites that you clicked on (for that search).

In addition, when you visit any site, your computer automatically sends information about it to that site (including your User agent and IP address). This information can often be used to identify you directly.

So when you do that private search, not only can those other sites know your search terms, but they can also know that you searched it. It is this combination of available information about you that raises privacy concerns.

DuckDuckGo prevents search leakage by default. Instead, when you click on a link on our site, we route (redirect) that request in such a way so that it does not send your search terms to other sites. The other sites will still know that you visited them, but they will not know what search you entered beforehand.

At some other search engines (including us), you can also use an encrypted version (HTTPS), which as a byproduct doesn't usually send your search terms to sites. However, it is slower to connect to these versions and if you click on a site that also uses HTTPS then your search is sent. Nevertheless, the encrypted version does protect your search from being leaked onto the computers it travels on between you and us.

At DuckDuckGo, our encrypted version goes even further and automatically changes links from a number of major Web sites to point to the encrypted versions of those sites. It is modeled after (and uses code from) the HTTPS Everywhere FireFox add-on. These sites include Wikipedia, Facebook, Twitter, and Amazon to name a few.

Another way to prevent search leakage is by using something called a POST request, which has the effect of not showing your search in your browser, and, as a consequence, does not send it to other sites. You can turn on POST requests on our settings page, but it has its own issues. POST requests usually break browser back buttons, and they make it impossible for you to easily share your search by copying and pasting it out of your Web browser's address bar.

Finally, if you want to prevent sites from knowing you visited them at all, you can use a proxy like Tor. DuckDuckGo actually operates a Tor exit enclave, which means you can get end to end anonymous and encrypted searching using Tor & DDG together.

You can enter !proxy domain into DuckDuckGo as well, and we will route you through a proxy, e.g. !proxy breadpig.com. This feature is part of our !bang syntax. Unfortunately, proxies can also be slow, and free proxies (like the one we use) are funded by arguably excessive advertising.

Because of these drawbacks in HTTPS, POST and proxies we decided to take the redirect approach to combat search leakage. However, we leave the choice up to you. You can deviate from the default on our settings page by toggling the redirect or address bar settings. You can also use our encrypted version.

Search History

Other search engines save your search history. Usually your searches are saved along with the date and time of the search, some information about your computer (e.g. your IP address, User agent and often a unique identifier stored in a browser cookie), and if you are logged in, your account information (e.g. name and email address).

With only the timestamp and computer information, your searches can often be traced directly to you. With the additional account information, they are associated directly with you.

Also, note that with this information your searches can be tied together. This means someone can see everything you've been searching, not just one isolated search. You can usually find out a lot about a person from their search history.

It's sort of creepy that people at search engines can see all this info about you, but that is not the main concern. The main concern is when they either a) release it to the public or b) give it to law enforcement.

Why would they release it to the public? AOL famously released supposedly anonymous search terms for research purposes, except they didn't do a good job of making them completely anonymous, and they were ultimately sued over it. In fact, almost every attempt to anonymize data has similarly been later found out to be much less anonymous than initially thought.

The other way to release it to the public is by accident. Search engines could lose data, or get hacked, or accidentally expose data due to security holes or incompetence, all of which has happened with personal information on the Internet.

Why would search engines give your search history to law enforcement? Simply because law enforcement asked for it, usually as part of a legal investigation. If you read privacy policies and terms of service carefully you will notice that they say they can give your information on court order.

This makes sense because they may be legally obligated to do so. However, search engines are not legally obligated to collect personal information in the first place. They do it on their own volition.

The bottom line is if search engines have your information, it could get out, even if they have the best intentions. And this information (your search history) can be pretty personal.

For these reasons, DuckDuckGo takes the approach to not collect any personal information. The decisions of whether and how to comply with law enforcement requests, whether and how to anonymize data, and how to best protect your information from hackers are out of our hands. Your search history is safe with us because it cannot be tied to you in any way.

Information

Information Not Collected

When you search at DuckDuckGo, we don't know who you are and there is no way to tie your searches together.

When you access DuckDuckGo (or any Web site), your Web browser automatically sends information about your computer, e.g. your User agent and IP address.

Because this information could be used to link you to your searches, we do not log (store) it at all. This is a very unusual practice, but we feel it is an important step to protect your privacy.

It is unusual for a few reasons. First, most server software auto-stores this information, so you have to go out of your way not to store it. Second, most businesses want to keep as much information as possible because they don't know when it will be useful. Third, many search engines actively use this information, for example to show you more targeted advertising.

Another way that your searches are often tied together at other search engines are through browser cookies, which are pieces of information that sit on your computer and get sent to the search engine on each request. What search engines often do is store a unique identifier in your browser and then associate that identifier with your searches. At DuckDuckGo, no cookies are used by default.

In response to efforts by the EFF and others, the major search engines have begun änonymizing"their search log data after periods of time. Sure, this is better than not doing so, but you should note that this does not make your search history anonymous in the same way that it is at DuckDuckGo.

What search engines generally do when they anonymize data is get rid of part of your IP address or turn it into something that doesn't look exactly like an IP address. And they do the same thing for uniquely identifying cookies.

However, in many cases, this so-called anonymous data can still tie your searches together, which can be used to reconstruct who you are and what you searched for. Additionally, search engines usually are silent on what they do with the User agent, which has been shown to also have enough information to often be personally identifiable, especially if isolated to a particular search session (day). Information Collected

At DuckDuckGo, no cookies are used by default. If you have changed any settings, then cookies are used to store those changes. However, in that case, they are not stored in a personally identifiable way. For example, the large size setting is stored as 's=l'; no unique identifier is in there. Furthermore, if you prefer not to use cookies to store settings, you can use URL parameters instead.

Additionally, if you use our !bang syntax/dropdown, which bangs you use are stored in a cookie so that we can list your most frequently used ones on top of the !bang dropdown box. Just like the other settings, this information is not saved on our servers at all, but resides solely on your computer. There is also a setting to turn this off, which you can also set via a URL parameter. Particular searches are of course not stored. An example cookie might look like:

```
php=2&yelp=19&java=4.
```

We also save searches, but again, not in a personally identifiable way, as we do not store IP addresses or unique User agent strings. We use aggregate, non-personal search data to improve things like misspellings.

Similarly, we may add an affiliate code to some eCommerce sites (e.g. Amazon & eBay) that results in small commissions being paid back to DuckDuckGo when you make purchases at those sites. We do not use any third parties to do the code insertion, and we do not work with any sites that share personally identifiable information (e.g. name, address, etc.) via their affiliate programs. This means that no information is shared from DuckDuckGo to the sites, and the only information that is collected from this process is product information, which is not tied to any particular user and which we do not save or store on our end. It is completely analogous to the search result case from the previous paragraph–we can see anonymous product info such that we cannot tie them to any particular person (or even tie multiple purchases together). This whole affiliate process is an attempt to keep advertising to a minimal level on DuckDuckGo.

Finally, if you give us feedback, it may be stored in our email. However, you can give ano-

nymous feedback (by not entering your email or other personal info on the feedback form). Information Shared

If you turn redirects off in the settings and you don't either turn POST on or use our encrypted site, then your search could leak to sites you click on. Yet as explained above, this does not happen by default.

Also, like anyone else, we will comply with court ordered legal requests. However, in our case, we don't expect any because there is nothing useful to give them since we don't collect any personal information.

Other

Other Search Engines

If you care about search privacy, you might also want to check out these other search engines that take it seriously by default.

Ixquick [privacy policy]

Each does things a bit differently in terms of privacy and very differently in terms of results. And not all go as far as DuckDuckGo in some aspects. However, none store your personal information by default, which make them all pretty safe in our opinion. Updates

If this policy is substantively updated, we will update the text of this page and provide notice to you at https://duckduckgo.com/about by writing '(Updated)' in red next to the link to this page (in the footer) for a period of at least 30 days. Feedback

I (Gabriel Weinberg) am the founder of Duck Duck Go and personally wrote this privacy policy. If you have any questions or concerns, please submit feedback.

GOOGLE

Bron: https://policies.google.com/privacy

Privacybeleid van Google

Wanneer u onze services gebruikt, vertrouwt u ons uw gegevens toe. We begrijpen dat dit een grote verantwoordelijkheid is en werken er hard aan om uw gegevens te beschermen en u er de controle over te geven.

Dit privacybeleid is bedoeld om u inzicht te geven in de gegevens die we verzamelen, waarom we deze gegevens verzamelen en hoe u deze gegevens kunt updaten, beheren, exporteren en verwijderen. Datum van inwerkingtreding 15 oktober 2019 | Gearchiveerde versies | Pdf downloaden

We bouwen een reeks services waarmee miljoenen mensen dagelijks de wereld op nieuwe manieren kunnen verkennen en er interactie mee kunnen hebben. Onze services bestaan onder meer uit:

Google-applicaties, -sites en -apparaten, zoals Zoeken, YouTube en Google Home; platforms,

zoals de Chrome-browser en het Android-besturingssysteem; producten die zijn geïntegreerd in apps en sites van derden, zoals advertenties en ingesloten Google Maps.

