Bachelorscriptie

Online privacy in ruil voor terrorismebestrijding

John Akkermans

23 januari 2007

Radboud Universiteit Nijmegen

Samenvatting

Het Internet en terrorisme hebben de afgelopen jaren, parallel aan elkaar, een centrale rol in onze maatschappij verworven. De voordelen van het Internet – anonimiteit en het wereldwijde karakter – lijken het een ideaal platform te maken voor het plannen en beramen van criminele of terroristische activiteiten. Door het wegnemen van de anonimiteit op het wereldwijde web wordt ook direct dit draagvlak voor terrorisme omver geworpen. Maar zo gemakkelijk is het niet; privacy is een grondrecht van de mens en deze wil zijn privacy gewaarborgd houden. Echter, met de toenemende angst voor terrorisme, zou het heel goed mogelijk kunnen zijn dat mensen wél bereid zijn om een gedeelte van hun privacy op te offeren. Dit onderzoek gaat in op die afweging.

Inhoudsopgave

1 Onderzoeksplan

1.1 Probleemstelling

De probleemstelling van mijn onderzoek heeft te maken met een belangrijk *issue* in de hedendaagse samenleving, terrorisme. Ik wil gaan onderzoeken of Nederlandse Internetgebruikers bereid zijn om een stukje van hun online privacy op te offeren in ruil voor meer veiligheid in de vorm van terrorismebestrijding. De onderzoeksvraag die daarbij hoort:

Zijn Nederlandse gebruikers van het Internet bereid om een deel van hun privacy op het Internet op te offeren in ruil voor meer veiligheid in de vorm van terrorismebestrijding? Waarom wel of waarom niet en hangt dit af van geslacht, leeftijd of mate van gebruik?

Binnen deze onderzoeksvraag zitten een aantal begrippen en omschrijvingen die strak(ker) gedefinieerd moeten worden en daarmee onderzoekbaar gemaakt moeten worden.

- Onder *Nederlandse gebruikers van het Internet* versta ik *inwoners van Nederland met een Nederlandse nationaliteit in de leeftijd van 18 jaar en ouder die minimaal een uur per week gebruik maken van het Internet.* Daarbinnen kunnen later weer aparte groepen worden onderscheiden naar leeftijd en gebruik (zie methode). Ik heb ervoor gekozen om de ondergrens qua leeftijd te leggen op 18 jaar, omdat ik denk dat het merendeel van de gebruikers onder deze leeftijd zich nog niet bewust zijn van terrorisme en de online gevaren en mogelijkheden met betrekking tot terrorisme.

- Onder *een deel van hun privacy op het Internet* versta ik *de mogelijkheid voor de overheid en de AIVD om gesprekken op MSN Messenger/Live Messenger en e-mailberichten op te slaan en surfdata op te vragen bij de Internet Service Providers in Nederland ten behoeve van bestrijding van terrorisme.*

- Onder *meer veiligheid in de vorm van terrorismebestrijding* versta ik *de mogelijkheid voor de overheid en de AIVD om, middels de op te vragen data, te zorgen voor een verbetering van het veiligheidsgevoel van de Nederlandse Internetgebruikers door deze data in te zetten in de bestrijding van terrorisme.*

1.2 Verantwoording

Het onderwerp terrorisme is natuurlijk uitermate actueel. En het gebruik van ICT daarin en in de bestrijding ervan is de laatste jaren ook een groot *issue* geworden. Ik ben benieuwd of Nederlanders bereid zijn een deel van hun privacy op te offeren in ruil voor een stuk veiligheid in de vorm van een betere bestrijding van de gevaren van terrorisme. Ook is het van belang om te onderzoeken hoe burgers aankijken tegen een belangrijk onderwerp als dit. Privacywetgeving is erg belangrijk en tegelijkertijd ook erg tweestrijdig. Er is vaak een kant die minder privacy wil, maar ik denk dat mensen over het algemeen niet bereid om zo maar een stukje privacy in te leveren. Tenzij er iets tegenover staat waarvan ze duidelijk een voordeel inzien.
Een andere reden voor mij om tot dit onderzoek te komen, is het feit dat ik gebruik kan maken van aspecten uit de cursussen uit de Bachelorfase die mij het meest interesseren.

Er is de afgelopen jaren – en zeker na 11 september 2001 – veel onderzoek gedaan naar privacy en terrorisme. Ook zijn er al enkele maatregelen doorgevoerd. Zo heeft de Europese Unie in 2005 besloten om bedrijven te dwingen om gegevens van telefoon-, internet- en emailverkeer langer op te slaan [1].

In de *Volkskrant* van 28 januari 2006 staat een artikel over hoe de Nederlanders wel heel gemakkelijk hun privacy lijken op te offeren als er maar voldoende zwaarte aan eventuele bedreigingen wordt gegeven [2]. Omdat ik dat toch een vrij subjectief stuk vind, denk ik dat ik met mijn onderzoek het geschetste beeld kan controleren.

Volgens een onderzoek van *R&M Interactive* uit 2001 heeft 72% van de Nederlandse Internetgebruikers er geen problemen mee als emailverkeer wordt afgetapt als deze gegevens worden gebruikt tegen terrorisme of zware criminaliteit [3]. Mijn onderzoek zal wat dat betreft breder van aard zijn omdat er niet alleen naar emailverkeer wordt gekeken, maar ook data van MSN/Live Messenger en surfdata worden betrokken.

In een onderzoek, uitgevoerd in 2004 door *Newcom Research & Consultancy*, blijkt bovendien dat Nederlanders niet bang zijn dat de privacy van burgers (in het algemeen) te veel wordt geschonden als de *AIVD* meer bevoegdheden bij opsporingsonderzoeken krijgt. Bijna de helft (49 procent) van de Nederlanders is van mening dat de AIVD momenteel onvoldoende bevoegdheden heeft; 35 procent is van mening dat de AIVD wel voldoende bevoegdheden heeft. Daarnaast is 49 procent van mening dat de AIVD onvoldoende in staat is haar taken naar behoren uit te voeren [4]. Hoewel mijn onderzoek naar iets anders vraagt (namelijk – kort door de bocht - of "Nederlanders" bereid zijn om een deel van hun *eigen* privacy op te offeren in ruil voor betere terrorismebestrijding), kan dit wel bevestigd worden in mijn eigen onderzoek. Als inderdaad ook de helft van mijn onderzoekselementen vindt dat de *AIVD* meer bevoegdheden moet krijgen, dan zullen ze ook eerder bereid te zijn om een deel van hun (eigen) privacy op te offeren.

1.3 Theoretisch kader

In termen van cursussen uit de Bachelor, zou je kunnen zeggen dat het kennisgebied globaal bestaat uit de cursussen *ICT & Samenleving*, *Security* en *Onderzoeksmethoden*. Het benutten van ICT voor de bestrijding van terrorisme is natuurlijk een uitstekend voorbeeld van het gebruik van ICT in de (hedendaagse) samenleving. Belangrijke aspecten daarbij zijn veiligheid en privacy (security). Omdat er Internetgebruikers zullen worden geïnterviewd, spelen natuurlijk ook facetten uit de cursus *Onderzoeksmethoden* een belangrijke rol in dit onderzoek.

In de praktijk bestaat het kennisgebied uit Informatie en Communicatie Technologie (ICT) en Sociale Wetenschappen. Iets specifieker; binnen de ICT ligt dit onderzoek vast in *security* en binnen de Sociale Wetenschappen in *privacy* en *terrorismebestrijding*.

1.4 Methode

De onderzoeksfunctie is hoofdzakelijk *beschrijvend*, omdat ik zal gaan beschrijven of gebruikers bereid zijn een deel van hun privacy op het Internet in te ruilen voor betere terrorismebestrijding. Ook zal het onderzoek enigszins *verklarend* zijn omdat ik probeer te verklaren waarom gebruikers hier wel of niet toe bereid zijn.

De deelvraag die ik zal gebruiken voor het beantwoorden van de onderzoeksvraag luidt:
Zijn de gebruikers van het Internet bereid een deel van hun online privacy af te staan?
De vraag kan worden gebruikt om te concluderen voor de onderzoeksvraag of het een rol speelt in de bereidheid dat de gegevens worden gebruikt alleen voor terrorismebestrijding.

