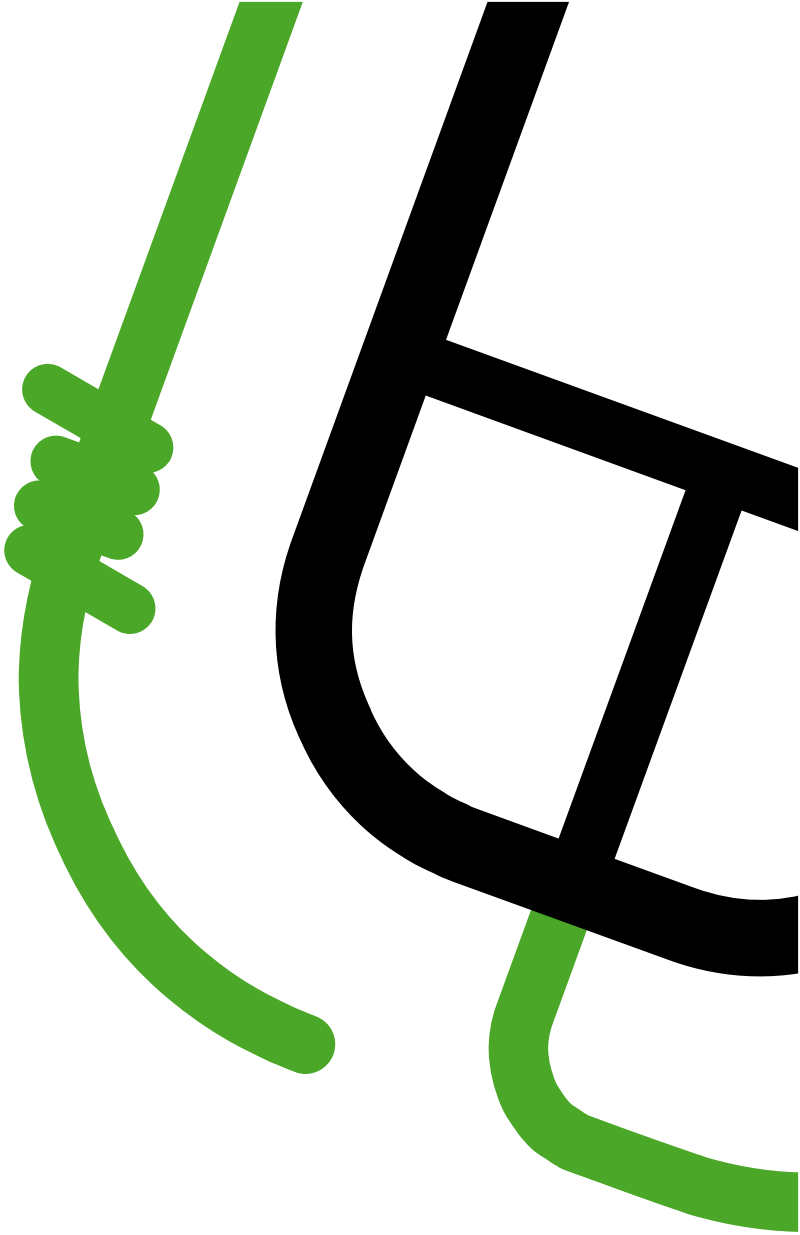
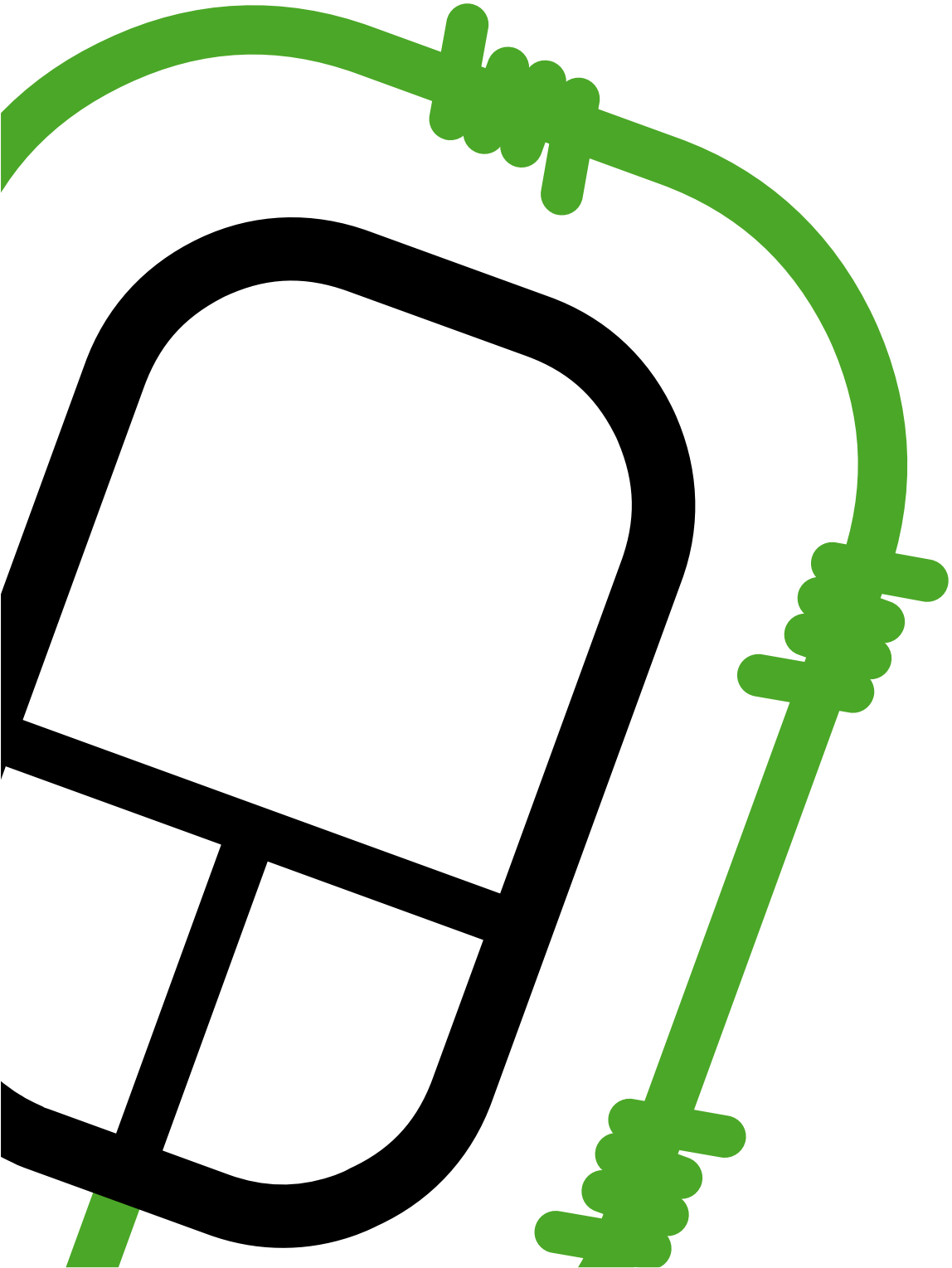
PRIVACY: VAN KENNIS TOT GEDRAG



Door: Renushka Madarie

1 juli 2016

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN



Soms zeggen mensen dat ze meer privacy willen, maar delen ze uiteindelijk toch veel informatie over zichzelf online. Dit fenomeen staat bekend als de privacyparadox. Eén van de verklaringen voor de privacyparadox is wellicht gebrek aan praktische kennis over het beschermen van je online privacy. Dit onderzoek richt zich op de relatie tussen kennis van privacytools en -issues enerzijds en, onder andere, bezorgdheid en daadwerkelijk privacybevorderend gedrag anderzijds. Uit de resultaten blijkt dat de relatie tussen kennis van privacytools en bezorgdheid afhankelijk is van hoeveel kennis mensen hebben van privacyissues. Ook blijkt dat privacybevorderend gedrag sterker gerelateerd is aan kennis over privacytools dan aan kennis over privacyissues.