U kunt onze services op vele verschillende manieren gebruiken om uw privacy te beheren. U kunt zich bijvoorbeeld aanmelden voor een Google-account als u content (zoals e-mails en foto's) wilt maken en beheren of als u relevantere zoekresultaten wilt krijgen. U kunt veel Google-services ook gebruiken als u bent uitgelogd of zonder überhaupt een account te maken, zoals zoeken op Google of YouTube-video's bekijken. U kunt er ook voor kiezen privé te browsen op het web via Chrome in de incognitomodus. In al onze services kunt u uw privacyinstellingen aanpassen om te beheren wat we verzamelen en hoe uw gegevens worden gebruikt.

We willen alles graag zo duidelijk mogelijk uitleggen en daarom hebben we voorbeelden, video's met uitleg en definities toegevoegd voor belangrijke termen. Als u vragen heeft over dit privacybeleid, kunt u contact met ons opnemen. Gegevens die Google verzamelt

We willen dat u inzicht krijgt in de typen gegevens die we verzamelen wanneer u onze services gebruikt. We verzamelen gegevens om betere services te kunnen leveren aan al onze gebruikers, van het vaststellen van basisinformatie (zoals de taal die u spreekt) tot meer complexe aspecten, zoals welke advertenties u het nuttigst vindt, welke mensen online het belangrijkst voor u zijn of welke YouTube-video's u mogelijk leuk vindt. De gegevens die Google verzamelt en de manier waarop die gegevens worden gebruikt, zijn afhankelijk van de manier waarop u onze services gebruikt en hoe u de privacyopties beheert.

Als u niet bent ingelogd op een Google-account, slaan we de gegevens die we verzamelen op met unieke ID's die zijn gekoppeld aan de browser of de app die of het apparaat dat u gebruikt. Zo kunnen we bijvoorbeeld tijdens verschillende browsesessies onthouden wat uw taalvoorkeuren zijn.

Wanneer u bent ingelogd, verzamelen we ook gegevens die we opslaan in uw Google-account en die we behandelen als persoonlijke gegevens.

Wanneer u een Google-account maakt, verstrekt u persoonlijke gegevens aan ons, zoals uw naam en een wachtwoord. U kunt er ook voor kiezen een telefoonnummer of betalingsgegevens toe te voegen aan uw account. Zelfs als u niet bent ingelogd op een Google-account kunt u ervoor kiezen ons gegevens te verstrekken, zoals een e-mailadres om updates over onze services te ontvangen.

We verzamelen ook de content die u maakt, uploadt of van anderen ontvangt wanneer u onze services gebruikt. Dit zijn onder meer de e-mails die u schrijft en ontvangt, foto's en video's die u opslaat, documenten en spreadsheets die u maakt en reacties die u achterlaat bij YouTube-video's. Gegevens die we verzamelen terwijl u onze services gebruikt

We verzamelen informatie over de apps, browsers en apparaten die u gebruikt om toegang te krijgen tot Google-services, waardoor we betere functies kunnen aanbieden, zoals automatische productupdates en het dimmen van uw scherm als uw batterij leeg raakt.

De gegevens die we verzamelen, bestaan onder meer uit unieke ID's, het browsertype en de instellingen ervan, het besturingssysteem, informatie over het mobiele netwerk (waaronder

de naam van de provider en het telefoonnummer) en het versienummer van apps. We verzamelen ook informatie over de interactie van uw applicaties, browsers en apparaten met onze services, waaronder IP-adressen, crashrapporten, systeemactiviteit en de datum, tijd en verwijzende URL van uw verzoek.

We verzamelen deze gegevens wanneer een Google-service op uw apparaat contact opneemt met onze servers, bijvoorbeeld wanneer u een app installeert uit de Play Store of wanneer een service controleert op updates of deze ontvangt. Als u een Android-apparaat met Google-apps gebruikt, neemt uw apparaat periodiek contact op met Google-servers om informatie te verstrekken over uw apparaat en verbinding met onze services. Deze informatie bestaat onder meer uit het apparaattype, de naam van de provider, crashrapporten en welke apps u heeft geïnstalleerd. Uw activiteit

We verzamelen gegevens over uw activiteiten op onze services, die we gebruiken om bijvoorbeeld een YouTube-video aan te raden die u mogelijk leuk vindt. De activiteitsgegevens die we verzamelen, kunnen onder meer bestaan uit:

- termen waarnaar u zoekt;
- video's die u bekijkt;
- weergaven van en interacties met content en advertenties;
- spraak- en audiogegevens als u audiofuncties gebruikt;
- aankoopactiviteiten;
- mensen met wie u communiceert of met wie u content deelt;
- activiteiten op sites en apps van derden die gebruikmaken van onze services;
- browsegeschiedenis op Chrome die u heeft gesynchroniseerd met uw Google-account.

Als u onze services gebruikt om oproepen te plaatsen en te ontvangen of sms'jes te verzenden en te ontvangen, kunnen we telefoonlogbestandsgegevens gebruiken, zoals uw telefoonnummer, door u gebelde nummers, nummers waardoor u gebeld wordt, doorschakelnummers, tijd en datum van oproepen en berichten, duur van oproepen, routeringsinformatie en oproeptypen.

U kunt naar uw Google-account gaan voor informatie over en het beheer van activiteitsgegevens die zijn opgeslagen in uw account.

Naar Google-account Uw locatiegegevens

We verzamelen gegevens over uw locatie wanneer u onze services gebruikt. Daardoor kunnen we u functies aanbieden zoals een routebeschrijving voor uw weekendje weg of de aanvangstijden van films in een bioscoop bij u in de buurt.

Uw locatie kan met een verschillende mate van nauwkeurigheid worden bepaald door:

- gps;
- IP-adres

- sensorgegevens van uw apparaat.
- informatie over zaken in de buurt van uw apparaat, zoals wifi-toegangspunten, zendmasten en Bluetooth-apparaten

De soorten locatiegegevens die we verzamelen, zijn deels afhankelijk van uw apparaat- en accountinstellingen. U kunt bijvoorbeeld de locatie van uw Android-apparaat in- of uitschakelen via de instellingen app van het apparaat. U kunt ook Locatiegeschiedenis inschakelen als u een privékaart wilt maken van waar u naartoe gaat met de apparaten waarbij u bent ingelogd.

In sommige omstandigheden verzamelt Google ook gegevens over u via openbaar toegankelijke bronnen. Als bijvoorbeeld uw naam wordt vermeld in de lokale krant, kan de zoekmachine van Google dat artikel indexeren en weergeven aan anderen als ze op uw naam zoeken. We kunnen ook gegevens over u verzamelen die afkomstig zijn van vertrouwde partners, waaronder marketingpartners die ons informatie verstrekken over potentiële klanten of onze zakelijke services en beveiligingspartners die ons informatie verstrekken om te beschermen tegen misbruik. We ontvangen ook informatie van adverteerders om namens hen advertenties en onderzoeksservices te bieden.

We gebruiken verschillende technologieën om gegevens te verzamelen en op te slaan, waaronder cookies, pixeltags, lokale webopslag, zoals browserwebopslag of gegevenscaches van apps, databases en serverlogbestanden. Waarom Google gegevens verzamelt

We gebruiken gegevens om betere services te ontwikkelen

We gebruiken de gegevens die we op al onze services verzamelen voor de volgende doeleinden: Onze services leveren

We gebruiken uw gegevens om onze services te leveren, zoals de verwerking van de termen waarnaar u zoekt om resultaten weer te geven of om u te helpen content te delen door ontvangers uit uw contacten voor te stellen. Onze services onderhouden en verbeteren

We gebruiken uw gegevens ook om ervoor te zorgen dat onze services werken zoals de bedoeling is, bijvoorbeeld door storingen bij te houden of problemen op te lossen die u aan ons rapporteert. We gebruiken uw gegevens ook om verbeteringen door te voeren in onze services. Zo helpt inzicht in zoektermen die vaak verkeerd worden gespeld ons bijvoorbeeld bij de verbetering van functies voor spellingcontrole in onze services. Nieuwe services ontwikkelen

We gebruiken de gegevens die we in bestaande services verzamelen om ons te helpen bij de ontwikkeling van nieuwe services. Het inzicht dat we bijvoorbeeld kregen in de manier waarop mensen hun foto's organiseerden in Picasa (de eerste foto-app van Google), hielp ons bij het ontwerp en de introductie van Google Foto's. Gepersonaliseerde services leveren, waaronder content en advertenties

We gebruiken de gegevens die we verzamelen om onze services voor u aan te passen, onder andere door aanbevelingen te doen, gepersonaliseerde content te bieden en aangepaste zoekresultaten weer te geven. Zo biedt de Beveiligingscheck bijvoorbeeld beveiligingstips die zijn aangepast aan de manier waarop u Google-producten gebruikt. En Google Play gebruikt

gegevens zoals apps die u al heeft geïnstalleerd en video's die u heeft bekeken op YouTube om u suggesties te doen voor nieuwe apps die u mogelijk interessant vindt.

Afhankelijk van uw instellingen kunnen we u ook gepersonaliseerde advertenties laten zien op basis van uw interesses. Als u bijvoorbeeld zoekt naar 'mountainbikes', kunt u een advertentie te zien krijgen voor sportmateriaal wanneer u een site bekijkt waarop advertenties van Google worden weergegeven. U bepaalt via uw advertentie-instellingen welke gegevens we gebruiken om u advertenties te laten zien.