De strategie bestaat uit in eerste instantie een literatuurstudie naar reeds gedane onderzoeken omtrent dit – actuele – onderwerp. Daarna ga ik een sluitende vragenlijst maken, waarmee ik alle

gegevens kan verzamelen om de deelvragen en de hoofdvraag te beantwoorden. Deze vragenlijst zal ik dan gaan voorleggen aan gebruikers van het Internet. Het lijkt me handig om de vragenlijst daarom online te zetten en gebruikers per e-mail te benaderen. Zo vermijd je dat je gebruikers gaat benaderen die niet of nauwelijks (maar in ieder geval minder dan een uur per week online zijn) gebruik maken van het Internet.
Om tot een representatieve groep te komen, wil ik dat minimaal 50 mensen de vragenlijst invullen.

Nederland heeft in 2006 een inwonersaantal van 16.334.210 mensen, waarvan er 3.975.626 onder de 20 jaar (0-19 jaar) zijn.
De som

18/20 * 3.975.626 = 3.578.063

levert het aantal mensen jonger dan 18 jaar (0-17) op.
(er wordt gedeeld door 20 omdat de genoemde leeftijdsklassen *0-19 jaar* ook 20 klassen beslaan).
Deze mensen maken geen deel uit van het onderzoek, waardoor de totale populatie uitkomt op 16.334.210 – 3.578.063 = 12.756.147 [5]

Omdat alleen de mensen die minimaal een uur per week online zijn in het onderzoek worden meegenomen, moet ook dat nog in de populatie worden verwerkt. Immers, nog niet iedere Nederlander voldoet hieraan. Ik heb de aanname gedaan dat mensen met een Internetaansluiting minimaal een uur in de week online zijn.
In 2006 heeft in Nederland 85% van alle inwoners een Internetaansluiting en is voor mij dus minimaal een uur per week online. [6]

85% van 12.756.147 is 10.842.725 en dat is de grootte van de populatie Nederlanders van 18 jaar en ouder, die minimaal een uur in de week online zijn.

Als foutmarge van de steekproefgrootte heb ik 15% gekozen, voor de betrouwbaarheid 95%, omdat dit vaak gebruikte percentages zijn en omdat op deze manier de steekproefgrootte binnen de perken van een bachelorscriptie blijft.

$15 = 1.96\sqrt{((p*(1-p)) / n)}$ ➔
$15 = 1.96\sqrt{((50*50) / n)}$ ➔
$15^2 = 1.96^2*((50*50) / n)$ ➔
$n = (1.96^2 * 50^2) / 15^2 = 43$

Als extra controle heb ik de steekproefgrootte ook nog berekend met een speciaal daarvoor bestemde online calculator. Ook daar kwam een steekproefgrootte van 43 uit. Om dat af te ronden, heb ik ervoor gekozen om een steekproef van 50 te nemen uit de populatie. De foutmarge is daarmee verkleind tot 13.86% [7].

Aan de hand van de leeftijden van de invullers wil ik daarna een opdeling in klassen maken. Om dit strategisch aan te pakken, wil ik een aantal ingangen naar de populatie gaan gebruiken:

- Vrienden (18-24 jaar)
- Familie (zeer divers, maar vooral >24 jaar)

Daarbij wil ik alle respondenten verzoeken om de vragenlijst "door te sturen" naar bekenden. Zo moet er automatisch een grote en tegelijkertijd diverse populatie ontstaan.

Ook wil ik een opdeling maken in soorten gebruikers:

- 1 t/m 7 uur per week online;
- 8 t/m 14 uur per week online;

- 15 t/m 21 uur per week online;
- 22 t/m 28 uur per week online;
- 29 uur of meer per week online;

Ik ben tot deze klassen gekomen omdat jongeren gemiddeld 2,5 uur per dag online zijn [8]. Dat heb ik als middenklasse genomen en daarboven en daaronder de klassen verder ingedeeld. Deze klassen gebruik ik in de vragenlijst en kunnen aan de hand van de antwoorden nog verder worden bijgesteld.

De vragenlijst zal kwantitatief van aard zijn; dat wil zeggen dat de resultaten statistisch zullen worden gebruikt om tot een conclusie en antwoord op de onderzoeksvraag te komen. Als er meer respondenten bereid zijn dan niet bereid zijn, mag worden geconcludeerd dat de Nederlandse Internetters bereid zijn om een deel van hun online privacy op te offeren voor terrorismebestrijding.

1.5 Tijd- en faseringschema

Omschrijving	**Werktijd**	**looptijd**
Onderzoeksplan opstellen	3 uur	1 week
Vragenlijst maken	10 uur	1 week
Gebruikers selecteren	2 uur	1 week
Geselecteerde gebruikers contacteren	2 uur	3 dagen
Vragenlijst afnemen en voortgang monitoren	5 uur	3 weken
Gebruikers selecteren en contacteren	3 uur	3 dagen
Resultaten verzamelen	3 uur	1 week
Resultaten analyseren	20 uur	2 weken
Resultaten verwerken in scriptie	30 uur	4 weken
Presentatie voorbereiden	3 uur	3 dagen
Resultaten presenteren	1 uur	1 dag

1.6 Referenties onderzoeksplan

[1] http://www.elsevier.nl/nieuws/europese_unie/artikel/asp/artnr/54457/zoeken/ja/index.html
[2] *De Volkskrant*, 28 januari 2006
[3] http://www.zdnet.nl/News.cfm?id=14271
[4] https://secure.mijnopinie.nl/index.php?pagina_id=2&nieuws_id=17&loginID=f535efab34ee99dc18eedb156267aace
[5] *Centraal Bureau voor de Statistiek*, Bevolking; kerncijfers, http://statline.cbs.nl/StatWeb/Table.asp?STB=T&LA=nl&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,(l-1)-l&HDR=G1
[6] *Centraal Bureau voor de Statistiek,* Onderzoek ICT gebruik bij personen, http://statline.cbs.nl/StatWeb/table.asp?STB=T&LA=nl&DM=SLNL&PA=71098ned&D1=33-133&D2=0-2&HDR=G1
[7] http://www.journalinks.be/steekproef/
[8] http://www.nu.nl/news/839490/50/Jongeren_MSN-en_het_liefst.html

2 Inleiding

Het Internet is de afgelopen jaren uitgegroeid tot een onmisbaar medium. Op alle niveau's van de samenleving speelt Internet inmiddels een enorme rol; in het bedrijfsleven, in sociale netwerken (vriendenkringen etc.), in de politiek, enzovoort.

Een groot voordeel van het Internet is de anonimiteit die gebruikers hebben en waarachter ze zich kunnen verschuilen. Anonimiteit laat zich definiëren als totale privacy. Niemand kent je en je identiteit blijft veilig verborgen achter je computerscherm. Dat is natuurlijk een goed en veilig gevoel, wat de gebruikers ook niet zomaar zullen willen opgeven.

Maar parallel aan de opkomst van het Internet in onze samenleving, loopt de opkomst van terrorisme. Sinds 11 september 2001 is de wereld veranderd. Alle mogelijk middelen worden sindsdien ingezet om een ramp als in de Verenigde Staten te voorkomen. Een van de media die nog relatief oncontroleerbaar is in deze context, is het Internet. Dat is uiteraard te wijten aan de eerdergenoemde anonimiteit waarachter ook terroristen zich simpel kunnen verschuilen.

Sinds enkele jaren wordt er daarom een debat gevoerd om deze anonimiteit gedeeltelijk af te breken. Natuurlijk zou het ideale scenario zijn dat de anonimiteit van terroristen totaal wordt afgenomen, en die van onschuldige gebruikers geheel intact blijft. Dat is echter een utopie, omdat juist aan de hand van Internetactiviteiten kan worden bepaald of iemand zich inlaat met terroristische activiteiten. Daarom is het inleveren van stuk privacy (en daarmee het wegnemen van anonimiteit) van alle gebruikers de enige oplossing om ook dit medium controleerbaar te maken in het kader van terrorismebestrijding.