INHOUD

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Bits of Freedom. Komt op voor jouw vrijheid en privacy op internet. Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd. Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam
020 – 123456789

info@bof.nl

01. WAAROM HOU JIJ JE BEZIG MET PRIVACY?

Waarom heb jij je cookie-instellingen aangepast? En waarom gebruik jij een VPN? Deze vragen kan je op meerdere manieren interpreteren en daar volgen logischerwijs verschillende antwoorden op. Een principieel antwoord zou kunnen zijn dat je zelf wilt bepalen welke informatie je deelt. Een technisch antwoord kan gaan over metadata en versleuteling. En een psychologisch antwoord? Wat heeft er toe heeft geleid dat jij privacybevorderend gedrag bent gaan vertonen? Grote kans dat je dat niet meer goed kunt navertellen. Toch is het waarschijnlijk dat je niet *out of the blue* overvallen bent door de gedachte "Vanaf nu ga ik mijn gegevens beter beschermen!"[1] Welke stappen vooraf lijken te gaan aan privacybevorderend gedrag zijn onderzocht in het onderzoek dat in dit rapport wordt besproken.

Inmiddels zijn meerdere factoren onderzocht die leiden tot privacybevorderend gedrag of dergelijk gedrag juist afremmen. De intentie hebben om tot gedrag over te gaan en bezorgdheid over privacy lijken belangrijke factoren.[2,3,4] Soms komt in onderzoeken een tegengesteld beeld naar voren wat betreft de intentie om privacybevorderend gedrag te tonen: mensen willen meer privacy, maar wanneer het er op aan komt, delen ze toch veel persoonlijke informatie online. Dit fenomeen staat ook wel bekend als de privacyparadox.[5] De privacyparadox is echter niet echt een paradox. Privacy kan wel belangrijk worden gevonden, maar hoeft niet altijd op te wegen tegen, bijvoorbeeld, financiële beloningen (denk korting en cadeautjes) of een gevoel van verbondenheid (denk sociale netwerken).[6,7] Daar komt bij dat privacy niet in elke context even belangrijk wordt gevonden.[8] Zo wordt bescherming van medische gegevens bijvoorbeeld belangrijker gevonden dan bescherming van foto's van je avondmaaltijd, ondanks dat al die foto's van je avondmaaltijd misschien ook wel veel zeggen over je fysieke en mentale gesteldheid. Tot slot kan de privacyparadox ook een gevolg zijn van een gebrek aan kennis over manieren waarop mensen hun privacy kunnen beschermen.[9] Zo kan iemand misschien wel anoniem willen blijven op het internet, maar simpelweg niet weten hoe dat moet.

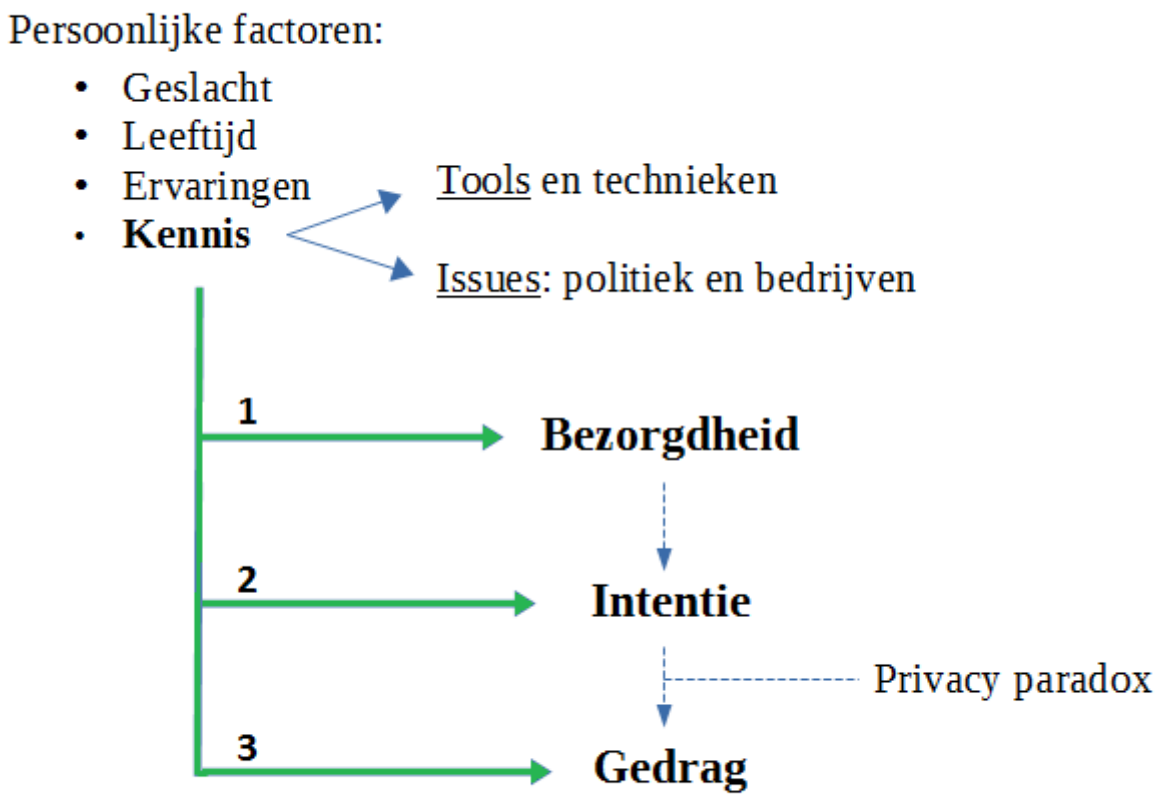
Bezorgdheid over privacy kan privacybevorderend gedrag beïnvloeden, maar wordt zelf ook weer beïnvloed door een aantal factoren. In de literatuur wordt onderscheid gemaakt tussen omgevingsfactoren en persoonlijke factoren.[10] Omgevingsfactoren zijn minder goed onderzocht en komen in dit onderzoek ook niet aan bod. Persoonlijke factoren die onderzocht zijn, zijn onder andere: persoonlijkheid, geslacht, leeftijd, negatieve ervaringen, en de perceptie van andermans privacy.[11] Bijvoorbeeld, negatieve ervaringen op het gebied van privacy leiden tot meer bezorgdheid over privacy en ouderen zijn over het algemeen bezorgder over hun privacy dan jongeren.[12]

Deze afbeelding is gebaseerd op Carnitas poutine with bacon gravy van Jessica Spengler, uitgebracht onder een Creative Commons Attribution 2.0

Hoe deze verschillende factoren direct of indirect gerelateerd zijn aan privacybevorderend gedrag is weergegeven in figuur 1. De persoonlijke factor die in dit rapport centraal staat is privacybewustzijn.