We laten geen gepersonaliseerde advertenties zien op basis van gevoelige categorieën, zoals ras, religie, seksuele geaardheid of gezondheid. We delen geen gegevens waarmee u persoonlijk geïdentificeerd kunt worden door adverteerders, zoals uw naam of e-mailadres, tenzij u ons hierom verzoekt. Als u bijvoorbeeld een advertentie ziet voor een bloemenzaak bij u in de buurt en de knop 'Tik om te bellen' selecteert, verbinden we uw oproep door en kunnen we uw telefoonnummer delen met de bloemenzaak.

Ga naar Advertentie-instellingen Prestaties meten

We gebruiken gegevens voor analyses en metingen om inzicht te krijgen in de manier waarop onze services worden gebruikt. Zo analyseren we bijvoorbeeld gegevens over uw bezoeken aan onze sites om zo onder meer het productontwerp te optimaliseren. We gebruiken ook gegevens over de advertenties waarmee u interactie heeft om adverteerders inzicht te bieden in de prestaties van hun advertentiecampagnes. Hiervoor gebruiken we verschillende tools, waaronder Google Analytics. Wanneer u een site bezoekt die gebruikmaakt van Google Analytics, kunnen Google en een Google Analytics-klant gegevens over uw activiteiten op die site linken met activiteiten op andere sites die gebruikmaken van onze advertentieservices. Met u communiceren

We gebruiken gegevens die we verzamelen (zoals uw e-mailadres) om rechtstreeks met u te communiceren. We kunnen u bijvoorbeeld een melding sturen als we verdachte activiteiten constateren, zoals een poging om vanaf een ongebruikelijke locatie in te loggen op uw Google-account. We kunnen u ook informeren over aanstaande veranderingen of verbeteringen van onze services. En als u contact opneemt met Google, houden we gegevens over uw verzoek bij om u te helpen eventuele problemen op te lossen. Google, onze gebruikers en het publiek beschermen

We gebruiken informatie om de veiligheid en betrouwbaarheid van onze services te helpen verbeteren. Dit omvat onder meer het detecteren en voorkomen van en reageren op fraude, misbruik, beveiligingsrisico's en technische problemen die schade kunnen veroorzaken bij Google, onze gebruikers of het publiek.

We maken gebruik van verschillende technologieën om uw gegevens voor deze doeleinden te verwerken. We gebruiken geautomatiseerde systemen die uw content analyseren om bijvoorbeeld aangepaste zoekresultaten, gepersonaliseerde advertenties of andere functies te bieden die zijn aangepast aan de manier waarop u onze services gebruikt. En we analyseren uw content om ons te helpen misbruik te detecteren, zoals spam, malware en illegale content. We maken ook gebruik van algoritmen om patronen in gegevens te herkennen. Google

Translate helpt bijvoorbeeld mensen in verschillende talen te communiceren door veelvoorkomende taalpatronen te detecteren in zinnen die u laat vertalen.

We kunnen de gegevens combineren die we verzamelen via onze services en op verschillende apparaten en deze gebruiken voor de hierboven beschreven doeleinden. Als u bijvoorbeeld video's van gitaarspelers bekijkt op YouTube, krijgt u mogelijk een advertentie te zien voor gitaarlessen op een site die onze advertentieproducten gebruikt. Afhankelijk van uw accountinstellingen kan uw activiteit op andere sites en in andere apps worden gekoppeld aan uw persoonlijke gegevens om de services van Google en de door Google geleverde advertenties te verbeteren.

Als andere gebruikers al beschikken over uw e-mailadres of andere gegevens waarmee u kunt worden geïdentificeerd, kunnen we aan deze gebruikers uw openbaar zichtbare Google-accountgegevens weergeven, zoals uw naam en foto. Daardoor kunnen mensen bijvoorbeeld aan een e-mail zien dat deze van u afkomstig is.

We vragen om uw toestemming voordat we uw gegevens gebruiken voor een doeleinde dat niet in dit privacybeleid wordt beschreven. Uw privacyopties

U beschikt over keuzes met betrekking tot de gegevens die we verzamelen en hoe deze worden gebruikt

In dit gedeelte worden de belangrijkste opties beschreven waarmee u uw privacy kunt beheren in onze services. U kunt ook de Privacycheck doen, waarbij u belangrijke privacyinstellingen kunt bekijken en aanpassen. In aanvulling op deze tools bieden we ook specifieke privacyinstellingen in onze producten. Meer informatie hierover vindt u in onze privacyhandleiding voor producten.

Naar de Privacycheck Uw gegevens beheren, bekijken en updaten

Wanneer u bent ingelogd, kunt u altijd uw gegevens bekijken en updaten door naar de services te gaan die u gebruikt. Foto's en Drive zijn bijvoorbeeld beide ontworpen om u te helpen specifieke soorten content te beheren die u via Google heeft opgeslagen.

We hebben ook een plek ingebouwd waar u gegevens kunt bekijken en controleren die u heeft opgeslagen in uw Google-account. Uw Google-account bevat onder meer: Privacyopties Activiteitsopties

Besluit welke typen activiteiten u wilt opslaan in uw account. U kunt bijvoorbeeld Locatiegeschiedenis inschakelen als u verkeersprognoses wilt voor uw dagelijkse route van en naar het werk of u kunt uw YouTube-kijkgeschiedenis opslaan om betere videosuggesties te krijgen.

Ga naar Activiteitsopties Advertentie-instellingen

Beheer uw voorkeuren over advertenties die aan u worden weergegeven op Google en op sites en apps die samenwerken met Google om advertenties weer te geven. U kunt uw interesses aanpassen, kiezen of uw persoonlijke gegevens worden gebruikt om advertenties relevanter voor u te maken en bepaalde advertentieservices in- en uitschakelen.

Ga naar Advertentie-instellingen Over u

Gegevens beheren die andere gebruikers over u te zien krijgen in Google-services.

Naar 'Over u' Aanbevelingen uit uw kringen

Kies of uw naam en foto worden weergegeven naast uw activiteiten, zoals recensies en aanbevelingen, die worden weergegeven in advertenties.

Naar 'Aanbevelingen uit uw kringen' Gegevens die u deelt

Als je G Suite gebruikt, kun je beheren met wie je gegevens deelt via je account op Google+.

Naar 'Gegevens die u deelt' Manieren om gegevens te bekijken en te updaten Mijn activiteit

Met 'Mijn activiteit' kunt u gegevens bekijken en controleren die worden gemaakt wanneer u Google-services gebruikt, zoals zoekopdrachten die u heeft uitgevoerd of uw bezoeken aan Google Play. U kunt browsen op datum en op onderwerp en uw activiteiten gedeeltelijk of volledig verwijderen.

Naar 'Mijn activiteit' Google Dashboard

Met Google Dashboard kunt u gegevens beheren die aan specifieke producten zijn gekoppeld.

Naar 'Dashboard' Uw persoonlijke gegevens

Beheer uw contactgegevens, zoals uw naam, e-mailadres en telefoonnummer.

Naar 'Persoonlijke gegevens' Als u bent uitgelogd, kunt u gegevens beheren die aan uw browser of apparaat zijn gekoppeld, waaronder de volgende gegevenstypen:

Personalisatie van zoekresultaten als u bent uitgelogd: Selecteer of uw zoekactiviteiten worden gebruikt om u relevantere resultaten en aanbevelingen te tonen. Instellingen voor YouTube: Pauzeer en verwijder uw YouTube-zoekgeschiedenis en uw YouTube-kijkgeschiedenis. Advertentie-instellingen: Beheer uw voorkeuren voor de advertenties die aan u worden getoond op Google en op sites en in apps die samenwerken met Google voor weergave van advertenties.

Uw gegevens exporteren, verwijderen en wissen

U kunt een kopie van de content in uw Google-account exporteren als u hier een reservekopie van wilt maken of de content wilt gebruiken in een service buiten Google.

Uw gegevens exporteren

U kunt ook verzoeken om verwijdering van content van specifieke Google-services op basis van de toepasselijke wetgeving.

Als u uw gegevens wilt verwijderen, kunt u het volgende doen:

Uw content verwijderen uit specifieke Google-services. Specifieke items zoeken en deze vervolgens verwijderen uit uw account via Mijn activiteit. Specifieke Google-producten verwijderen, waaronder uw gegevens die aan deze producten zijn gekoppeld. Uw gehele Google-account verwijderen.

Uw gegevens verwijderen.

En tot slot kunt u via Inactiviteitsvoorkeuren iemand anders toegang verlenen tot delen van uw Google-account als u onverwacht niet in staat bent uw account te gebruiken.

Er zijn andere manieren om te controleren welke gegevens Google verzamelt, ongeacht of u bent ingelogd op een Google-account. U kunt dit onder andere op de volgende plaatsen doen:

Browserinstellingen: U kunt uw browser bijvoorbeeld zodanig configureren dat een melding wordt weergegeven wanneer Google een cookie heeft ingesteld in uw browser. U kunt uw browser ook zodanig configureren dat alle cookies van een specifiek domein of van alle domeinen worden geblokkeerd. Denk er echter aan dat onze services cookies nodig hebben om naar behoren te functioneren, bijvoorbeeld voor zaken als het onthouden van uw taalvoorkeuren. Instellingen op apparaatniveau: Uw apparaat kan beschikken over opties waarmee u kunt bepalen welke gegevens we verzamelen. U kunt bijvoorbeeld locatie-instellingen wijzigen op uw Android-apparaat.