Ik heb onderzoek gedaan naar de bereidheid van Nederlandse gebruikers van het Internet om een stuk privacy in te leveren in ruil voor terrorismebestrijding. Ook heb ik bekeken of deze bereidheid al dan niet afhangt van een aantal demografische factoren (als leeftijd, nationaliteit) en de mate van het Internetgebruik. De onderzoeksvraag van dit onderzoek is daarmee vastgesteld op:

Zijn Nederlandse gebruikers van het Internet bereid om een deel van hun privacy op het Internet op te offeren in ruil voor meer veiligheid in de vorm van terrorismebestrijding? Waarom wel of waarom niet en hangt dit af van geslacht, leeftijd of mate van gebruik?

In deze scriptie zal ik allereerst de begrippen van het onderzoek vastzetten. Wat wordt bijvoorbeeld verstaan onder het inleveren van een *stuk privacy* of *een deel van hun privacy* in het kader van dit onderzoek? Vervolgens zal ik uiteenzetten wat er aan onderzoek op dit gebied reeds is gedaan. Dat kan helpen bij het trekken van conclusies en kan tevens bepaalde conclusies verklaren. Daarna zal ik verslag doen van mijn onderzoek en de resultaten analyseren en conclusies trekken.

Veel leesplezier toegewenst,

John Akkermans
13 december 2006

3 Afbakening

Mensen hebben verschillende opvattingen en zullen dus ook anders denken over privacy. Daarom is het van belang om af te bakenen wat er in het kader van dit onderzoek wordt verstaan onder privacy. Er bestaan verschillende definities, die onderling sterk van elkaar verschillen. Ook is de definitie in de loop der jaren aangepast (zeker door de opkomst van de computer en het Internet).
Het *Van Dale* woordenboek uit 1970 geeft als definitie van privacy *persoonlijke vrijheid, het ongehinderd in eigen kring of met een partner ergens kunnen vertoeven.*[1] Deze definitie heeft niets in zich wat betrekking heeft op het hedendaagse informatietijdperk.
Wikipedia omschrijft privacy als de *persoonlijke levenssfeer (..) het gaat onder meer om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven, en het recht om vertrouwelijk te communiceren via, brief, telefoon, e-mail en dergelijke. Privacy betekent dat men dingen kan doen zonder dat de buitenwereld daar inbreuk op maakt of zelfs weet van heeft.* [2]
In deze hedendaagse omschrijving is inmiddels opgenomen dat privacy ook betrekking kan hebben op het digitale leven op het Internet.

Het blijkt niet mogelijk om een eenduidige definitie te vinden voor privacy, omdat dit afhankelijk is van de omgeving waarbinnen het begrip wordt gebruikt. De wetgeving rondom privacy is bijvoorbeeld niet universeel over Europa, laat staan over de gehele wereld. Omdat dit onderzoek zich richt op gebruikers van het Internet in Nederland, heb ik de definitie die geldt in Nederland gebruikt voor dit onderzoek. Daarmee wordt privacy gedefinieerd als:

DEF: privacy is de persoonlijke levenssfeer, waarbij het gaat onder meer om de bescherming van persoonsgegevens, de bescherming van het eigen lichaam en van de eigen woning, de bescherming van familie- en gezinsleven, en het recht om vertrouwelijk te communiceren via, brief, telefoon, e-mail en dergelijke. Privacy betekent dat men dingen kan doen zonder dat de buitenwereld daar inbreuk op maakt of zelfs weet van heeft. [2]

Voor dit onderzoek heb ik in het onderzoeksplan tevens een definitie gegeven voor wat er wordt bedoeld met het inleveren van een stukje privacy, wat op zichzelf natuurlijk bijzonder vaag is. Wat is nu precies een *stukje* privacy?

DEF: onder een stuk(je) of een deel van privacy wordt verstaan de online privacy, in dit onderzoek bestaande uit Messenger-gesprekken, e-mailverkeer, surfdata en chatdata.

Hiermee zijn mijns inziens de meeste *kweekvijvers* voor terroristische activiteiten afgedekt. Onder Messenger vallen voor mij alle applicaties waarmee het mogelijk is een real-time gesprek te voeren op het web, zoals daar zijn *Live Messenger/MSN Messenger*, *AOL Messenger*, *Yahoo Messenger*, *ICQ*, etc.

Daarnaast behoeft de uitspraak van een stukje privacy *inleveren* ook een toelichting. Wat wordt verstaan onder het *inleveren* van het eerder gedefinieerde stukje privacy?

DEF: het inleveren van een stuk(je) privacy houdt in dat deze gegevens worden opgeslagen door de Internet Service Providers (ISP) en dat deze gegevens kunnen worden opgevraagd door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en andere opsporingsinstanties, louter ten behoeve van terrorismebestrijding.

De Internet Service Providers (ISP) zijn in dit geval de bedrijven die het voor de gebruikers mogelijk maken om zich op het Internet te begeven. De gebruikers hebben een abonnement bij deze provider waarmee ze een pakket tot hun beschikking hebben om te internetten.

Dan moet ook worden vastgesteld wat ik in dit onderzoek versta onder *Nederlandse gebruikers van het Internet*.

DEF: onder Nederlandse gebruikers van het Internet versta ik inwoners van Nederland met een Nederlandse nationaliteit in de leeftijd van 18 jaar en ouder die minimaal een uur per week gebruik maken van het Internet.

Tot slot zal ik definiëren wat ik bedoel met *meer veiligheid in de vorm van terrorismebestrijding*.

DEF: onder meer veiligheid in de vorm van terrorismebestrijding versta ik de mogelijkheid voor de overheid en de AIVD om, middels de op te vragen data, te zorgen voor een verbetering van het veiligheidsgevoel van de Nederlandse Internetgebruikers door deze data in te zetten in de bestrijding van terrorisme.

Hiermee zijn de vage en te ruime begrippen afgebakend tot eenduidige definities. Dat is essentieel om consistentie aan te brengen in het onderzoek. Er bestaat nu immers een duidelijke omschrijving voor de begrippen die zonder strakke definitie door verschillende mensen op een verschillende manier kunnen worden geïnterpreteerd.

4 Eerder onderzoek

2.1 Verenigde Staten

Er is al veel onderzoek gedaan naar mogelijkheden om online privacy op te offeren in ruil voor terrorismebestrijding. Echter, een groot struikelblok werpt zich al direct bij het begin op; mensen blijken niet bereid om hun persoonlijke informatie prijs te geven en willen anoniem blijven op het Internet. In de Verenigde Staten is veel onderzoek gedaan naar de bereidheid van mensen om op het Internet hun persoonlijke gegevens prijs te geven. Dit is dan nog los van de vraag of het wordt gebruikt voor terrorismebestrijding, maar het geeft natuurlijk wel aan dat het niet zonder meer aan te nemen is dat mensen hun online privacy willen opofferen.

In de Verenigde Staten is het aantal onderzoeken naar het inperken van (online) privacy voor terrorismebestrijding enorm toegenomen na 11 september 2001, de dag dat het land getroffen werd door de grootste terroristische aanslag ooit. In de onderzoeken zijn twee kanten te onderscheiden: een kant die concludeert dat online privacy moet worden ingeperkt voor terrorismebestrijding en een kant die concludeert dat privacy een grondrecht van de burgers is en dat deze nooit mag worden opgeofferd.

Een onderzoek van de Universiteit van Pennsylvania uit 2003 toont aan dat 85% van de gebruikers van het Internet geen toestemming geven om hun persoonlijke gegevens op te laten slaan of uit te laten wisselen wanneer ze deze in (moeten) vullen op een website. [3]

Sheetel Asrani heeft een paper geschreven waarin hij zijn gedachten uiteenzet over security versus privacy. Hij zegt dat Osama Bin Laden de terroristische aanslagen van 11 september 2001 volledig heeft kunnen opzetten via het Internet en dat het in deze tijd mogelijk gemaakt moet worden om dat te kunnen beheersen of voorkomen. Maar hij maakt daarbij duidelijk dat het moeilijk zal zijn om een goede afweging te vinden tussen enerzijds de wens van online privacy en anderzijds de beveiliging tegen terrorisme. En dat is wat ik in dit onderzoek heb geprobeerd te achterhalen.
In de Verenigde Staten is er na 11 september 2001 direct een nieuwe wet aangenomen, de USA PATRIOT Act (Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act). Deze wet heeft het voor machtsuitvoerders gemakkelijker gemaakt om online activiteiten bij te houden en te monitoren, waarbij er inbreuk gemaakt kan worden op privacy rechten uit de grondwet.