02. PRIVACYBEWUSTZIJN

Privacybewustzijn kan worden omschreven als aandacht voor of weet hebben van privacypraktijken en de risico's daarvan.[13,14] Dit omvat bijvoorbeeld weten of organisaties informatie over jou hebben en hoe deze informatie wordt gebruikt. Eerder onderzoek heeft relaties aangetoond tussen privacybewustzijn en bezorgdheid over privacy. Zo is gebleken dat mensen bezorgder zijn over hun privacy naarmate ze het minder acceptabel vinden dat hun gegevens voor andere doeleinden worden gebruikt dan oorspronkelijk is toegezegd door de organisatie die hun gegevens heeft verwerkt. Mensen die dit delen van persoonlijke gegevens zonder toestemming minder acceptabel vinden weten vaak ook minder goed hoe zij ongewenste e-mails van organisaties kunnen weren.[15] Wanneer organisaties toestemming vragen voor het verzamelen en gebruiken van gegevens, lijken privacyzorgen af te nemen.[16] Voor het huidige onderzoek is privacybewustzijn vertaald naar "kennis over online privacy". Kennis over online



Figuur 1. Relaties die zijn onderzocht in dit onderzoek.

privacy omvat hier kennis over online privacytools en -technieken, en kennis over privacyissues die op de agenda van Bits of Freedom staan. De volgende hoofdvraag is opgesteld voor dit onderzoek:

Zijn kennis over online privacy en online privacybevorderend gedrag aan elkaar gerelateerd?

Om deze vraag te beantwoorden is een aantal subvragen opgesteld:

1. Is er een relatie tussen kennis over online privacy en bezorgdheid over online privacy?
2. Is er een relatie tussen kennis over online privacy en de intentie tot privacy-bevorderend gedrag?
3. Is er een relatie tussen kennis over online privacy en daadwerkelijk privacybevorderend gedrag?

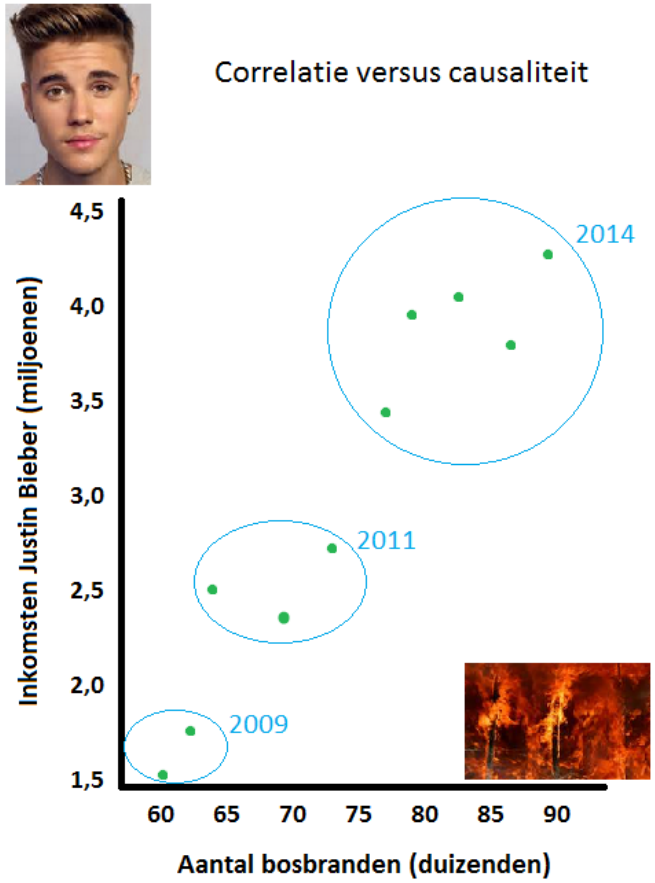
03. OPZET ONDERZOEK

Om de hoofdvraag en subvragen te onderzoeken, is een vragenlijst opgesteld. De geanalyseerde vragen, antwoordopties, en statistieken per vraag staan in bijlage A. De vragenlijst is online verspreid. Bits of Freedom heeft de vragenlijst aangekondigd in een blog op haar website, op haar Facebookpagina, op haar Twitteraccount en in haar nieuwsbrief. Daarnaast is de vragenlijst ook aangekondigd op de websites van Tweakers en het Criminologisch Netwerk Nederland. Tot slot is de vragenlijst verspreid in het persoonlijke netwerk van medewerkers van Bits of Freedom. De vragenlijst heeft ongeveer drie weken open gestaan. In totaal hebben 1224 personen de vragenlijst geopend. Het aantal vragenlijsten dat volledig is ingevuld, is 1023.

04. WIE DEDEN MEE AAN HET ONDERZOEK?

Ongeveer driekwart van de respondenten is man en 17,1% is vrouw. Een kleine minderheid (4,2%) kon of wilde zich niet plaatsen in de categorie man of vrouw. De gemiddelde leeftijd van de respondenten is 43,5 jaar. De jongste respondent was 15 jaar, de oudste 77. Driekwart van de respondenten heeft weleens minstens één van de volgende negatieve ervaringen op het gebied van privacy zelf meegemaakt: (1) censuur, (2) per ongeluk persoonlijke gegevens invullen op een fraudulente website, (3) weten dat je telefoonnummer bij onbekenden (personen of organisaties) terecht is gekomen, (4) identiteitsfraude. De betrokkenheid bij Bits of Freedom was vrij groot onder de respondenten. Betrokkenheid bij Bits of Freedom werd gemeten met de vraag hoe goed respondenten op de hoogte waren van de activiteiten van Bits of Freedom. De antwoordschaal liep van 1 (zeer slecht) tot en met 5 (zeer goed). Hoewel deze vraag niet verplicht was, hebben slechts 37 respondenten deze vraag niet ingevuld. Bijna tweederde van de respondenten die de vraag wel hebben ingevuld, gaf zichzelf een score van 4 of hoger op deze schaal.

Een ruime meerderheid van de respondenten (902; 88,2%) gaf aan zowel een smartphone als een computer regelmatig te gebruiken. Verder gaven 114 (11,1%) respondenten aan alleen een computer regelmatig te gebruiken en 6 (0,1%) respondenten gaven aan alleen een smartphone te gebruiken. Slechts één respondent gebruikt nauwelijks of nooit een smartphone en computer. De groep van respondenten die alleen een smartphone of een computer gebruikt verschilt op demografische kenmerken van de groep van respondenten die zowel een smartphone als computer gebruikt alléén qua leeftijd. Gebruikers van óf een smartphone óf een computer zijn gemiddeld iets ouder (51,6 jaar) dan gebruikers van zowel een smartphone als een computer (42,5 jaar).