Uw gegevens delen Wanneer u gegevens deelt

In veel van onze services kunt u gegevens delen met andere mensen en zelf bepalen hoe u deze gegevens deelt. U kunt bijvoorbeeld video's openbaar delen op YouTube of u kunt ervoor kiezen uw video's privé te houden. Denk eraan dat als u gegevens openbaar deelt, uw content toegankelijk kan worden via zoekmachines, waaronder Google Zoeken.

Als je bent ingelogd en interactie hebt met bepaalde Google-services (zoals reacties voor een YouTube-video achterlaten of een app op Play beoordelen), worden je naam en foto naast je activiteit weergegeven. We kunnen deze informatie ook weergeven in advertenties afhankelijk van je instelling 'Aanbevelingen uit jouw kringen'. Wanneer Google uw gegevens deelt

We delen persoonlijke gegevens niet met bedrijven, organisaties en individuen buiten Google, behalve in de volgende gevallen: Met uw toestemming

We delen persoonlijke informatie buiten Google als we uw toestemming hebben. Als u bijvoorbeeld een Google Home gebruikt om een reservering te maken via een boekingsservice, krijgen we uw toestemming voordat we uw naam of telefoonnummer delen met het restaurant. We vragen om uw uitdrukkelijke toestemming voordat we gevoelige persoonlijke informatie delen. Met domeinbeheerders

Als u student bent of werkt voor een organisatie die gebruikmaakt van Google-services (zoals G Suite), hebben uw domeinbeheerder en resellers die uw account beheren toegang tot uw Google-account. Ze kunnen mogelijk het volgende doen:

Informatie bekijken en bewaren die is opgeslagen in uw account, zoals uw e-mail. Statistieken over uw account bekijken, zoals bijvoorbeeld hoeveel apps u installeert. Uw accountwachtwoord wijzigen. De toegang tot uw account opschorten of beëindigen. Uw accountgegevens ontvangen om te voldoen aan de van toepassing zijnde wet- en regelgeving, wettelijke procedures of verzoeken van overheidsinstanties. Uw mogelijkheden beperken om uw gegevens te verwijderen of te bewerken of uw privacyinstellingen aan te passen.

Voor externe verwerking

We leveren persoonlijke gegevens aan onze partners en andere vertrouwde bedrijven of individuen zodat ze de gegevens voor ons kunnen verwerken, op basis van onze instructies en in overeenstemming met ons privacybeleid en andere passende vertrouwelijkheids- en beveiligingsmaatregelen. We maken bijvoorbeeld gebruik van dienstverleners om ons te helpen met klantenondersteuning. Om juridische redenen

We delen persoonlijke gegevens buiten Google als we te goeder trouw van mening zijn dat toegang, gebruik, behoud of openbaarmaking van de gegevens redelijkerwijs nodig is om:

te voldoen aan de van toepassing zijnde wet- en regelgeving, wettelijke procedures of verzoeken van overheidsinstanties. We delen informatie over het aantal en het soort verzoeken dat we van overheden ontvangen in ons Transparantierapport; de van toepassing zijnde Servicevoorwaarden af te dwingen, waaronder het onderzoeken van mogelijke schendingen; fraude en technische of beveiligingsproblemen te detecteren, te voorkomen of anderszins aan te pakken; de rechten, eigendom of veiligheid van Google, onze gebruikers of het publiek te beschermen, zoals vereist of toegestaan volgens de wet.

We kunnen niet-persoonlijke gegevens openbaar delen en met onze partners, zoals uitgevers, adverteerders, ontwikkelaars of houders van rechten. We delen gegevens bijvoorbeeld openbaar om trends te laten zien voor het algemene gebruik van onze services. We staan ook specifieke partners toe gegevens te verzamelen uit uw browser of van uw apparaat voor advertentie- en meetdoeleinden via hun eigen cookies of soortgelijke technologieën.

Als Google betrokken is bij een fusie, overname of verkoop van activa, blijven we de vertrouwelijkheid van uw persoonlijke gegevens waarborgen en stellen we de betreffende gebruikers op de hoogte voordat persoonlijke gegevens worden overgedragen of onderworpen aan een ander privacybeleid. Uw gegevens veilig houden

We bouwen veiligheid in onze services in om uw gegevens te beschermen

Alle Google-producten zijn voorzien van sterke beveiligingsfuncties die uw gegevens voortdurend beschermen. Het inzicht dat we verkrijgen bij het onderhoud van onze services, helpt veiligheidsdreigingen te detecteren en automatisch te blokkeren, zodat deze u nooit bereiken. Als we toch iets risicovols detecteren waarvan we denken dat u daarvan op de hoogte moet zijn, informeren we u daarover en begeleiden we u via stappen waarmee u beter beveiligd blijft.

We werken er hard aan u en Google te beschermen tegen ongeautoriseerde toegang tot of ongeautoriseerde aanpassing, openbaarmaking of vernietiging van gegevens die in ons bezit zijn. We nemen onder andere de volgende maatregelen:

We gebruiken versleuteling om uw gegevens privé te houden tijdens de overdracht. We bieden een reeks beveiligingsfuncties, zoals Safe Browsing, Beveiligingscheck en authenticatie in twee stappen om u te helpen uw account te beschermen. We evalueren onze handelswijzen op het gebied van verzameling, opslag en verwerking van gegevens, waaronder fysieke beveiligingsmaatregelen, om ongeautoriseerde toegang tot systemen te voorkomen. We beperken de toegang tot persoonlijke gegevens tot medewerkers van Google, contractanten en

vertegenwoordigers die deze gegevens moeten kennen om ze te verwerken. Iedereen met deze toegang is onderworpen aan strenge contractuele vertrouwelijkheidsverplichtingen en kan worden bestraft of ontslagen als hij of zij niet aan deze verplichtingen voldoet.

Uw gegevens exporteren en verwijderen

U kunt altijd een kopie van uw gegevens exporteren of gegevens uit uw Google-account verwijderen

U kunt een kopie van de content in uw Google-account exporteren als u hier een reservekopie van wilt maken of de content wilt gebruiken in een service buiten Google.

Uw gegevens exporteren

Als u uw gegevens wilt verwijderen, kunt u het volgende doen:

Uw content verwijderen uit specifieke Google-services. Specifieke items zoeken en deze vervolgens verwijderen uit uw account via Mijn activiteit. Specifieke Google-producten verwijderen, waaronder uw gegevens die aan deze producten zijn gekoppeld. Uw gehele Google-account verwijderen.

Uw gegevens verwijderen. Je gegevens bewaren

We bewaren de verzamelde gegevens voor kortere of langere perioden afhankelijk van wat de gegevens zijn, hoe we ze gebruiken en hoe je de instellingen configureert:

Sommige gegevens (zoals de content die u maakt of uploadt) kunt u op elk gewenst moment verwijderen. U kunt ook activiteitsgegevens verwijderen die in uw account zijn opgeslagen, of deze na een bepaalde periode automatisch laten verwijderen. Andere gegevens (zoals advertentiegegevens in serverlogboeken) worden na een bepaalde periode automatisch verwijderd of geanonimiseerd. We bewaren sommige gegevens totdat je je Google-account verwijdert, zoals informatie over hoe vaak je onze services gebruikt. En sommige gegevens bewaren we voor een langere periode als dat nodig is voor rechtmatige zakelijke of juridische doeleinden, zoals beveiliging, fraude- en misbruikpreventie of financiële administratie.

Als je gegevens verwijdert, volgen we een verwijderingsprocedure om ervoor te zorgen dat je gegevens veilig en volledig worden verwijderd van onze servers of alleen in geanonimiseerde vorm worden bewaard. We proberen ervoor te zorgen dat onze services voorkomen dat gegevens per ongeluk of kwaadwillend worden verwijderd. Daarom kan het zijn dat er enige vertraging zit tussen het moment waarop je iets verwijdert en het moment waarop kopieën worden verwijderd uit onze actieve en back-upsystemen.

Bekijk meer informatie over de bewaarperioden voor gegevens die Google hanteert, waaronder hoelang het duurt om je gegevens te verwijderen. Naleving en samenwerking met regelgevende instanties

We evalueren dit privacybeleid regelmatig en zorgen ervoor dat we uw gegevens verwerken op een manier die aan dit beleid voldoet. Gegevensdoorgiften

We beschikken over servers over de hele wereld en uw gegevens kunnen worden verwerkt op servers die zich buiten het land bevinden waarin u woont. Gegevensbeschermingswetge-

ving verschilt per land en sommige landen bieden meer bescherming dan andere. Ongeacht waar uw gegevens worden verwerkt, passen we dezelfde bescherming toe zoals beschreven in dit beleid. We voldoen ook aan bepaalde juridische kaders die verband houden met de overdracht van gegevens, zoals de Privacy Shield-kaders tussen de EU en de VS en tussen Zwitserland en de VS.

Wanneer we formele schriftelijke klachten ontvangen, reageren we door contact op te nemen met de persoon die de klacht heeft ingediend. We werken samen met de betreffende regelgevende instanties, waaronder lokale autoriteiten voor gegevensbescherming, om klachten over de overdracht van uw gegevens te verhelpen die we niet rechtstreeks met u kunnen oplossen. Europese vereisten

Indien de gegevensbeschermingswetgeving van de Europese Unie (EU) van toepassing is op uw gegevens, bieden we de in dit beleid beschreven opties, zodat u gebruik kunt maken van het recht op inzage om uw gegevens te updaten, te wissen en de verwerking ervan te beperken. U heeft ook het recht om bezwaar te maken tegen de verwerking van uw gegevens of om de gegevens te exporteren naar een andere service.