In deze wet staat dat Internetverkeer mag worden afgetapt als deze gegevens relevant zijn voor een lopend crimineel onderzoek. Er moet dus duidelijk een aanwijzing zijn dat de persoon die wordt afgeluisterd, ook daadwerkelijk criminele activiteiten uitvoert. PATRIOT maakt het dus mogelijk dat bezochte websites, emailberichten en invoer in zoekmachines in de gaten kunnen worden gehouden, en indien nodig gebruikt kunnen worden om criminele (terroristische) activiteiten te stoppen of te voorkomen.

Maar, er is meer. De wet geeft ook toestemming tot het installeren van een Internet surveillance programma, genaamd *Carnivore*. Dit programma is in het diepste geheim ontwikkeld en uitgegeven in 1999, maar werd pas een jaar later publiekelijk aangekondigd. Het gaf dus al vóór de komst van PATRIOT een mogelijkheid tot het aftappen van internetdata. *Carnivore* kon alle vormen van internetactiviteit onderscheppen: emailberichten, bezochte websites en internettelefoongesprekken.

Er is echter ook veel kritiek op *Carnivore*. Omdat het programma kon worden ingesteld zonder enige sporen na te laten, was het onmogelijk om vast te stellen door wie het programma werd gebruikt of voor welke soort te verkrijgen informatie deze werd ingezet. Kortom, de kans op misbruik van het programma was te groot.

Toch is PATRIOT een groot succes geworden. De overheid had al flink wat mogelijkheden om online activiteiten in de gaten te houden, maar deze wet en het feit dat daarin het gebruik van *Carnivore* werd toegestaan, heeft de surveillancemogelijkheden van de overheid alleen maar sneller en goedkoper gemaakt. [4]

Ook wordt er al geruime tijd samengewerkt door landen over de gehele wereld in het aftappen van (Internet)communicatie.
Sinds de jaren '70 is er systeem in gebruik waarin de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland samenwerken bij het wereldwijd afluisteren van alle communicatie. Dit systeem heet ECHELON. Eind jaren '90 heeft het systeem een update ondergaan en ging het verder als ECHELON II.

Het systeem is vernoemd naar het type computer *Echelon*, waarmee grote hoeveelheden data worden doorzocht op een specifiek onderdeel. Op zogenaamde volglijsten staan targets, die moeten worden afgeluisterd. Dit kunnen namen, adressen, internetadressen, etc. zijn. Deze targets worden als een soort trefwoord gebruikt om de onderschepte communicatie te doorzoeken.
In 2000 kwam ECHELON in opspraak. Grote bedrijven zouden voor enorme bedragen het systeem hebben gebruikt voor commerciële doeleinden. Tot een verbod op het gebruik van ECHELON heeft het niet geleid. [5]

Dat er ook een grote keerzijde zit aan de nieuwe regels betreffende het makkelijker kunnen onderscheppen van internetactiviteiten, blijkt wel uit de kwestie met professor Mike Adams, verbonden aan de faculteit Rechten van de University of North-Carolina in Wilmington. Hij werd na de aanslagen van 11 september gedwongen om zijn e-mailverkeer openbaar te maken naar aanleiding van een ontvangen e-mail van een studente die daarin opperde dat de imperialistische politiek van de Verenigde Staten in het Midden-Oosten de aanslagen zouden hebben veroorzaakt. Adams reageerde fel op de e-mail en gaf aan dat hij het pertinent oneens was met het door de studente geschetste beeld. Ook stuurde hij haar e-mail door naar derden. Toen de studente daarna (fysiek) werd bedreigd deed zij beroep op de *open-records law* van North-Carolina, waarmee ze inzage wilde krijgen in de e-mails die Adams naar derden had gestuurd. De universiteit kon uiteindelijk niet anders dan Adams dwingen zijn e-mailverkeer openbaar te maken. Het begin van een grote rel.

De genoemde *open-records law* voorziet erin dat ambtenaren verplicht kunnen worden gesteld om hun documenten openbaar te maken voor het publiek als daarom gevraagd wordt (met een legitieme reden uiteraard). Professor Adams werkt een Rijksuniversiteit, en in de Verenigde Staten worden deze mensen gezien als (staats)ambtenaren. [6]

Ook is er sinds 1991 jaarlijks een conferentie in de Verenigde Staten, Engeland of Canada die ingaat op de kwestie online privacy voor veiligheid; de *Conference on Computers, Freedom and Privacy* (CFP). Tijdens deze conferenties komen diverse onderzoekers vertellen waarom het wel of niet nodig is dat er online privacy moet worden ingeleverd voor de veiligheid. [7]

In een *Special Report* van *United States Institue of Peace (USIP)* staat erg uitgebreid en helder omschreven wat het Internet te bieden heeft aan terroristen en waarom dit medium zo

gemakkelijk kan worden gebruikt voor het plannen van terroristische activiteiten. De voordelen van het Internet (wereldwijd, toegankelijk, veel toehoorders, veel informatiestromen) maken het tevens een ideaal platform voor terroristen. *USIP* heeft een scan uitgevoerd op het Internet en daaruit kwamen honderden websites naar voren die terroristen dienen en ondersteunen. In het report wordt ook ingegaan op de mogelijkheden om te voorkomen dat het Internet dient als platform voor terroristen. De voor- en nadelen daarvan moeten goed worden afgewogen. Sommige maatregelen kunnen de overheid in staat stellen om meer surveillancemogelijkheden te verkrijgen, maar schenden tegelijkertijd de privacy van de burger. Het bestrijden van terrorisme vraagt dan dus een hoge prijs en dat is ook exact de probleemstelling van mijn onderzoek. [8]

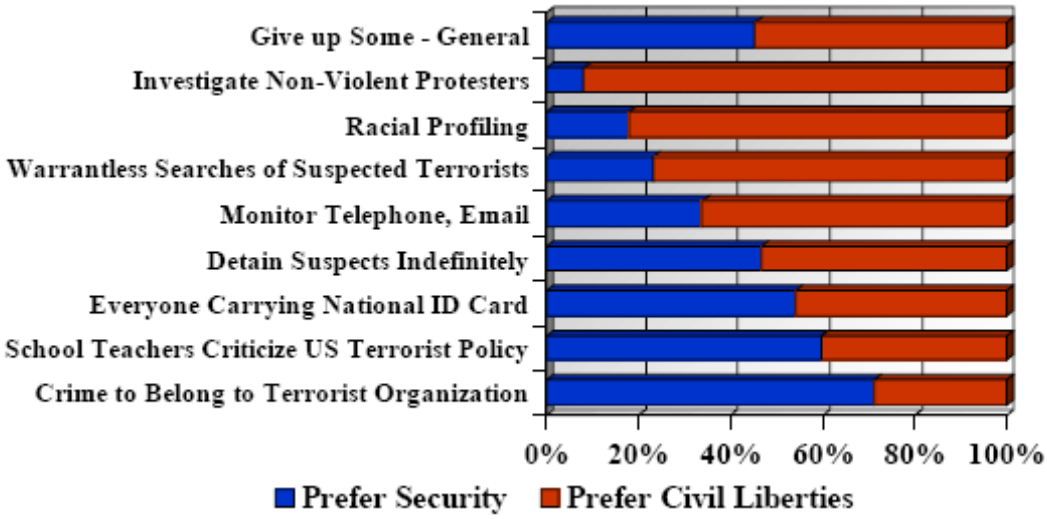
Khalid Al-Midhar werd in 1999 opgemerkt toen hij een bespreking had met handlangers van Osama Bin Laden. Zijn naam werd in de Verenigde Staten op een *watchlist* gezet, maar in 2001 kwam de FBI erachter dat hij al in het land was. Toen ze uitvonden waar hij was, stonden de Twin Towers op instorten, was het Pentagon aangevallen en waren er meer dan 5000 doden. Al-Midhar had onder zijn eigen naam een vliegticket kunnen kopen voor een van de terreurvluchten. Met de technologische mogelijkheden was het mogelijk geweest om hem te stoppen, maar dat was dan ten koste gegaan van de privacy. Toch geven polls na 11 september aan dat het merendeel van de Amerikanen bereid is om een stuk online privacy in te leveren voor meer veiligheid; 86% is voor meer gebruik van gezichtsherkenning, 81% wil meer controle op bank- en creditcardtransacties en 68% is voor invoering van een nationale identiteitskaart. [9]