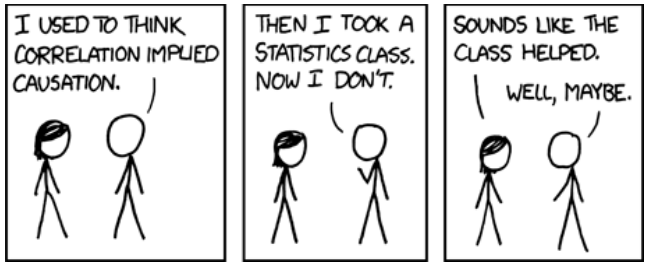
Figuur 2. Correlatie impliceert geen causaal verband. NB: de gegevens in deze grafiek zijn niet op feiten gebaseerd.

05. EEN NOOT OVER CORRELATIES

Veel van de analyses in dit onderzoek zijn gebaseerd op correlaties. Belangrijk om te weten over correlaties is dat deze geen causaal verband (oftewel, een oorzaak-gevolg relatie) impliceren. Correlaties kunnen wel een aanwijzing zijn voor causale verbanden, maar bieden geen sluitend bewijs. Dit komt omdat er dikwijls meerdere verklaringen zijn voor de gevonden correlaties. In dit onderzoek is dan ook geen causaliteit onderzocht, maar waar mogelijk wordt causaliteit wel logisch beredeneerd. Weet je nog niet wat een correlatie is, wil je wel leren wat het is, en misschien zelfs een nobele poging doen de statistiek in bijlage C te begrijpen, sla dit stuk dan niet over. Het lezen van de informatie in deze paragraaf is echter geen vereiste om de rest van het rapport te begrijpen.

In gewone mensentaal kan “correlatie” worden vertaald naar samenhang, of verband, of je denkt “cor” weg en komt uit op het meer simpele “relatie”. Dat is het dan ook. Een relatie tussen X en Y. Niets meer, niets minder. Tussen allerlei dingen kun je ~~cor~~relaties (verbanden, samenhang) onderzoeken. Tussen het aantal koeien en bloemen in de wei, tussen de gezondheid van een boom en de hoeveelheid Wi-Fi in de buurt van die boom[17], tussen het testosterongehalte van bankiers en de risico’s die zij nemen[18], et cetera. Een ~~cor~~relatie kan variëren in sterkte (zwak, sterk) en richting (positief, negatief). Bij een positieve relatie stijgt A wanneer B ook stijgt. Bij een negatieve relatie stijgt A terwijl B daalt. Een zwakke positieve relatie is bijvoorbeeld de hoeveelheid regen op een dag en de hoeveelheid gezeur van je partner. Hoe meer regen, hoe meer gezeur, maar het gezeur is ook afhankelijk van heel veel andere dingen. Er wordt dus niet áltijd meer gezeurd wanneer het meer regent. Een sterke negatieve relatie is bijvoorbeeld het aantal kattenplaatjes op internet en de hoeveelheid werk die wordt verzet. Voor iedereen geldt: hoe meer kattenplaatjes je online ziet, hoe minder uren je besteedt aan werk. Kan hieruit worden afgeleid dat katten je van het werk houden? Nee, want gebrek aan werk kan ook leiden tot een grotere behoefte aan afleiding door De Kat. Een relatie tussen A en B betekent dus niet automatisch dat A tot B leidt of andersom. Tot slot moet ook rekening worden gehouden met het feit dat andere factoren ten grondslag kunnen liggen aan een relatie tussen A en B. In figuur 2 is geschetst hoe het aantal bosbranden stijgt met het succes van Justin Bieber. Echter,

wanneer de meetmomenten worden gegroepeerd per jaartal lijkt het verstrijken van de tijd een rol te spelen in de geschetste relatie.