Voor gebruikers woonachtig in de Europese Economische Ruimte of Zwitserland is Google Ireland Limited de verwerkingsverantwoordelijke voor uw informatie, tenzij anderszins aangegeven in een servicespecifieke privacymededeling. Met andere woorden, Google Ireland Limited is de aangesloten Google-entiteit die verantwoordelijk is voor de verwerking van uw informatie en de naleving van de toepasselijke privacywetgeving.

We verwerken uw gegevens voor de doeleinden zoals beschreven in dit beleid op basis van de volgende rechtsgronden: Met uw toestemming

We vragen om je toestemming voor de verwerking van je gegevens voor specifieke doeleinden en je hebt het recht om je toestemming op elk gewenst moment in te trekken. We vragen bijvoorbeeld om je toestemming om gepersonaliseerde services te bieden, zoals advertenties op basis van je interesses. We kunnen ook om je toestemming vragen om je spraak- en audioactiviteit te verzamelen voor spraakherkenning. Je kunt deze instellingen beheren in je Google-account. Wanneer we gerechtvaardigde belangen nastreven

We verwerken uw gegevens voor onze gerechtvaardigde belangen en die van derden waarbij we passende beschermingsmaatregelen toepassen die uw privacy beschermen. Dit houdt in dat we uw gegevens onder meer kunnen verwerken voor het volgende:

Het aanbieden, onderhouden en verbeteren van onze services zodat ze voldoen aan de behoeften van onze gebruikers. De ontwikkeling van nieuwe producten en functies die nuttig zijn voor onze gebruikers. Inzicht krijgen in de manier waarop mensen onze services gebruiken om de prestaties van onze services te waarborgen en verbeteren. Aanpassing van onze services om u een betere gebruikerservaring te bieden. Marketing om gebruikers te informeren over onze services. Advertenties bieden, zodat we veel van onze services gratis beschikbaar te maken (en als advertenties worden gepersonaliseerd, vragen we om je toestemming) Het detecteren, voorkomen of anderszins aanpakken van fraude, misbruik, beveiligings- of technische problemen met onze services. Bescherming van de rechten, het eigendom of de

veiligheid van Google, onze gebruikers of het publiek, zoals vereist of toegestaan volgens de wet, waaronder gegevens vrijgeven aan overheidsinstanties Uitvoering van onderzoek waarmee onze services worden verbeterd voor onze gebruikers en die het publiek tot voordeel strekken. Voldoen aan verplichtingen jegens onze partners, zoals ontwikkelaars en houders van rechten. Handhaving van juridische vorderingen, waaronder het onderzoeken van mogelijke schending van toepasselijke servicevoorwaarden.

Wanneer we een service aanbieden

We verwerken uw gegevens om een service te bieden waarom u op grond van een contract heeft verzocht. We verwerken bijvoorbeeld uw betalingsgegevens wanneer u extra opslag aanschaft voor Google Drive. Wanneer we voldoen aan wettelijke verplichtingen

We verwerken uw gegevens wanneer we een wettelijke verplichting hebben dit te doen, bijvoorbeeld wanneer we reageren op juridische procedures of afdwingbare verzoeken van overheidsinstanties.

Als u vragen heeft, kunt u contact opnemen met Google en ons bureau voor gegevensbescherming. U kunt ook contact opnemen met uw lokale gegevensbeschermingsautoriteit als u zorgen heeft over uw rechten op grond van de lokale wetgeving. Over dit beleid Wanneer dit beleid van toepassing is

Dit privacybeleid is van toepassing op alle services die worden verstrekt door Google LLC en haar aangesloten entiteiten, waaronder YouTube, Android en services die worden aangeboden op externe sites, zoals advertentieservices. Dit privacybeleid is niet van toepassing op services met een afzonderlijk privacybeleid waarin dit algemene privacybeleid niet is opgenomen.

Dit privacybeleid is niet van toepassing op:

het gegevensbeleid van andere bedrijven en organisaties die adverteren in onze services; services die worden aangeboden door andere bedrijven of individuen, waaronder producten of sites die onze Google-services bevatten, die kunnen worden weergegeven in de zoekresultaten of waarnaar in onze services een link is opgenomen.

Wijzigingen in dit beleid

We kunnen dit privacybeleid van tijd tot tijd wijzigen. We beperken uw rechten onder dit privacybeleid niet zonder uw uitdrukkelijke toestemming. We vermelden altijd de datum waarop de laatste wijzigingen zijn aangebracht en we bieden toegang tot gearchiveerde versies die u kunt bekijken. Indien er aanzienlijke wijzigingen worden aangebracht, geven we een duidelijkere melding hiervan (waaronder, voor bepaalde services, een e-mailbericht met wijzigingen in het privacybeleid).

Andere nuttige bronnen

De volgende links leiden naar nuttige bronnen waar u meer informatie over procedures en privacyinstellingen kunt vinden.

Uw Google-account is de plek waar u veel van de instellingen vindt waarmee u uw account

kunt beheren De Privacycheck begeleidt u door de belangrijkste privacyinstellingen voor uw Google-account In het Veiligheidscentrum van Google vindt u meer informatie over onze ingebouwde beveiliging, privacyopties en tools die u helpen om online digitale basisregels voor uw gezin in te stellen De Privacyvoorwaarden bieden meer context met betrekking tot dit privacybeleid en onze Servicevoorwaarden Het gedeelte Technologieën bevat meer informatie over: Hoe Google cookies gebruikt technologieën die worden gebruikt voor advertenties; hoe Google patroonherkenning gebruikt om dingen te herkennen, zoals gezichten op foto's; Hoe Google gegevens gebruikt van sites of apps die onze services gebruiken

QWANT

Bron: https://about.qwant.com/legal/privacy

Privacy policy Team Qwant Last update : 23/02/2017

Qwant ensures that your privacy is protected, and this is the cornerstone of our philosophy. We don't use any cookie nor any tracking device that may allow us to track your browsing habits or to establish your profile. You are of course entitled to the rights provided by the EU General Data Protection Regulation ("GDPR"), but we also forbid ourselves from collecting an important amount of data that others collect, which are useless to provide you with the services you need. We never try to find out who you are or what you are personally doing when you use our search engine. When we do need to collect data, we do not disclose nor sell it for commercial or other uses. We use it exclusively to provide you with the services offered by Qwant.

This Privacy Policy is aimed at explaining in further details our ethical approach towards personal data, and at explaining the few cases where we have to collect information about you, the reasons why we collect such data, and the way we might use it. It also presents the security measures that we apply to protect their confidentiality, and reminds your rights and how to exercize them. How does Qwant protect your privacy?

We should always ask our search engine what are the personal data that it does not collect

As a principle, Qwant does not collect data about its users when they search. Plain and simple.

When you use Qwant as a search engine, we don't put any cookie on your browser that may allow us or others to recognize you or to follow you everywhere on the Internet. We don't use any tracking device (pixel, fingerprinting…). We don't collect and we don't store any history or your searches. When you search, your query is instantly anonymized by being dissociated from your IP address, in accordance with what the French data controller advices. Long story short, what you are doing with Qwant is part of your privacy and we don't want to know.

Qwant has a Privacy office dedicated to protecting your privacy. It also has a Data Protection Officer (DPO). Both work closely with eachother to ensure that the relevant regulation regarding personal data is applied as strongly as it should.

The DPO keeps an updated register of all processing of personal data made by Qwant for his services. For instance, when you create an account on the site, you can choose to fill in your profile and this is a processing of personal data for which the register will say how data may be kept (and how long), and who can access it.

We commit to do anything we can to ensure the security and confidentiality of our users personal data, including by preventing data damage, loss, or access by unauthorized third parties. Qwant's URL has the HTTPS header that shows users they communicate with Qwant through a secure channel using the TLS protocol. Technically, TLS ensures users that their data can't be intercepted by fraud. Moreover, the green lock that you see on most browsers when using Qwant certifies that you are browsing a secure website. When do we collect personal data, and why?

Qwant does not require any registration to use its search engine. However, you may want to register an account to sign-in and enjoy advanced functionalities such as the possibility to save search results in favorites, or create Boards.

In such cases, we collect some personal data such as your name, firstname and email address:

when you register to our services. You are free to manage yourself all the information related to your account (information changes, corrections, updates and deletion); or when you use forms available on our website, so that Qwant can process your request.

Qwant also collects connection data, not associated with your search queries, only to ensure the security of its information system and, if you create or modify Boards, to respect the obligation to identify content creators mandated by law.

Even when you are connected with an ID, we don't use any cookie nor any other tracking device when you browse the site. The only technology that may be installed on your browser, called "local storage", is used to locally save your settings (language, activation or deactivation of options...). You can delete personal data stored in your "local storage" by deactivating cookies in your browser. However, this deactivation may prevent you from accessing some functionalities of the site, such as your browsing preferences.