Toch stelt Bruce Schneier dat de data mining systemen nooit terroristische plots kunnen ontdekken. Terroristische aanvallen zijn uniek, apart en complex en kunnen daardoor niet worden ontdekt door automatische computersystemen. Dat moet gebeuren door mensen en daarom vindt Schneier dat als we privacy opgeven door onze gegevens te laten monitoren door computersystemen, dan doen we dat voor niets. [10]

Tot slot heb ik een aantal onderzoeken onder elkaar gezet waarin Amerikanen werd gevraagd naar hun bereidheid tot het inleveren van privacy voor terrorismebestrijding.
In mei 2006 is een onderzoek gedaan door de *Washington Post* naar hoe de Amerikanen aankijken tegen het programma van de *National Security Agency (NSA)* waarin is bepaald dat telefoongesprekken worden opgeslagen. Hierbij gaf 63% aan dit acceptabel te vinden, tegen 35% onacceptabel. Tevens vond 65% van de ondervraagden het belangrijker dat terrorisme werd, ook al zou hun privacy daarmee geschonden worden; 31% vond dat privacy niet mocht worden opgeofferd, ook al zou daarmee de bestrijding van terrorisme worden beperkt. [11]

In januari 2006 is er een telefonische enquête gehouden onder 1001 volwassen Amerikanen, waaruit bleek dat 64% van de respondenten vond dat de federale opsporingsinstanties inbreuk maken op de privacy van de burgers met hun surveillance mogelijkheden. Toch is een kleine meerderheid (51%) voor de surveillance om terrorisme te bestrijden. [12]

Het *Institute for Public Policy and Social Research (IPPSR)* van de Michigan State University, heeft onderzocht hoe Amerikanen denken over de afweging veiligheid ten opzichte van privacy op bepaalde gebieden. De conclusies zijn weergegeven in onderstaande figuur:



Als het gaat om terroristische activiteiten of organisaties, blijkt de meerderheid de voorkeur te geven aan veiligheid. Voor de andere gebieden, geeft de meerderheid toch de voorkeur aan het behoud van de privacy. [13]

2.2 Nederland

Zeker na 11 september 2001 is het logisch dat er in de Verenigde Staten veel onderzoek is gedaan betreffende online privacy en het inperken daarvan in de strijd van terrorisme. Maar, ook in andere landen is de dreiging van en de angst voor terrorismebestrijding toegenomen. Zo ook in Nederland, waar men ook al flink wat onderzoek heeft gedaan naar hoe terroristische activiteiten op het anonieme Internet kunnen worden opgevangen en in de toekomst wellicht kunnen worden voorkomen. Omdat ik mijn onderzoek heb gericht op gebruikers van het Internet in Nederland, heb ik ook enkele eerdere onderzoeken voor Nederland doorgenomen.

Een onderzoek van *R&M Interactive* uit september 2001 toont aan dat Nederlandse Internetgebruikers er geen problemen mee hebben als de Nederlandse overheid e-mail aftapt in het kader van terrorismebestrijding. Zij concluderen dit toen bleek dat 72% van de Internetters aangaf hier geen bezwaren tegen te hebben. [14]

Misschien wordt dit hoge percentage gevoed door het feit dat de Nederlandse internetter bang is voor misbruik van het Internet door terroristen. Uit een onderzoek van *CentERdata* (stichting die verbonden is aan de Universiteit van Tilburg) uit 2003 blijkt dat 88% van de Nederlanders denkt dat terroristen het Internet kunnen misbruiken om een aanslag te kunnen plegen op de elektriciteitsvoorziening, het betalingstelsel, het transportstelsel of grote ondernemingen. Daarnaast denkt 25% dat er ook daadwerkelijk een terroristische aanslag wordt gepleegd in de samenleving via het Internet in de twee jaar na het onderzoek (in de periode 2003-2005 dus). [15]

In november 2004 heeft *Newcom Research & Consultancy* reeds onderzoek gedaan naar of Nederlanders privacy in willen leveren voor terrorismebestrijding. Toen gaf 65% aan dat men niet bang was dat hun privacy te veel in gevaar zou komen als persoonlijke gegevens zouden worden gebruikt in opsporingsonderzoeken van de AIVD. Daar tegenover stond dat 15% hier wel bang voor was.

Ook hebben zij per methode afzonderlijk onderzocht of de respondent het aanvaardbaar vindt dat deze kan worden toegepast door de AIVD. Daaruit bleek dat het controleren van internetbezoek voor veel mensen geen probleem was. Zo vond 35% het opsporen en controleren

van verdachte zoekopdrachten en 23% het controleren van het bezoeken van specifieke websites altijd aanvaardbaar.
De mogelijkheid om e-mails te onderzoeken vond 46% alleen aanvaardbaar bij potentiële dreiging vanuit een bepaalde persoon. [16]

In *De Groene Amsterdammer* van 20 oktober 2001 wordt ingegaan op de reactie van Nederland op de aanslagen van 11 september 2001 in de Verenigde Staten. Er werd een "Actieplan Terrorisme en Veiligheid" opgesteld, waarin 43 punten werden opgenomen. Het eerste punt is "uitbreiding van inlichtingen- en veiligheidsdiensten". De auteur is zeer verbaasd dat de Nederlandse burgers niet in actie kwamen en het allemaal wel best leken te vinden. Hij haalt daarbij ook de opiniepeilingen aan waaruit blijkt dat Nederlanders privacy willen inleveren voor meer veiligheid. Hij stelt, met behulp van de Twentse hoogleraar communicatiewetenschap en privacyexpert Jan van Dijk, dat dit een illusie is. Van Dijk stelt dat met het inperken van privacy voor alle burgers terroristen en vredelievende burgers over een kam worden geschoren. Het zou alleen het angstgevoel onder de burgers vergroten. Bovendien zegt hij dat het niet bewezen kan worden dat aanslagen als die van 11 september voorkomen hadden kunnen worden als er ruimere technologische mogelijkheden waren geweest. [17]

Ook Lodewijk Asscher vindt dat het bestaan van spionagediensten die onvoldoende gecontroleerd (kunnen) worden in strijd met grondrechten. De gebeurtenissen van 11 september hebben het falen van de inlichtingendiensten volgens hem overduidelijk aangetoond. Er is echter geen bewijs dat meer afluistermogelijkheden de aanslagen hadden kunnen voorkomen. [18]

Arno Smits besteedt in zijn proefschrift "Strafvorderlijk onderzoek van telecommunicatie" aandacht aan het feit dat er te veel misgaat bij Amerikaanse opsporingsdiensten als het gaat om het aftappen van communicatie. Smits stelt dat dit in Nederland waarschijnlijk ook het geval zal zijn, maar dat dat niet te controleren is doordat er "sluier van geheimzinnigheid" rondom de Nederlandse opsporingsdiensten. Hoewel tappen één van de populairste opsporingsmethodes is in Nederland, is de regelgeving rondom tappen volgens hem gebaseerd op wetten uit 1926 en 1971. De nieuwste ontwikkelingen in telecommunicatie zijn niet gevangen in regelgeving. Daarmee blijkt maar weer hoe complex de afweging tussen privacy en terrorismebestrijding in elkaar zit; ook juridisch gezien moet het helemaal worden onderbouwd. [19]

In de Volkskrant stond in 2001 een artikel waarin wordt ingegaan op de vraag of de veiligheid wordt gediend met het inleveren van privacy. In het dagelijks leven hechten burgers veel belang aan hun privacy, maar direct na de aanslag op 11 september in de Verenigde Staten gingen meteen stemmen op om afstand te doen van een deel van onze burgerlijke vrijheden om de westerse samenleving tegen terrorisme te beschermen. De omvang en de gevolgen van de aanslag waren toen nog niet eens duidelijk. De auteur vindt het niet zo'n gekke gedachte; als de burger doelwit blijkt van terrorisme, is het inleveren van een beetje privacy wel het minste wat hij kan doen. Maar wederom wordt hoogleraar Jan van Dijk aangehaald om dat te weerleggen: "De aanslag in de Verenigde Staten vormt statistisch gezien een incident en een incident kan nooit de vergaande conclusies rechtvaardigen die er nu door ven aan worden verbonden.
De Utrechtse historicus E. Jonker sluit daarbij aan: "Privacy is een soort barometer van het maatschappelijk welbevinden: we eisen het op als we ons sterk voelen, we doen er afstand van als we worden bedreigd." [20]