06. KENNIS EN ZORGEN

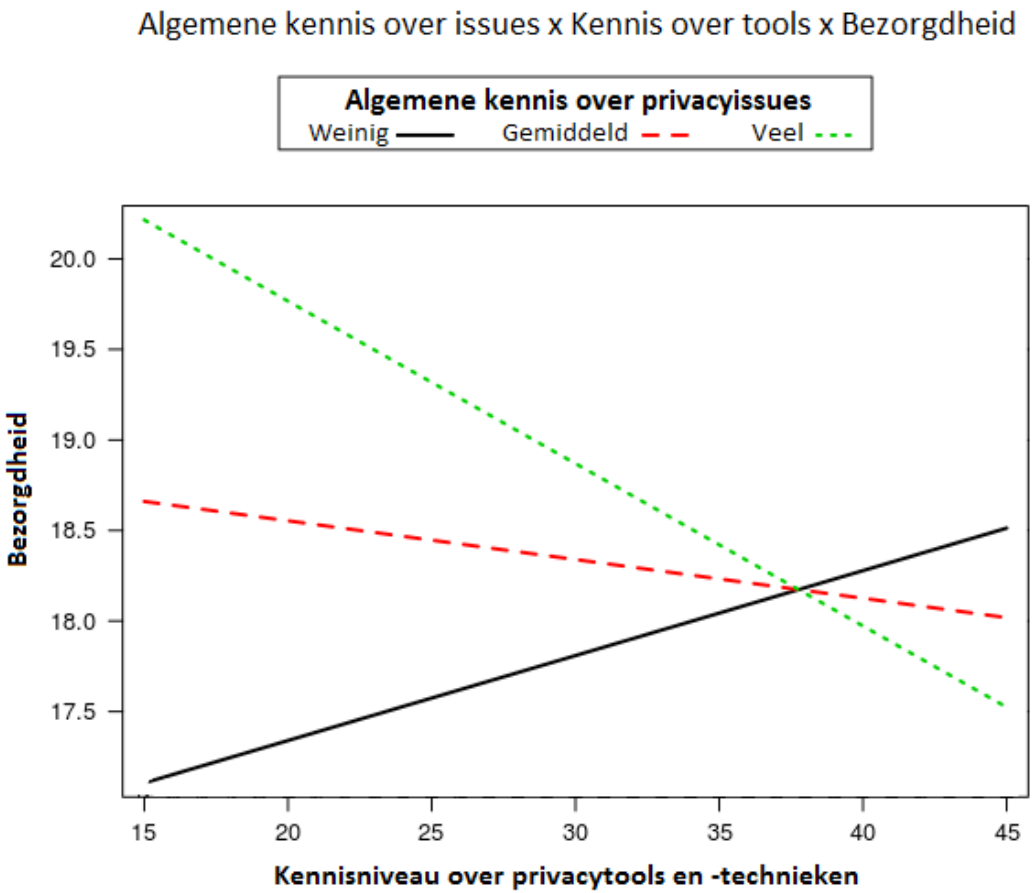
Vragen

Privacykennis is gedefinieerd als kennis over privacytools en -technieken enerzijds en kennis over privacyissues anderzijds. Zo is bijvoorbeeld gevraagd hoe goed respondenten bekend zijn met Tor, VPN, spyware en cookies.[19] Kennis over privacyissues is gemeten aan de hand van zes stellingen en twee open vragen. Een voorbeeld van een stelling is: “Er bestaat een gezichtsherkenningsapp waarmee je foto’s van mensen kunt koppelen aan hun profiel op sociale media.” Respondenten konden bij iedere stelling aangeven of zij wisten of dachten dat de stelling juist of onjuist was. Het antwoord bij een stelling werd goed gerekend als de respondent het juiste antwoord (vrij) zeker wist. Een vraag werd *bijna goed* gerekend als de respondent het juiste antwoord dacht te weten. Een voorbeeld van een open vraag is: “Sinds 1 januari 2016 zijn organisaties verplicht ernstige datalekken te melden. […] Vraag: Hoeveel datalekken zijn er […] tot en met halverwege mei binnen gekomen?” Voor een “goed” antwoord is een foutmarge van ongeveer 12% toegepast. Voor een “bijna goed” antwoord is een foutmarge van ongeveer 30% toegepast. De motivering voor deze foutmarges is te vinden in bijlage A onder de punt 6: “Open vragen”. Het totaal aantal goede vragen is in dit onderzoek gebruikt als indicator voor “expert kennis”. De som van het totaal aantal goede en bijna goede vragen is in dit onderzoek gebruikt als indicator voor “algemene kennis”.

Bezorgdheid is gemeten aan de hand van vijf vormen van privacyschending. Op een schaal van 1 (helemaal niet) tot 5 (heel erg) konden respondenten aangeven hoeveel zorgen zij zich maken over deze verschillende vormen van privacyschending.[20, 21]

Resultaten

Respondenten die alleen een computer of smartphone regelmatig gebruiken, scoorden iets lager op de kennisvragen over privacytools en -technieken dan de respondenten die zowel een computer als smartphone regelmatig gebruiken. Ook had de eerste groep iets minder expert kennis over privacyissues dan de tweede groep. Omdat de groepen verschillen qua kennisniveau zijn deze niet samengevoegd. Als er bijvoorbeeld een relatie is tussen kennis en zorgen in de eerste groep, maar niet in de tweede groep, dan kan deze relatie uitblijven in de analyse van de samengestelde groep. Dit zou suggereren dat er geen relatie is terwijl die wel bestaat, maar slechts in een bepaalde groep. Omdat vrij weinig respondenten óf een computer óf een smartphone regelmatig gebruiken, hebben de resultaten in dit rapport alleen betrekking op de groep respondenten die zowel een computer als smartphone regelmatig gebruiken. Bij elke analyse in dit rapport is ook nog gecontroleerd voor de invloed van betrokkenheid bij Bits of Freedom (zie bijlage C voor uitleg hierover).



Figuur 3. Interactie tussen algemene kennis over privacyissues, kennis over privacytools en -technieken en hoe bezorgdheid over privacy.

Kennis over privacytools en -technieken, en kennis over privacyissues lijken in eerste instantie niet gerelateerd te zijn aan hoe bezorgd iemand is over zijn of haar privacy. Wanneer kennis over tools en technieken, en algemene kennis over privacyissues worden gecombineerd, blijkt er wel een relatie te zijn tussen deze persoonskenmerken en bezorgdheid. De relatie tussen kennis van tools en technieken, en bezorgdheid is afhankelijk van hoeveel algemene kennis iemand van privacyissues heeft. Deze relatie is geschetst in figuur 3. Voor mensen die veel algemene kennis hebben, geldt: hoe meer kennis van tools en technieken, hoe minder bezorgd zij zijn over hun privacy. Voor mensen die weinig algemene kennis hebben van privacyzaken geldt het omgekeerde: hoe meer kennis zij hebben van tools en technieken, hoe bezorgder zij zijn over hun online privacy. Let op, deze bevindingen impliceren niet dat mensen bezorgder worden over hun privacy wanneer ze meer kennis over privacytools en -issues vergaren. Het is ook mogelijk dat mensen met meer zorgen over hun privacy meer informatie zoeken over hoe zij zichzelf kunnen beschermen, of meer informatie zoeken om hun bezorgdheid te bevestigen. Omdat geslacht, leeftijd, en eerdere negatieve ervaringen op het gebied van online privacy ook van invloed kunnen zijn op bezorgdheid over online privacy, is ook naar deze persoonlijke factoren gekeken. Zoals eerder gezegd, zijn negatieve ervaringen gemeten door aan

respondenten te vragen of zij de volgende gebeurtenissen zelf hebben meegemaakt: censuur, identiteitsfraude, onbekenden die je telefoonnummer hebben, en het per ongeluk invullen van je gegevens op een fraudulente website. De geslachtscategorie “anders” is bij deze analyses buiten beschouwing gelaten, omdat veel respondenten die voor deze optie kozen ook geen antwoord gaven op de vragen naar hun leeftijd en opleidingsniveau. Dit doet vermoeden dat veel respondenten in deze geslachtsgroep de “anders”-optie hebben gebruikt om hun geslacht niet op te geven, in plaats van dat zij zich daadwerkelijk niet kunnen plaatsen in de categorie “man” of “vrouw”. Bovendien is de “anders”-groep te klein om apart te analyseren.

Uit de analyses is gebleken dat geslacht, leeftijd, en eerdere negatieve ervaringen inderdaad bezorgdheid over online privacy beïnvloeden. Vrouwen lijken zich meer zorgen te maken dan mannen en hoe ouder iemand is, hoe bezorgder diegene is. Verder blijkt ook dat – niet geheel verrassend – hoe meer negatieve ervaringen mensen hebben meegemaakt, hoe bezorgder zij zijn over hun online privacy.

07. KENNIS EN INTENTIE

Vragen

In de vragenlijst werd gevraagd waar respondenten nog meer over zouden willen leren. Deze vraag diende ter informatie voor Bits of Freedom om een indicatie te krijgen waar zij haar volgers meer of beter over kan informeren. Daarom is de vraag niet verplicht gesteld. De antwoorden op deze vraag zijn ook geïnterpreteerd als een intentie tot privacybevorderend gedrag. Onderwerpen waar respondenten uit konden kiezen waren onder andere: Veilig internetten, beveiliging van je telefoon, en politiek en privacy. In totaal hebben 799 (88,6%) respondenten minstens één optie aangevinkt. Voor deze onderzoeksvraag zijn kennisvragen geanalyseerd, dus wordt hier weer alleen gekeken naar de groep respondenten die zowel een smartphone als computer regelmatig gebruikt. Omdat niet duidelijk is of respondenten de vraag hebben overgeslagen, of niet geïnteresseerd waren in de onderwerpen, zijn alleen de 799 respondenten die minstens één optie hebben aangevinkt, meegenomen in deze analyse.