Users personal data are collected and processed by Qwant solely for the following purposes:

- the technical management of the user's account(s) and available services, in accordance with our Terms of Use ;
- the management of information requests, in the context of the use of the services;
- the management of job applications, in the context of Qwant's recruitement processes;
- the management of delisting requests, requests related to rights regarding personal data, and content removal requests, in the context of the compliance by Qwant of its legal obligations;
- the security of Qwant's information system, in the context of the management of the security and smooth operation of the
- services;

What do we do with this personal data?

Personal data that you transmit are never disclosed or sold by Qwant to third parties, except for job applications that may be shared with recruiting partners, unless you ask us not to. Your data is stored on servers that belong to us and is never send to third-party technical parteners. Our host (as identified in our Terms) only provides a secure location for our servers, and can't access it. How long do we keep this personal data?

Users personal data is kept as long as you use the services provided by the site.

For Qwant and Qwant Junior accounts, your data is removed 7 days after you request that the account be deleted. During that time, you can reactivate your account by using your login information.

Regarding data collected for the processing of information requests, Qwant deletes them within 6 months after the receipt of the request.

For data that may be collected when you make a request (delisting, rights related to your personal data, content removal), the duration of retention depends on what the law prescribes for each of these rights. For more details, please refer to the next section of this Privacy Policy, entitled "What are your rights and how can you exercize them".

For job applications, we retain the data for a maximum of two years, where they may be transmitted to partners, unless stated otherwise by the candidate.

For connection data, we do not collect directly identifiying information (we do not store your IP address). The information we process for user queries are a hashed IP address and approximate geolocation.

For Qwant Boards, French law makes it mandatory to keep some connection data (e.g. user ID used, URL or position, nature of the operation, time...) for one year. This delay starts when you create, modify of delete content on Qwant Boards, and for data related to the account, from the date you request the account removal. All data related to you account will be deleted 7 days after you request the removal, unless otherwise stated by legal obligations. What are your rights and how can you exercize them?

Qwant is governed by the European General Data Protection Regulation (GDPR), which grants specific rights related to your personal data when processed by Qwant:

- right to access, rectify, delete data under the conditions set forth by the regulation;
- right the oppose the processing under the conditions set forth by the regulation;
- right to limit the processing of personal data under the conditions set forth by the regulation;
- right to data portability;
- right to make a claim before a control authority;

You may exercize such rights by contacting us:

sending a postal mail to QWANT – Direction Ethique & Affaires Juridiques, 7 rue Spontini, 75116 Paris, France ; sending an electronic request to privacy@qwant.com.

Right to access

You can ask us if we have any information related to you, and ask us information regarding their processing (for instance, the categories of data we process). This right allows you to ask Qwant to give you all this information.

Information related to this right to access (such as your contact info) are kept one year after Qwant has answered, then removed when such delay is over. Right to rectify or suppress

You can modify or delete information that you entered in your profile, in your Qwant account.

For job applications, you can request rectifications by replying to the automated e-mail you received when applying, or by sending a mail to privacy@qwant.com.

For forms for delisting requests and other rights exercizing requests, you can ask to rectify data by sending a mail to privacy@qwant.com.

Information associated to this right to rectify or suppress (such as your contact info) are kept for one year after Qwant has answered, then removed when such delay is over. Right to erasure

This right allows you to have to data erased as soon as possible by Qwant.

You can erase your data by following the instructions detailed here. From the date you ask for your account to be closed, the data will be deleted after 7 days, subject to our legal obligations.

You also can ask for your job application to be erased if you don't want it to be processed by Qwant anymore. From the day we receive your application, all data will be deleted at the latest 15 days after the receipt.

Information associated to the exercize of the right to erasure are stored for one year from the day Qwant answers, then deleted after this delay. Right to be forgotten (right to delisting)

It is a specific right that the European Court of Justice (ECJ) has recognized, that Qwant applies fully. When the search query with your full name and firstname delivers results which are untrue, obsolete or excessive, you can request that related web results be delisted. Your request will be processed on a case by case basis, and referenced URLs will be delisted only if the balance of interests does not impose to have the public right of information prevail (for instance if you are an elected representative who is trying to make a controversial statement disappear).

Information about this right to be forgotten (such as your contact info) are kept for one year after Qwant has answered, and entirely removed when the legal delay is over (3 years). Right to oppose

As the name says, the right to oppose allows you to oppose data processing by Qwant. You may, for instance, choose to delete your account.

For job applications, you are entitled to refuse that your data be transmitted or retained.

Information about this right to oppose (such as your contact info) are kept for one year after Qwant has answered, and entirely removed when the legal delay is over (3 years). Right to restriction of processing

This right allows you to obtain the temporary withdrawal of published data when its accuracy is challenged, for a period that allows Qwant to procede with necessary checks.

Information related to the exercize of this right (for instance your data) are stored for a period of one year following the day Qwant answers, then deleted when this delay is over. Right to data portability

This right allows to receive the data you have communicated, or to ask Qwant to transmit them to another data controller (another website for instance). In practice, following article 20 of the GDPR, the right to portability applies to your Boards.

Information related to the exercize of this right (for instance your contact info) are stored for one year from the day Qwant answers, then deleted when this delay is over.

You can get a copy of your data by connecting to your Qwant account and clicking “Receive a copy of my data” in your account. How about ads? Aren’t they tracked?

Qwant is a free search engine open to anyone. Our main source of revenues comes from ads displayed on Qwant results page. But we take pride of doing it while respecting both your privacy and your search experience of Qwant. Qwant does not track people, and this is never going to change.

We believe you will possibly find commercials interesting when they are directly related to what you are searching. Through their numerous formats, ads have too often taken over the use experience. On Qwant, you will never see intrusive ads that get in the way of what are looking for. With such commitments, we hope to demonstrate that such responsible and respectful behavior is possible. We have been working for several month at identifying and designing solutions aligned with those principles. We believe we now have designed a simple and efficient offering by working with the Microsoft Bing ad network.

Therefore, every ad that Qwant displays fully adheres to the values we defend and our quality standards. When you use Qwant, no personal information whatsoever is neither captured or transmitted to advertisers. In details:

- – No third party cookies
- – No trackers
- – No behavioral targeting
- – No campaigns mixing legit and promotional content (native advertising)

We believe advertising can be a responsible business model. How does Qwant index the web?

We continue our efforts to index all the Web diversity. Our crawlers relentlessly visit the global Web to refine our results. Nevertheless, this requires both a lot of resources and time: some parts of the Web are not yet perfectly indexed. In the meantime, our agreement with Micro-

soft Bing allows us to complement our own results with those of Microsoft Bing to offer the best possible results from all around the Web.

STARTPAGE

Bron: https://www.startpage.com/en/search/privacy-policy.html

In short

Startpage.com doesn't log or share your personal information.

We don't track you. We don't profile you. Period. The longer version

We believe privacy is a fundamental human right. With Startpage.com you can search and browse the internet privately. Not because you have something to hide, but because you have a lot to protect!

Protecting your privacy is all about having control over your data. At Startpage.com, we help you control and protect what's yours:

It's Your Data. Not Big Data! !

Why we don't collect any "personal data"

It's the best way to safeguard your privacy.

If information isn't collected, it can't be stolen, demanded, leaked or abused.

How do we define "personal data?"

To maximize your privacy, we use a broad definition.

Our definition of personal data is based on the privacy laws and regulations of the EU, including the General Data Protection Regulation (GDPR). These are widely regarded as the strongest privacy protections in the world. We consider any information about you or your behavior that can be traced back to you as personal data.

Information we don't collect So let's be perfectly clear:

We don't record your IP address The only exception is for automated search requests (robots) that rapidly submit more queries to our servers than any normal human would. When our software detects potential abuse, we register and block the offending IP address in order to keep our service safe and free.

We don't serve any tracking or identifying cookies This is about "goodänd "bad"cookies. Cookies are small pieces of data that are sent to your hard drive by websites you visit."Bad"cookies have unique elements that can track all kinds of personal information. We don't serve any of those. Startpage.com uses just one "good"cookie called "preferencesïn order to remember the search preferences you choose. It's completely anonymous and expires after not visiting Startpage.com for 90 days.

We don't record your search queries

Saves us headaches and disk space.

When you search, your query is automatically stripped of unnecessary metadata including your IP address and other identifying information. We send the anonymized search query to Google and return the search results to you. We don't log your searches.

To prevent abuse such as robotic high-volume querying, we anonymously determine the frequency of popular search keywords as a part of our anti-abuse measures, while protecting your privacy.

How we have implemented truly anonymous analytics

We only count aggregate numbers.

We do measure overall traffic numbers and some other – strictly anonymous – statistics. These stats may include the number of times our service is accessed by a certain operating system, a type of browser, a language, etc., but we don't know anything about individual users.

How we keep Startpage.com free without using "personal data"

Without tracking-ads - as we don't share personal info with anyone.

Most online advertising today is personalized, meaning that online advertising services track what you do online and profile you in order to serve tailored ads. We don't do that at Startpage.com. No tracking. No profiling!

Our search result pages may include a small number of clearly labeled "sponsored links,"which generate revenue and cover our operational costs. Those links are retrieved from platforms such as Google AdSense. In order to enable the prevention of click fraud, some non-identifying system information is shared, but because we never share personal information or information that could uniquely identify you, the ads we display are not connected to any individual user.

It's a myth that search engines need to profile you in order to earn decent money. Startpage.com serves strictly non-personalized ads. Sure, our ads make only a fraction of what other search engine ads make, but they pay all our bills.