Tot slot heb ik nog een televisieprogramma van de IKON bekeken. In het programma *Factor* wordt ingegaan door vier personen. Ik heb van alledrie hun standpunten genoteerd:

J. Kohnstamm (voorzitter College Bescherming Persoonsgegevens)

Alleen als blijkt dat de huidige opsporings- en surveillancemiddelen niet voldoende zijn, kan er een afweging gemaakt om privacy in te leveren voor meer veiligheidsmaatregelen. Echter, de er zijn voldoende middelen beschikbaar, alleen worden die niet efficiënt gebruikt. Hij verwijst ook naar de Verenigde Staten, waar er – door ontzettend veel concurrentie tussen de opsporings- en veiligheidsdiensten – niet goed wordt samengewerkt en er veel informatie verbrokkeld blijft. Dat sluit weer aan bij het verhaal over Kahlid Al-Midhar.
Nederland staat in de top voor wat betreft het aftappen van telefoongesprekken, maar uit cijfers blijkt dat in omringende langen het oplossingspercentage veel hoger ligt.
Kohnstamm vindt het verbazingwekkend dat mensen in de afweging privacy – veiligheid steeds weer lijken te kiezen voor veiligheid en hij wil dat mensen op de waarde van de bescherming van persoonsgegevens gewezen worden. Ook onschuldige mensen kunnen door het inleveren van veel privacy in het *datamining-net* terecht komen en daarvoor is hij erg huiverig.

H. Duijst (directeur Securicor)
De politiek moet bepalen of er meer middelen moeten komen, maar als je niks te verbergen hebt zou je ook niet tegen meer veiligheidsmaatregelen (zoals het inleveren van privacy) moeten zijn. Als je bepaalde zaken wilt achterhalen, zul je bepaalde dingen moeten openzetten, anders kom je nooit tot de benodigde informatie. Wanneer je veiligheid én openheid wilt garanderen, komt automatisch de veiligheid in het geding en dus kom je er uiteindelijk niet onderuit om een stukje vrijheid op te geven.

B. Bohler (advocaat)
De rechtstaat is door alle nieuwe middelen langzaam aan het verdwijnen. Terrorisme moet worden bestreden door het benutten van de middelen die bestaan in een rechtstaat.
Je kunt privacy en veiligheid niet tegen elkaar wegstrepen, want absolute veiligheid kan nooit worden gegarandeerd en het inleveren van vrijheid omdat we er veiliger van zouden worden is een schijnargument. Ze vindt verder dat mensen erop moeten worden gewezen dat er van iedereen gegevens zullen worden verzameld en niet alleen van de terroristen. [21]

5 Methode

5.1 Onderzoekselementen

De onderzoekselementen zijn de eenheden die onderzocht gaan worden. Zij hebben bepaalde eigenschappen die je in het onderzoek wilt gaan verklaren, vergelijken, bepalen, etc. [22]
Omdat er al veel onderzoek is gedaan in dit kader in de Verenigde Staten en omdat het het bereik van het onderzoek niet te ruim zou maken, heb ik me in dit onderzoek beperkt tot Nederlandse gebruikers van het Internet.

Uiteindelijk is het vraagstuk in dit onderzoek – inperking van online privacy voor terrorismebestrijding – van belang voor elke gebruiker van het Internet. Immers, iedereen die zich op het Internet begeeft, heeft die online privacy tot zijn beschikking. Daarom heb ik ook gekozen om de onderzoekselementen niet verder in te perken dan dat deze wekelijks gebruik maken van het Internet.

Echter, het onderwerp terrorisme is behoorlijk complex en nog niet iedereen kan een goede inschatting maken van de gevaren ervan ten opzichte van het belang dat men hecht aan de eigen online privacy. Dat is de reden dat ik wel heb ingeperkt tot een minimale leeftijd van 18 jaar. Ik heb dus aangenomen dat Internetgebruikers van 18 jaar en ouder een onderbouwde mening hebben over de balans tussen het afstaan van een stuk online privacy en het bestrijden van terrorisme.

5.2 Variabelen

De variabelen zijn de eigenschappen van de onderzoekselementen die in het onderzoek worden betrokken. [22]
In dit onderzoek heb ik, naast een aantal demografische variabelen, de variabelen aangewezen die een waarde geven aan de mening van het onderzoekselement of deze bereid is om een stukje privacy en die een waarde geven aan de mening of deze bereid is om een stukje privacy in te leveren voor terrorismebestrijding.

5.3 Dataverzameling

Dit onderzoek vraagt naar het gebruik van vragenlijsten om de benodigde data te verzamelen. De data die nodig is om de onderzoeksvraag te kunnen beantwoorden, zijn waardes voor de variabelen. Dat wil zeggen; leeftijden, nationaliteiten, meningen, etc.
Omdat het onderzoek betrekking had op gebruikers van het Internet heb ik besloten om de vragenlijst online te zetten en de onderzoekselementen via e-mail te benaderen.

Om conclusies te kunnen trekken over mate van gebruik en leeftijd worden de respondenten opgedeeld in klassen. De leeftijdsklassen heb ik achteraf bepaald omdat vooraf niet kan worden geschat hoe de leeftijdsverdeling zou komen te liggen (dat was inherent aan de gekozen methode voor steekproefselectie).
De klassen voor de mate van gebruik had ik wel vooraf vastgesteld:

- 1 t/m 7 uur per week online;
- 8 t/m 14 uur per week online;
- 15 t/m 21 uur per week online;
- 22 t/m 28 uur per week online;

- 29 uur of meer per week online.

Ik ben tot deze klassenindeling gekomen, nadat ik op het Internet een onderzoek had gelezen over het aantal uren dat jongeren gemiddeld op het Internet doorbrachten. [23]

De vragenlijst bestaat uit hoofdzakelijk gesloten vragen, waarbij de antwoordenmogelijkheden dus vooraf zijn vastgesteld. Omdat ik ook in het onderzoek heb opgenomen waarom mensen wel of niet bereid zijn een stukje privacy in te leveren, moet ook die vraag in het onderzoek worden opgenomen. Dat levert echter een dilemma op. Ik had eerdere onderzoeken kunnen opzoeken om de antwoordenmogelijkheden bij die vraag te geven (gesloten vraag), maar ik denk dat respondenten dan beïnvloed zouden worden door deze mogelijke antwoorden. Ze zouden antwoorden kunnen geven, waar ze eigenlijk niet zelf aan hadden gedacht, maar pas na het lezen ervan (omdat ze al staan gegeven) besluiten dat dat ook reden voor hen is.

In termen van het TAP-paradigma, zou je kunnen zeggen dat het referentiekader van de respondent dan beïnvloed zou worden. Dat houdt dan verband met Perspective.
Het TAP-paradigma is een uitgangspunt bij het opstellen en evalueren van vragenlijsten. De afkorting TAP staat voor Topic (begrijpelijkheid van de vraag, goede definitie), Applicability (toepasbaarheid van de vraag) en Perspective (interpretatiekader). [22]

Daarom heb ik besloten de motivatievragen open te houden en de antwoorden achteraf zelf in te delen in antwoordklassen.

De vragenlijst is als bijlage bij deze scriptie toegevoegd.

5.4 Representatieve steekproef

Ik heb twee ingangen tot de onderzoekselementen gebruikt, te weten vrienden en familie. De eerste categorie bevat de leeftijden 18 t/m 24 jaar en de tweede is zeer divers maar hoofdzakelijk ouder dan 24 jaar. Op deze manier heb ik getracht om de groep respondenten in ieder geval qua leeftijd zo breed mogelijk te nemen.