Resultaten

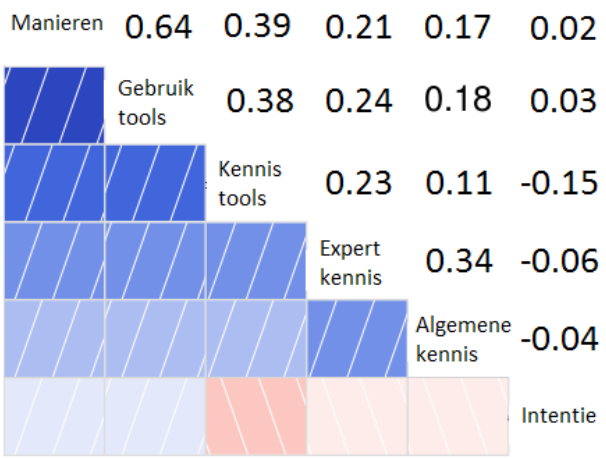
Over de relatie tussen kennis en intentie kan gezegd worden dat meer kennis over privacytools en -technieken leidt tot minder interesse in het leren over privacyonderwerpen. Hoewel ook hier slechts correlaties zijn onderzocht, is het in dit geval logischer dat de relatie één kant op gaat: meer kennis over tools en technieken leidt er toe dat iemand minder geneigd is om op zoek te gaan naar nieuwe informatie. Als iemand meer zou willen leren, kan dat niet plots leiden tot een aftakeling van zijn of haar kennis. Tussen kennis over privacyissues en intentie om meer te leren kon geen relatie worden ontdekt. Hierbij moet worden opgemerkt dat de intentievragen vooral gefocust waren op privacytools en -technieken, en niet zozeer op privacyissues. Tot slot blijkt dat bezorgdheid over online privacy en meer willen leren ook gerelateerd zijn. Hoe bezorgder iemand is, hoe meer privacyonderwerpen hem of haar interesseren.

08. KENNIS EN GEDRAG

Vragen

Om daadwerkelijk privacygedrag te meten is gekeken naar het gedrag dat mensen nu vertonen. Respondenten werden gevraagd op welke manieren zij zich momenteel bezighouden met online privacy. Dit waren vragen over het gebruik van (grotendeels) dezelfde privacytools en -technieken die aan bod

kwamen bij de kennisvragen over privacytools en -technieken. Daarnaast is nog gevraagd op welke manieren respondenten bezig zijn met online privacy anders dan het gebruik van privacytools en -technieken. Voorbeelden van andere manieren zijn: praten met vrienden over online privacy of organisaties volgen die zich bezighouden met online privacy.



Figuur 4. Correlaties tussen factoren die zijn onderzocht.

Resultaten

In figuur 4 is te zien hoe kennis en gedrag aan elkaar gerelateerd zijn. Een blauwe kleur laat een positieve relatie zien. Een rode kleur laat een negatieve relatie zien. Zoals eerder gezegd is er een positieve relatie wanneer X en Y samen stijgen. Een negatieve relatie betekent dat X groter wordt, terwijl Y kleiner wordt. Daarnaast geldt dat relaties sterker zijn naarmate de kleur donkerder wordt.

Uit figuur 4 valt af te leiden dat mensen die vaak tools en technieken gebruiken om hun privacy te beschermen, ook vaker op andere manieren bezig zijn met het onderwerp ‘online privacy’. Verder is het bezig zijn met online privacy (zowel door tools te gebruiken als op andere manieren) sterker gerelateerd aan de hoeveelheid kennis van privacytools en -technieken dan aan de hoeveelheid kennis van privacyissues. Oftewel, je bezig houden met privacy lijkt sterker gerelateerd aan kennis over oplossingen (weten hoe jij je privacy vergroot) dan aan kennis over problemen (weten dat je privacy wordt bedreigd). Dit resultaat bevestigt het idee dat een gebrek aan praktische kennis over hoe je privacy te vergroten, bijdraagt aan de privacyparadox[22].

In figuur 4 is ook de relatie tussen intentie enerzijds en kennis van tools en issues en privacygedrag anderzijds te zien. Een relatie tussen intentie en gedrag is hier zo goed als afwezig. Dit heeft waarschijnlijk te maken met het feit dat gevraagd is naar wat respondenten nog meer zouden willen leren in plaats van wat ze nog meer zouden willen doen. Om een relatie tussen intentie en gedrag in het vervolg aan te tonen, zouden de intentie- en gedragvragen wellicht ook beter gematcht kunnen worden[23]. Bijvoorbeeld, wanneer gevraagd wordt hoe vaak iemand een VPN gebruikt, moet ook gevraagd worden hoe vaak iemand een VPN wil gebruiken, in plaats van of iemand meer privacytools (in het algemeen) wil gebruiken.

09. CONCLUSIE

Dit onderzoek was gericht op de relaties tussen privacykennis, privacyzorgen, intenties tot privacy-bevorderend gedrag, en daadwerkelijk privacy-bevorderend gedrag. Uit de resultaten kan worden afgeleid dat de relatie tussen kennis en zorgen complex is. De relatie tussen kennis over privacytools en -technieken en bezorgdheid is afhankelijk van hoeveel algemene kennis over privacyissues mensen hebben. Kennis van tools en technieken heeft ook invloed op de intentie om meer privacybevorderend gedrag te tonen. Hoe meer kennis, hoe minder sterk de intentie om meer te leren over privacy. Tot slot zijn privacykennis en privacygedrag vrij sterk aan elkaar

gerelateerd. Deze relatie is het sterkst voor de kennis van tools en technieken en het gebruik van tools en technieken.

BIJLAGE A. DE VRAGENLIJST

Hieronder vind je de vragen zoals die aan de respondenten gesteld zijn. Alleen de vragen die geanalyseerd zijn, zijn in deze bijlage opgenomen.

De vragenlijst was gemaakt en verspreid met het programma LimeSurvey. De resultaten zijn geanalyseerd met het programma voor R.

1. Welke van de volgende apparaten heb je in je bezit of gebruik je regelmatig?

- Smartphone
- Computer/laptop
- Allebei: zowel smartphone als computer/laptop
- Geen van beide

2. Hoe bekend ben je met de volgende zaken?
Schaal: Nooit van gehoord – ken ik van naam – basale kennis – enige technische kennis – diepgaande technische kennis

Subvragen:

- Tor
- VPN
- Versleuteld mailen
- Cookies
- https://
- Spyware
- Metadata
- Man-in-the-middle attack
- Browser plug-ins

3. Hoe vaak ben je op de volgende manieren bezig met het onderwerp 'online privacy'?
Schaal: Nooit – nauwelijks – soms – vaak – (bijna) altijd

Subvragen:

- Expres onjuiste gegevens opgeven
- De privacyinstellingen van internetdiensten doorlopen en aanpassen
- Specifieke chat apps gebruiken uit privacy- of veiligheidsoverwegingen
- Organisaties die zich inzetten voor privacy volgen
- Praten met vrienden over privacygerelateerde onderwerpen

4. Hoe vaak pas je de volgende technieken toe om je privacy te vergroten?
Schaal: Schaal: Nooit – nauwelijks – soms – vaak – (bijna) altijd

Subvragen:

- Tor
- VPN
- Versleuteld mailen
- Aangepaste cookie-instellingen
- Browser plug-ins (bijv. HTTPS Everywhere of Privacy Badger)
- Een code om je telefoon of simkaart te ontgrendelen
- De GPS-functie op je telefoon alleen aanzetten wanneer je deze nodig hebt

5. Stellingen:
De stelling over netneutraliteit ("Internetproviders mogen specifieke online diensten, zoals Spotify en Netflix, gratis aanbieden") is er uit gehaald. Deze was in eerste instantie zo geformuleerd dat het "juiste antwoord" niet juist was. De respondenten die de vragenlijst invulden vóór dit gecorrigeerd was, scoorden dan ook anders (vaker "onjuist") dan de respondenten die de vragenlijst invulden na de correctie (vaker "juist").