We protect you on our site – and beyond

This privacy policy applies only to the Startpage.com website.

Once you click on a search result, you leave our site and our privacy protection. This is true for sponsored links, search results and other external links. Unless ... you use our "Anonymous View "feature - shown behind the search results. This is a great privacy tool that allows you to continue to browse in full privacy.

We don't disclose or sell your contact information

You ask for support, not spam.

When you contact us via email or through our support center, we'll use your contact information to respond to you. We won't sell or share this info with anyone else. You'll have the

option to subscribe to our newsletter, from which you can unsubscribe at any time.

How we respond to governmental requests for data

They can't request what we don't have.

Any request will have to come from Dutch judicial authorities. We'll only comply if we're legally obliged to do so. But we're not likely to receive requests by governments to hand over user data – simply because we don't have any.

We will never comply with any voluntary surveillance program

Big Brother would like some help?

Hell no! Fortunately, we are based in the EU, where we have strong laws that protect your right to privacy. European governments can't legally force service providers like Startpage.com to implement a blanket spying program.

Startpage.com complies with the GDPR

And we can help you comply, too.

We are located in the EU, and we fully comply with applicable privacy laws and regulations of the EU, including the General Data Protection Regulation (GDPR). These are widely regarded as the strongest privacy protections in the world.

Looking for a quick win to improve your own GDPR compliance? Setting Startpage.com as the default search engine on all your organization's IT equipment will help you minimize the amount of personal data that is processed by or for your organization. This can also help you implement important privacy principles, such as data minimization, storage limitation, privacy by design and privacy by default.

In the EU you have a "right to be forgotten"

When enough is enough.

Citizens in the EU have the right to request the deletion of search results that disclose their personal data when those results are inaccurate or no longer relevant. Find out how we have implemented this right here . Dutch Data Protection Authority

We are always here to help

If you have any feedback or complaint about our services in general, or more specifically about how your privacy is protected when you use our services, please let us know via the contact details below. In accordance with EU privacy laws and regulations, you have the right to lodge a complaint with the national supervisory authority responsible for the protection of personal data if you think we have unlawfully processed your personal data. For the Netherlands, this supervisory authority is the Dutch Data Protection Authority, which you can contact here .

Our company and contact information

Still have privacy questions?

Startpage.com is owned and operated by Startpage BV, Postbus 1079, 3700 BB Zeist, The Netherlands. Representative for the Privacy Policy is Robert E.G. Beens. You can contact us at

PRIVACY: It's not just our Policy - it's our Mission! Startpage.com

WOLFRAM ALPHA

Bron: https://www.wolfram.com/legal/privacy/wolfram/

LEGAL INFORMATION Wolfram Privacy Policy

Wolfram understands your concerns about how your information is used and shared, and we endeavor to use such information carefully and sensibly. This policy explains how the information you provide is collected and used. What Information Do We Collect?

We may collect both personally identifiable information about you and non-personally-identifiable information through your experience on our websites, from your use of our services and products, and via other voluntary contact with you (collectively "Services").

The personally identifiable information we collect through our Services primarily consists of information you submit to us, including your name, email address and other personal information that you willingly provide. Because participation in our Services is voluntary, you have a choice of whether or not to disclose such information.

In addition to information that you provide to us voluntarily, we receive some additional personally identifiable information and non-personally-identifiable information whenever you interact with our Services online, including your Internet Protocol (IP) address, browser type and version, referral URLs and other data automatically supplied by most common web browsers.

We may also collect information from third-party sites, as described below in What Information Do We Collect from Third-Party Sites? How Is Your Information Used?

The information we obtain from users, site participants and visitors helps us enhance and refine our Services. Non-personal information collected about you through your experience, queries and feedback is used to better understand the entire population that is utilizing our Services and how we might improve the collective experience. Except as noted below, we track and record IP addresses that access our Services for internal reporting, diagnostic analysis and security purposes only.

Your IP address is used to determine, when possible, your approximate geographical location, which affects the computations or outputs provided by our Services for such things as default currency and units of measure based on what country you are in. Your browser type may be used to optimize your display, for example on mobile devices or to work around limitations of a particular browser. Referrer URLs may be used to generate usage statistics and analyze usage patterns.

If you provide your email address to us, we may email you in response, as well as notify you of other offers or services that may be of interest. When you send email or other communica-

tion to us, we may retain that communication to respond to you and improve our Services. If at any time you want to stop receiving communication from us, please click the unsubscribe link in the footer of any email message from us, or contact our customer service online or by phone at 1-800-WOLFRAM. However, please note that we may still contact you with transactional communications associated with any software or service agreements you have with us or in direct response to any communication you send us. Disclosures of Your Information

We do not sell, rent, trade or lease your information to third parties. Any information we share shall be subject to the parameters associated with your requested Services and preferences.

When we share personal information, we require the recipient to protect your personal information in compliance with the law. Wolfram may share information with affiliates, partners, service providers, authorized resellers and distributors and relevant third parties in order to fulfill the limited purposes described herein.

Any collected information (personal and non-personal) associated with your use of our Services may also be subject to disclosure to government authorities or other authorized third parties pursuant to a lawful request, subpoena or other process that legally compels disclosure of that information.

We may also preserve, use or disclose your information if necessary to enforce our Terms of Use and related agreements; to detect, prevent or otherwise address fraud, security or technical issues, including suspiciously high-volume use of our Services; to respond to support requests; or to protect the rights, property or safety of our company, our users or others. What Information Do We Collect from Third-Party Sites?

When you use our Services to connect to or access data from a third-party site ("TPS"), including but not limited to social networking sites, we may collect personally identifiable information about you from any TPS profile for which you give our Services access credentials.

By authorizing these Services to access your TPS profile, you are authorizing us, in accordance with this Privacy Policy, to collect, store and use any and all information that your privacy settings at the TPS allow our Services to access through the TPS application programming interface ("API").

Because the linkage between any TPS and our Services is completely voluntary and our Services' abilities to access your information at the TPS require that linkage, and any information transmitted is controlled by your privacy settings at the TPS, you have a choice of whether or not to disclose such information. Links to Third-Party Websites

From time to time, our Services may contain links to other websites. We do not exercise any control over these websites, and we are not responsible for their privacy practices or content. We encourage all users to read the privacy policies of each and every website visited when following links from our Services. This Privacy Policy applies solely to information collected by our Services. Cookies

When you visit our websites, they, like most websites, send one or more cookies—small identifiers—to your computer that store information about your session and preferences as well as information that can help improve our Services. While we do use strictly necessary and

functional cookies for basic site functionality, as well as security and fraud investigation purposes, our primary purpose in using all other cookies is to enhance and improve your user experience by understanding and remembering your preferences, and by general tracking of our user trends. We utilize the following types of cookies:

Default cookies: These strictly necessary and functional cookies support and facilitate the provision of services that you have requested on our websites, and may enable enhanced features. Additional cookies: These cookies collect information that we utilize to support the measurement of our websites. On specific sites, Wolfram may use third-party cookies when working with outside partners for analytics and to optimize delivery of information that may be of interest to you. We do not have access to read or write such third-party cookies, nor do we directly control the manner in which they may be used.

Most browsers are initially set up to accept cookies, but can typically be configured to block all cookies or block all third-party cookies. Please be aware that our websites may not have full functionality for you if your browser is set to block some or all cookies. Depending on your location, you may also be prompted to provide your consent to all cookies, other than strictly necessary and functional cookies, each time you visit our websites. Any information about you collected by us is retained and protected in accordance with the laws governing your location.

To opt out of cookies that allow information to be delivered to you, such as targeted (or -interest-based") advertising, via third-party ad groups we may work with, there are options for controlling the ads you receive. Please note, however, that opting out does not prevent you from seeing the ads; it only makes them less relevant or tailored to your interests. One way you may opt out can be found at the National Advertising Initiative Consumer Opt Out website here. Security

We take appropriate measures to ensure the security of our Services. These include precautions to safeguard your personal information against loss, theft and misuse, as well as against unauthorized access, alteration, disclosure or destruction of data.

Despite our efforts to protect your personal information, there is always some risk that an unauthorized third party may find a way around our security systems or that transmissions of your information over the internet may be intercepted. Your use of our Services constitutes an acceptance of such risk. Accessing Our Data Servers

Various Wolfram Services offer some functionality for which they must access our data servers through the internet. When they do so, our data servers receive information similar to what our web servers receive when you visit our websites, as well as various Service-specific identifying information.

Specifically, using Wolfram|Alpha, or utilizing the Wolfram|Alpha functionality within other Services, will trigger the collection of information about the specific query. Some queries may require collecting additional information, such as session information covering the history of Wolfram Mathematica evaluations or the content of Wolfram Finance Platform notebooks containing the Wolfram|Alpha query. You can choose to prevent these Services from acces-

sing our servers by disconnecting from the internet or by using the Internet Connectivity item in the Help menu to tell the Service not to connect to the internet. If you choose not to allow these Services to access our servers, our Services will not be able to perform certain functions.