Om verder tot een representatieve groep te komen, heb ik berekend hoeveel mensen de vragenlijst in zouden moeten vullen.
Nederland heeft in 2006 een inwonersaantal van 16.334.210 mensen, waarvan er 3.975.626 onder de 20 jaar (0-19 jaar) zijn.
De som

$$18/20 * 3.975.626 = 3.578.063$$

levert het aantal mensen jonger dan 18 jaar (0-17) op.
(er wordt gedeeld door 20 omdat de genoemde leeftijdsklassen *0-19 jaar* ook 20 klassen beslaan).
Deze mensen maken geen deel uit van het onderzoek, waardoor de totale populatie uitkomt op 16.334.210 – 3.578.063 = 12.756.147 [24]

Omdat alleen de mensen die minimaal een uur per week online zijn in het onderzoek worden meegenomen, moet ook dat nog in de populatie worden verwerkt. Immers, nog niet iedere Nederlander voldoet hieraan. Ik heb de aanname gedaan dat mensen met een Internetaansluiting minimaal een uur in de week online zijn.
In 2006 heeft in Nederland 85% van alle inwoners een Internetaansluiting en is voor mij dus minimaal een uur per week online. [25]

85% van 12.756.147 is 10.842.725 en dat is de grootte van de populatie Nederlanders van 18 jaar en ouder, die minimaal een uur in de week online zijn.

Als foutmarge van de steekproefgrootte heb ik 15% gekozen, voor de betrouwbaarheid 95%, omdat dit vaak gebruikte percentages zijn en omdat op deze manier de steekproefgrootte binnen de perken van een bachelorscriptie blijft.

$15 = 1.96\sqrt{((p*(1-p)) / n)}$ ➔
$15 = 1.96\sqrt{((50*50) / n)}$ ➔
$15^2 = 1.96^2*((50*50) / n)$ ➔
$n = (1.96^2 * 50^2) / 15^2 = 43$

Daarmee is berekend dat de steekproefgrootte 43 moet zijn. Ik heb dat afgerond naar 50, omdat daarmee makkelijker gerekend kan worden en omdat de betrouwbaarheid daarmee nog een beetje wordt verbeterd.

6 Resultaten en analyse

Op 20 december 2006 ben ik begonnen met het ordenen van de data uit de vragenlijsten. De vragenlijst had op dat moment ruim twee weken online gestaan en was ingevuld door 69 respondenten.

Ik heb bij de resultaatverwerking en de analyse van deze resultaten dezelfde volgorde gehanteerd als in de vragenlijst. Per onderdeel geef ik eerst een overzicht van de resultaten, gevolgd door een analyse daarvan.
Dit is puur een overzicht van de binnengekomen antwoorden. Voor de conclusies in het kader van dit onderzoek is het nodig dat respondenten die niet voldoen aan de gestelde criteria voor onderzoekselementen (leeftijd, mate van gebruik, etc.) niet worden meegerekend. Dit komt tot uiting in sectie 7.

De ordening en daaropvolgende analyse heb ik uitgevoerd met behulp van Microsoft Excel. Ik heb voor dit programma gekozen omdat ik de resultaten van de vragenlijsten onder meer als Excel-bestand kon downloaden. Ook beheers ik Excel goed en vind ik het een handig maar niet overdreven complex programma. Met behulp van een enkele functie is het bijvoorbeeld erg gemakkelijk om het aantal respondenten met een bepaald antwoord te laten bepalen.

6.1 Leeftijd

Er werd de respondenten gevraagd naar hun leeftijd in jaren. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.1.1 Resultaten

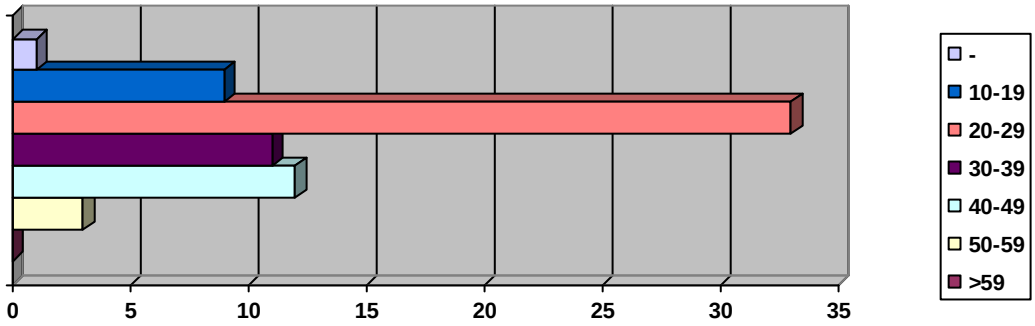
Allereerst heb ik de leeftijden geordend om daarmee een goede indeling in klassen te kunnen maken.

	0	1	2	3	4	5	6	7	8	9
0										
1				1		1		1	1	5
2	2	3	8	6	5	3	2		2	2
3	3		1	2		1	1	1		2
4	1	2	1		1	1	2	1	2	1
5		2	1							
6										
7										

Geen leeftijd ingevuld: 1
Totaal respondenten: 69

De cijfers op de y-as representeren de tientallen van de leeftijd, de cijfers op de x-as representeren de eenheden jaar binnen het tiental. Ter illustratie; er zijn dus 8 respondenten met de leeftijd van 22 jaar. Er was één respondent die geen leeftijd in heeft gevuld.

Grafische representatie:

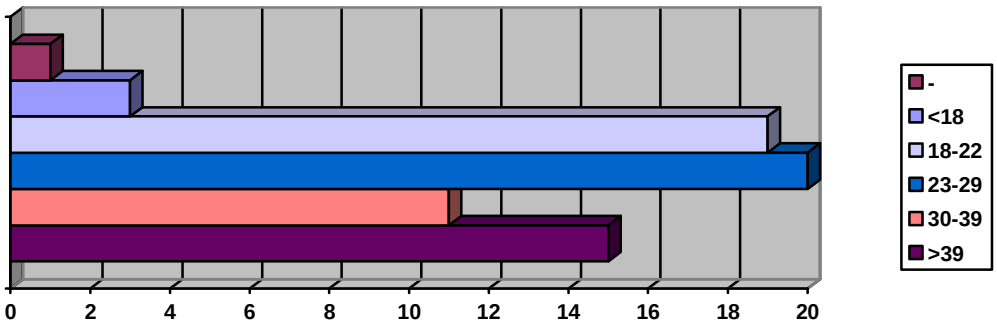


6.1.2 Analyse

In de bovenstaande grafische representatie is duidelijk te zien dat een groot deel van de respondenten in de categorie *20-29* valt.
Voor de analyse heb ik dan ook besloten om andere klassen te gebruiken dan hierboven in de grafiek staan vermeld.
Aan de hand van de resultaten, heb ik de respondenten ingedeeld in leeftijdsklassen:

jonger dan 18 jaar	3	waarvan de jongste respondent 13 jaar is
18 t/m 22 jaar	19	
23 t/m 29 jaar	20	
30 t/m 39 jaar	11	
40 jaar en ouder	15	waarvan de oudste respondent 52 jaar is
niets ingevuld	1	
Totaal respondenten	69	

Grafische weergave:



Op deze manier zijn de klassen ongeveer even groot en zijn er geen heel grote verschillen in de aantallen respondenten die in elke klasse vallen.
Het valt echter nog altijd op dat de respondenten veelal vallen in de leeftijden 18 t/m 29 jaar. Deze groep mensen lijkt dus het meeste gebruik te maken van het Internet, maar dat is niet wat in dit onderzoek verder geanalyseerd behoeft te worden.
Verder is nog opvallend dat – ondanks dat de groep "jongere" respondenten erg groot is – de "oudste" groep van respondenten weer groter is dan de tussenliggende klasse *30 t/m 39 jaar*.

Het blijkt dat 3 respondenten niet voldoen aan het criteria *18 jaar of ouder*. Hun resultaten over de bereidheid om een stukje online privacy in te leveren voor terrorismebestrijding, zullen niet worden meegerekend in de conclusies. Hetzelfde geldt voor de ene respondent die geen leeftijd invulde.

6.2 Geslacht

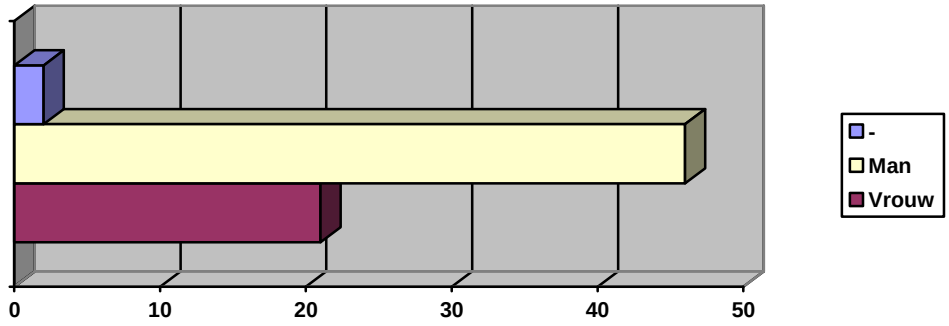
Er werd de respondenten gevraagd naar hun geslacht. Mogelijke antwoorden daarvoor waren *man* of *vrouw*. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.2.1 Resultaten

De respondenten zijn opgedeeld naar geslacht.