- De politie mag inmiddels webcams en microfoons van de computers van verdachten hacken om ze te observeren.

- Google maakt gebruik van de inhoud van berichten die van en naar Gmailaccounts zijn verzonden om gerichte advertenties te tonen.
- Wanneer je foto's en video's op Facebook plaatst, dan mag Facebook zelf bepalen wat zij daar vervolgens mee doet.
- Er bestaat een gezichtsherkenningsapp waarmee je foto's van mensen kunt koppelen aan hun profiel op sociale media.
- In 2015 was in Nederland het aantal slachtoffers van geweldsmisdrijven en het aantal slachtoffers van (poging tot) inbraak bij elkaar opgeteld nog altijd hoger dan het aantal mensen dat werd gehackt.

6 Open vragen:

De foutmarges op deze vraag zijn bepaald door te kijken naar het antwoordpatroon van de respondenten. Bij de eerste vraag waren er bijvoorbeeld relatief weinig mensen die het goede antwoord (36 landen) wisten, maar vrij veel mensen gaven '40' aan. Minder mensen noemden een getal tussen de 41 en 44, terwijl weer meer mensen '45' zeiden. Zo ging het ook de andere kant op met de getallen 30 en 25. Deze getallen zijn daarom gekozen als grenzen voor 'juist' en 'bijna juist' en komen neer op een foutmarge van respectievelijk ongeveer 12% en 30%. Dezelfde methode is toegepast op de tweede vraag.

- Het Italiaanse bedrijf Hacking Team levert spionagesoftware aan overheden. Vraag: Van hoeveel landen is het bekend dat zij Hacking Team hebben betaald voor spionagesoftware?
- Sinds 1 januari 2016 zijn organisaties verplicht ernstige datalekken te melden. Bij datalekken gaat het om persoonsgegevens die bijvoorbeeld zijn gelekt, gestolen, of gewijzigd zonder dat de organisatie daarvan wist. Vraag: Hoeveel datalekken zijn er in vier en een halve maand (oftewel, tot en met halverwege mei) binnen gekomen?

7. Hoe bezorgd ben je dat…

Schaal: 1 (Helemaal niet) tot en met 5 (Heel erg)

- ...er inbreuk wordt gemaakt op jouw privacy wanneer je het internet gebruikt?
- ...er te veel persoonlijke informatie van je wordt gevraagd wanneer jij je ergens registreert of wanneer jij online aankopen doet?
- ...er informatie over jou gevonden kan worden op jouw oude computer of telefoon?
- ...je e-mail ontvangt van personen (of organisaties) die zich voordoen als iemand (of iets) anders?
- …de berichten die je online verstuurt, gelezen kunnen worden door iemand anders dan de persoon of organisatie voor wie de berichten bedoeld zijn?

8. Waar zou de overheid de meeste aandacht aan moeten besteden volgens jou?

Bij deze vraag is onderzocht of de rangorde samenhangt met, onder andere, kennisniveau en privacybevorderend gedrag. Kennisniveaus van zowel privacytools als privacyissues waren niet gerelateerd aan de verdeling van de onderwerpen over de rangen. Wel bleek bijvoorbeeld dat mensen die meer bezig zijn met online privacy het onderwerp internetcriminaliteit een hogere rang gaven dan mensen die minder bezig zijn met online privacy.

Onderwerpen:

- Handhaven van het recht op vrijheid van meningsuiting.

- Bevorderen van de controle van burgers over gegevens die zij online delen met organisaties.
- Aanpakken van geweld op straat.
- Aanpakken van internetcriminaliteit.
- Beschermen van persoonsgegevens.

9. Over welke onderwerpen zou je graag meer willen weten?

	% aangevinkt
Veilig gebruik maken van het internet	45,9
Computerbeveiliging	35,9
Telefoonbeveiliging	34,2
Tabletbeveiliging	20,6
Politiek en privacy	63,7
Alternatieven voor internetdiensten die je privacy schenden	69,5

BIJLAGE B. 1023 RESPONDENTEN

De meerderheid van de respondenten is man (78,2%), 17,5% is vrouw, en 4,1% wilde of kon niet kiezen tussen de categorieën man en vrouw. De gemiddelde leeftijd was 43 jaar. De jongste respondent was 15 jaar, de oudste 77. Ongeveer 8% van de respondenten zit op de middelbare school of heeft de middelbare school als hoogste opleidingsniveau. Weer 8% gaf MBO als hoogste opleidingsniveau aan. Ongeveer driekwart is hoger opgeleid, dat wil zeggen HBO of hoger. Het aantal werkzame respondenten is 70,4%, terwijl het aantal studerende respondenten 7,4% is. De rest (22,2%) was niet werkzaam of wilde niet zeggen of hij/zij werkzaam is. De sectoren waarin studerende respondenten wilden werken na hun studie is zeer divers. De meest gekozen sector is ICT (41,6%). Op de tweede plaats staat Onderwijs/Opleiding/Onderzoek (9,1%) en op de derde plaats staat de Overheid (6,5%). Dezelfde verdeling volgt wanneer gekeken wordt naar de sectoren waarin werkzame respondenten werken: ICT (22,7%), Onderwijs/Opleiding/Onderzoek (5,8%), en Overheid (3,7%).

De meest voorkomende privacyschending bij de respondenten was dat hun telefoonnummer bij personen of organisaties terecht was gekomen die zij niet eerder zelf hebben gecontacteerd (71,3%). De tweede meest voorkomende privacyschending was censuur (19,7%). Identiteitsfraude en phishing was door respectievelijk 3,6% en 4,9% van de respondenten meegemaakt. De meeste respondenten (64,0%) zijn goed tot zeer goed op de hoogte van de activiteiten van Bits of Freedom. Daarentegen gaf 9,1% van de respondenten aan slecht tot zeer slecht op de hoogte te zijn van de activiteiten van Bits of Freedom.

BIJLAGE C. DE BELANGRIJKSTE STATISTISCHE ANALYSES

1. Verschillen in kennis

Gebruikers van een smartphone én computer lijken meer kennis te hebben van privacytools en -issues dan gebruikers van een smartphone óf computer. Om te toetsen of de verschillen in kennis statistisch significant zijn, zijn de groepsgemiddeldes onderworpen aan een t-toets voor twee onafhankelijke steekproeven. Omdat kennis van privacytools en expert kennis van privacyissues niet normaal verdeeld zijn, is de wilcoxontoets in deze gevallen gebruikt.

Wilcoxontoets.