Under normal circumstances, we will never release information on accesses to our servers. We may, however, release information as described above in Disclosures of Your Information. Accessing Our Services from Third-Party Sources

This section is only applicable to Wolfram|Alpha and the Wolfram Cloud:

These Services may additionally be accessed through web widgets, scripts or gadgets that are embedded on third-party sites. If you choose to access these Services via such tools, then depending on the third-party technology, your personal information and input may be passed on to the third party's servers prior to being processed by our Services. Data Retention and the GDPR

We collect and hold personal data about our customers, users and enthusiasts, employees and others in the European Union who access our resources and services in a manner consistent with the lawful bases as outlined in the European Union's General Data Protection Regulation (GDPR). Please see the Data Retention Policy Addendum to Wolfram's Privacy Policies, which outlines our GDPR compliance in collecting, processing and using your personal data. It also describes how you can contact us to review any personal data and withdraw any consent you have given us to store it. Changes to This Privacy Policy

We may update or modify this Privacy Policy from time to time in the future. Any such updates or modifications shall be effective immediately upon their announcement. Please refer often to this document online for the latest information. Questions, Concerns and More Information

For information on policies related to the use of our Services, see our Legal portal.

If you have any questions or concerns about this Privacy Policy, you may contact us online, by email at myprivacy@wolfram.com or by US mail at Wolfram, Attn: Legal Department, 100 Trade Center Drive, Champaign, IL 61820-7237 USA.

By using our Services, you are telling us either that you are 18 years or older and legally able to form contracts, or that an adult with authority to act on your behalf has agreed to these terms and to be responsible for ensuring your compliance with them in your use of the Services and any results you obtain from them. If you don't want to be bound by these terms, do not use the Services or their results.

Revised September 27, 2019

YAHOO

Bron: https://www.verizonmedia.com/
policies/us/en/verizonmedia/privacy/products/searchservices/index.html

Yahoo Search Information Collection & Use Practices

Search

- When you conduct a search on a product or service that uses our search technology, we collect information from your experience, such as your search queries.
- Search Assist helps you find what you are looking for by automatically offering popular search terms and new topics to consider. Search Assist may base suggestions on aggregated searches across all users and your individual search history.
- The Yahoo Search History tool allows you to see what you've searched for in the past. Learn how to manage your Search History tool.
- When you use Yahoo Search, you may see relevant, private results selected from other sources, such as your Yahoo Mail. Only you can see your private search results when you're signed in. Learn how to manage, including turning off, Private Results.
- Some advertising you receive may be customized based on your searches or related terms at Verizon Media. Please visit our Opt-Out page to learn more about the information used to personalize your search experience. If you opt-out, you will continue to see ads Verizon Media serves on these websites, but they won't be customized to your interests or search history.
- Visit the Search Preferences page to manage your Yahoo Search experience, including Safe Search, Search History, and Private Results.
- Yahoo Search uses image recognition algorithms to identify public figures, scenes, actions, or objects to make it easier to search images.

Search Partners

- A variety of third party providers help power Verizon Media search and sponsored search services.
- We may share your search query, IP address, and other depersonalized information from your web browser or app, such as a unique identifier for your web browser, with these search partners.
- These third party providers may use this information, as well as your search results clicks, to provide more relevant advertising and search results, for search product improvement, research and analysis, and to help detect and defend against fraudulent activity on sponsored or contextual search results.
- We may reformat results provided by these search partners to provide an enhanced search experience to you.
- To learn more about the data collection and use practices by these search partners, please visit our Third Parties page.

Sponsored Search Results

- Search results may consist of sites that have paid for placement in the search results. Learn more.

- Search results may contain tracking URLs provided by Yahoo Search Marketing and/or our Search Partners to identify clicks from the search results page.

Assistants

- Yahoo Assistants are a new category of products and services using artificial intelligence guided by humans. These include chat bots operating in messenger platforms, virtual personal assistants and stand-alone apps accessed on Verizon Media or through third-party apps and services. Assistants may collection information about you in a manner different from other search technologies.
- Yahoo Assistants may interact and converse with you to answer questions, help complete tasks or perform other activities. Assistants rely on our personnel and automated systems to respond to questions or instructions from users.
- We may collect information about you when you use our Assistants, including your conversations and interactions with the Assistant, your Yahoo ID and information associated with your account.
- We may also collect information provided by a third-party (including apps, messaging platforms and other services) interacting with our Assistants, which could include: your account information with the third-party, such as user ID, name, photo, phone number, email address; and device information such as device ID, device type, operating system, and mobile carrier.
- Verizon Media's personnel and our automated systems may have access to all communications content as it is sent, received, and when it is stored, in order to fulfill your requests, further product and services development, and provide personalized experiences and advertising through Verizon Media's products and services.
- When you are communicating with our Assistants through a third-party, please read that company's privacy policy to better understand what information it may retain and for what purposes.
- Location information collected through the Yahoo Assistants may not appear in the Location Management page.

Other

Users who are European residents can request that certain URLs be blocked from search results in certain circumstances.

YANDEX

Bron: https://yandex.com/company/privacy

Our Commitment to Users' Privacy

For over twenty years, Yandex has served millions of users, working to maintain their trust

through our commitment to protecting their privacy and freedom of expression online. Our commitment to users is rooted in Yandex's wider responsibility to respecting human rights.

Data privacy and security is an important part of this commitment. Our detailed Privacy Policy helps users understand more about what data we collect, the reasons why we collect data, who has access to that data, and how users can control it. In addition to the detailed privacy policy, we also provide the following explanations to ensure our users understand our policies.

Reasons we collect user data At Yandex, it's our goal to help consumers and businesses better navigate the online and offline world. A large part of that is offering highly personalised services that cater to each individual user. Users are different, and data such as their preferences, location, and online history is critical to provide them with the best possible services. To that end, our services take into account various types of relevant data to personalise the experience for each user. For instance, our music streaming service Yandex. Music recommends artists or songs that match individual tastes of every user based on which songs they "likedänd which they skipped, among many other factors. Similarly, a user's search history helps Yandex choose the most relevant search results specifically for that user. Someone who enters [nevermind] in the search bar might be looking for a definition of "nevermind", while someone else may be searching for the Nirvana album. Personalising a user's experience using historical data improves both the current experience and helps Yandex to develop new products and services. And the more data we utilize, the better the experience we can provide to our users.

User data we collect We collect user data in two main ways – through Yandex profiles that users create and through users' interactions and activities on Yandex services. Yandex users can sign up for a Yandex.Passport, or profile, in which they manually enter their name, phone number, and other information, such as age, sex, location, and time zone. When users log in to our services or apps, data about their interactions with the service or app is automatically added to their Yandex.Passport profile. Yandex services automatically collect technical information such as cookie files, IP addresses, and geographic location to better understand users' preferences and settings. The amount of time we store users' data varies depending on which service and feature is being used and how actively our users manage their data settings. Some data is deleted when requested by a user, some data is deleted automatically, and some data is retained for longer periods of time to operate our various services effectively.

How we protect our users' data Yandex takes your data security very seriously and follows rigorous data protection rules to ensure our users' data is secure and their privacy is protected. All data is processed automatically in our system, and we prohibit access to the data by any individual other than in times of necessity such as for Yandex customer support or other obligatory administrative and technical help. We also always encrypt all stored confidential information, such as passwords. Our technological infrastructure securely protects the data that we handle. We implemented a secure HTTPS protocol for all Yandex services, meaning all data is encrypted as it moves between the user and Yandex. We also integrated special protection measures where security is particularly important, such as processing online payments according to the international PCI DSS security standard.

Instances in which we share our users' data Protecting user's data is a priority for Yandex and it's important for our users to know about the instances in which we share users' data and why. Yandex does not sell or share user data with third parties but does share necessary data with some partners in order to provide Yandex services; we also share aggregated user data through our web analytics tools, and to satisfy legal requests. Yandex shares select data with a partner when it's necessary to operate a service. For instance, Yandex.Taxi works with taxi companies and their drivers require information about a user's location so that they can pick up the passengers. Similarly, when a user buys concert tickets through our ticketing service, Yandex.Afisha, the venue box office needs the user's information to be able to deliver the tickets to the user. Some of our analytics services, such as our web analytics reporting tool Yandex.Radar, provide aggregated statistics on user behavior. However, these services do not receive any personal information on individual users and strictly provide aggregated reporting. In some cases, Yandex may be required to provide user data by law. Yandex complies with the laws and regulations in areas in which it operates, including legal requests for information. If we receive a formal request for user data, our top priority is to protect users and we first ensure that there is legal ground for the request. If we find that the request is legitimate, we comply with the authorities to provide only the amount of data absolutely necessary to fulfil the request. If we find that the request is without merit, we refuse to fulfil the request and work with respective authorities to ensure strict compliance with the applicable law. Among other things, email correspondence of Yandex users can only be accessed on the basis of an official court order related to a particular user as we protect the secrecy of correspondence under Russian law.

How our users can control their data It's vital to Yandex to provide our users with information about how they can control and manage their personal data. Users can view part of the data, including personal information, available to Yandex and its services on Yandex.Passport. You can edit or delete this information, or change the settings of your personal Yandex account, at any point. Yandex users and all Internet users have the ability to further control their data through their browser settings by managing their cookies. Yandex.Browser's Help page outlines information about the use of cookies and any related privacy risks and tells users about the ways in which they can customize their settings. If you have any further questions or for more details about how Yandex processes user data, please read our Privacy Policy. To submit any concerns about privacy online, please visit the appropriate support page. You can navigate to the proper form for the relevant service and submit more detailed information about issues in the feedback form.