Kennis van privacytools en -technieken	Gemiddelde	Mediaan	Sig.
Smartphone *of* computergebruikers	29.82	29	W = 39812 p < .001
Smartphone *en* computergebruikers	33.43	34	

Expert kennis van privacyissues	Gemiddelde	Mediaan	Sig.
Smartphone *of* compuergebruikers	2.03	2	W = 45494 p < .01
Smartphone *en* computergebruikers	2.43	3	

T-toets voor twee onafhankelijke steekproeven.

Algemene kennis van privacyissues	Gemiddelde	Sig.
Smartphone *of* compuergebruikers	3.77	F = 0.26 p = .61
Smartphone *en* computergebruikers	3.95	

2. Relatie tussen kennis en bezorgdheid

Om te bepalen of er een relatie is tussen kennis en bezorgdheid, is een regressie analyse gedaan. In de regressieanalyses is gecontroleerd voor de invloed van betrokkenheid bij Bits of Freedom. Dit wil zeggen dat de factor ‘betrokkenheid bij Bits of Freedom’ is opgenomen in de analyses zodat kan worden bepaald of de andere factoren nog steeds gerelateerd zijn aan bezorgdheid naarmate betrokkenheid toe- of afneemt. De reden dat voor betrokkenheid bij Bits of Freedom is gecontroleerd, is dat wij sterk het vermoeden hebben dat mensen die erg betrokken zij bij Bits of Freedom (helaas nog) niet representatief zijn voor de Nederlandse samenleving. Zo lijkt Bits of Freedom bijvoorbeeld meer mannen dan vrouwen, meer hoger- dan lageropgeleiden, en meer hoemoes- dan niet hoemoeseters aan te trekken.

Uit de tabel op de volgende pagina met de resultaten van de regressie analyse kan worden afgeleid dat betrokkenheid bij Bits of Freedom een betere voorspeller is van bezorgdheid over privacy dan alle andere factoren in de regressieanalyse. Tegelijkertijd is ook te zien dat factoren als geslacht en leeftijd, en zelfs de interactie tussen kennis van tools en kennis van issues significant gerelateerd blijven ongeacht de mate van betrokkenheid bij Bits of Freedom. Hierbij moet worden opgemerkt dat de groep respondenten ook vanwege andere factoren die niet gemeten zijn waarschijnlijk niet heel representatief is voor de Nederlandse samenleving. Voorzichtigheid blijft dus geboden bij het generaliseren van de resultaten naar de algemene bevolking of andere bevolkingsgroepen.

Multiple lineaire regressie analyse: relatie tussen bezorgdheid, kennis, en andere persoonlijke factoren.

Predictoren	β	*t*	*p*
Privacykennis			
Kennis tools	–.08	-1.89	.06
Kennis issues (expert)	.07	1.71	.07
Kennis issues (algemeen)	.01	0.18	.86
Kennis tools x kennis issues (algemeen)	–.08	-2.30	.02
Overige persoonskenmerken			
Geslacht[a]	.09	2.40	.02
Leeftijd	.10	2.94	.00
Negatieve ervaringen	.08	2.34	.02
Betrokkenheid bij Bits of Freedom	.17	4.56	.00

Het model is statistisch significant (R^2 = .07, F = 7.92, p < .001).

[a] Geslacht gecodeerd als: man = 0, vrouw = 1.

3. Kennis, intentie en gedrag

Multiple lineaire regressie analyse: relaties tussen kennis en gedrag.

Predictor	R^2	F	β
Model 1: uitkomst = overige manieren	.38	135.04*	
Kennis tools			.42*
Kennis issues (expert)			.10*
Kennis issues (algemeen)			.04
Betrokkenheid bij Bits of Freedom			.26*
Model 2: uitkomst = gebruik tools	.36	124.33*	
Kennis tools			.44*
Kennis issues (expert)			.15*
Kennis issues (algemeen)			.02
Betrokkenheid bij Bits of Freedom			.18*

* p < .001

Correlatietabel.

	Manieren	Gebruik tools	Kennis tools	Kennis issues expert	Kennis issues algemeen	Intentie	Zorgen
Manieren	-						
Gebruik tools	**.64****	-					
Kennis tools	.39**	.38**	-				
Kennis issues expert	.21**	.24**	.23**	-			
Kennis issues algemeen	**.17****	**.18****	.11**	.34**	-		
Intentie	**.02**	**.03**	–.15**	–.06*	**–.04**	**-**	
Zorgen	**.23****	**.16****	–.01	.08*	**.04**	**.26****	-

Dikgedrukte getallen zijn pearson's *r* correlaties, niet-dikgedrukte getallen zijn kendall's tau correlaties.
*$p < .05$; **$p < .001$.

EINDNOTEN

1. Dit zou overigens wel een geniale gedachte kunnen zijn. Eureka!-momenten komen eerder wanneer je *niet* gefocust bent. Bron: ten Broeke, A. (28 januari 2008). Eureka! in het brein. *Kennislink*. Van: www.kennislink.nl/publicaties/eureka-in-het-brein

2. Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2-3), 181-202.

3. Dienlin, T., & Trepte, S. (2015). Is the privacyparadox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.

4. Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of advertising*, *28*(3), 37-51.

5. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacyparadox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100-126.

6. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61-80.

7. Pötzsch, S. (2008). Privacy awareness: A means to solve the privacyparadox?. *IFIP Summer School on the Future of Identity in the Information Society,* 226-236. Springer Berlin Heidelberg.

8. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

9. Deuker, A. (2009). Addressing the privacyparadox by expanded privacy awareness–the example of context-aware services. *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life,* 275-283. Springer Berlin Heidelberg.

10. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

11. Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48-56.

12. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

13. Pötzsch, S. (2008). Privacy awareness: A means to solve the privacyparadox?. *IFIP Summer School on the Future of Identity in the Information Society,* 226-236. Springer Berlin Heidelberg.

EINDNOTEN

14. Deuker, A. (2009). Addressing the privacyparadox by expanded privacy awareness–the example of context-aware services. *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life,* 275-283. Springer Berlin Heidelberg.

15. Culnan, M. J. (1993). " How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS quarterly*, *17*(3), 341-363.

16. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS quarterly*, *35*(4), 989-1016.

17. Bialik, C. (10 december 2010). Trees and Wi-Fi may co-exist after all. *The Wall Street Journal.* Van: http://blogs.wsj.com/numbers/trees-and-wi-fi-may-co-exist-after-all-1018/

18. Leslie, L. (30 juni 2012). Too much testosterone, too much confidence: the psychology of banking. *The Guardian*. https://www.theguardian.com/business/2012/jun/30/banking-psychology-testosterone-confidence-sex

19. Hargittai, E., & Hsieh, Y. P. (2012). Succinct survey measures of web-use skills. *Social Science Computer Review, 30*(1), 95-107.

20. Dienlin, T., & Trepte, S. (2015). Is the privacyparadox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.

21. Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

22. Deuker, A. (2009). Addressing the privacyparadox by expanded privacy awareness–the example of context-aware services. *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life,* 275-283. Springer Berlin Heidelberg.

23. Dienlin, T., & Trepte, S. (2015). Is the privacyparadox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285-297.