Man	46
Vrouw	21
Niets ingevuld	2
Totaal respondenten	69

Grafische representatie:



6.2.2 Analyse

Er hebben aanzienlijk meer mannen dan vrouwen de vragenlijst ingevuld. Twee respondenten hebben geen geslacht opgegeven en deze respondenten worden dan ook niet meegenomen in de conclusies van dit onderzoek.

6.3 Nationaliteit

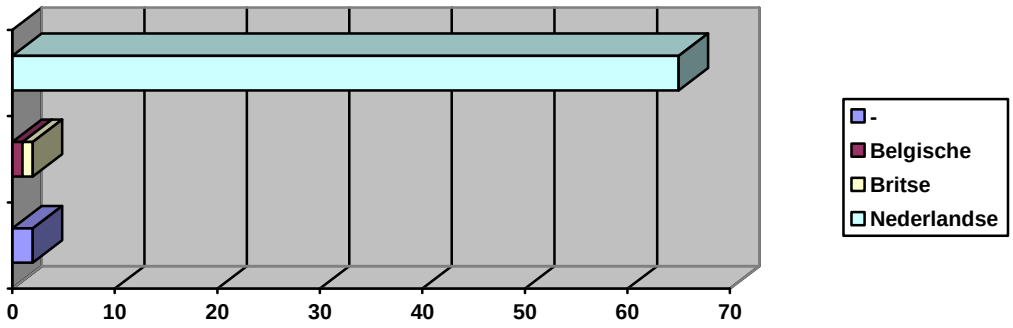
Er werd de respondenten gevraagd naar hun nationaliteit. Als ze meer dan een nationaliteit zouden hebben, werd gevraagd de nationaliteit te kiezen waar men zich het meest mee verbonden voelt. Mogelijke antwoorden daarvoor waren *Nederlandse* of *anders, namelijk*…. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.3.1 Resultaten

De respondenten zijn opgedeeld naar nationaliteit.

Nederlandse	65		
Anders	2	Belgische	Britse
Niets ingevuld	2		
Totaal respondenten	69		

Grafische representatie:



6.3.2 Analyse

Twee respondenten gaven geen antwoord op deze vraag. Op twee andere respondenten na, gaven alle respondenten aan de Nederlandse nationaliteit te hebben. Daarmee voldoen ze dus vrijwel allemaal aan het gestelde criteria voor de onderzoekselementen.
Eén respondent gaf aan de Belgische nationaliteit te hebben, één andere respondent gaf aan de Britse nationaliteit te hebben. Twee respondenten hebben geen nationaliteit ingevuld. De resultaten van deze vier respondenten zullen niet worden meegenomen in de conclusies van dit onderzoek.

Het was misschien interessant geweest om ook een conclusie te trekken over hoe verschillende nationaliteiten zouden hebben geantwoord op de bereidheid op privacy in te leveren in ruil voor terrorismebestrijding, maar er waren te weinig (slechts twee) respondenten met een andere nationaliteit dan de Nederlandse, om daar echt een gedegen oordeel over te kunnen bepalen. Dit was trouwens niet opgenomen in de oorspronkelijke opzet van het onderzoek.

6.4 Woonland

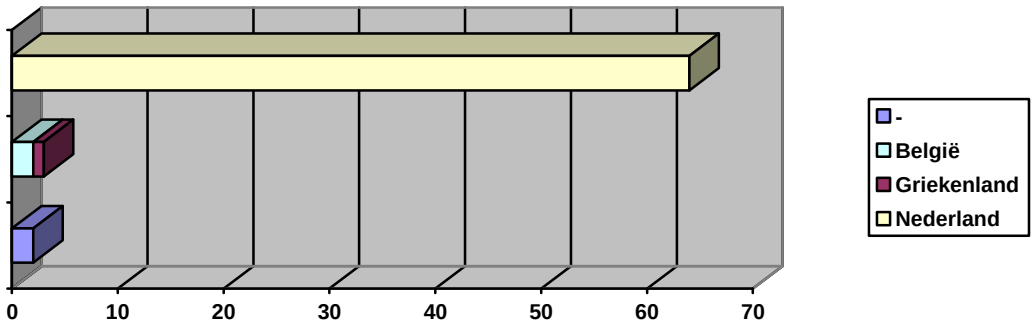
Er werd de respondenten gevraagd naar het land waarin ze woonachtig zijn. Mogelijke antwoorden daarvoor waren *Nederland* of *anders, namelijk*…. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.4.1 Resultaten

De respondenten heb ik opgedeeld naar woonland.

Nederland	64		
Anders	3	2x België	Griekenland
Niets ingevuld	2		
Totaal respondenten	69		

Grafische representatie:



6.4.2 Analyse

Op vier respondenten na, gaven alle respondenten aan woonachtig te zijn in Nederland. Daarmee voldoen ze dus vrijwel allemaal aan het gestelde criteria voor de onderzoekselementen.
Twee respondenten gaven aan te wonen in België, één andere vulde in woonachtig te zijn in Griekenland. Twee respondenten hebben niets ingevuld. De resultaten van deze vier respondenten worden niet meegenomen bij de conclusie in dit onderzoek.

Het was misschien interessant geweest om ook een conclusie te trekken over hoe respondenten die woonachtig zijn in verschillende landen zouden hebben geantwoord op de bereidheid op privacy in te leveren in ruil voor terrorismebestrijding, maar er waren te weinig (slechts drie) respondenten met een ander woonland dan Nederland, om daar echt een gedegen oordeel over te kunnen bepalen. Dit was trouwens niet opgenomen in de oorspronkelijke opzet van het onderzoek.

6.5 Mate van gebruik

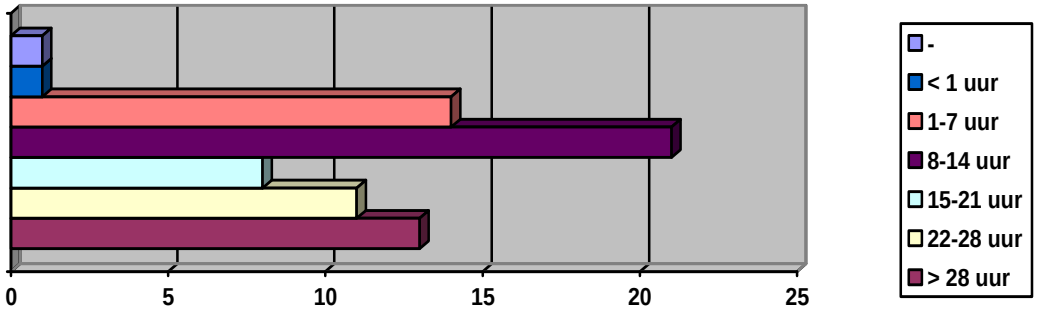
Er werd de respondenten gevraagd naar hoeveel uren ze gemiddeld per week online zijn. Mogelijke antwoorden daarvoor waren de antwoordklassen *minder dan 1 uur, 1 t/m 7 uur, 8 t/m 14 uur, 15 t/m 21 uur, 22 t/m 28 uur* of *29 uur of meer* (zie voor verantwoording van deze klassen sectie 5.3). Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.5.1 Resultaten

De respondenten zijn opgedeeld naar het aantal uren dat ze online zijn.

minder dan 1 uur online	1
1 t/m 7 uur online	14
8 t/m 14 uur online	21
15 t/m 21 uur online	8
22 t/m 28 uur online	11
29 uur of meer online	13
Niets ingevuld	1
Totaal respondenten	69

Grafische representatie:



6.5.2 Analyse

Het valt duidelijk af te lezen dat de meeste respondenten vallen in de klasse *8 t/m 14 uur online*. Opvallend is misschien verder nog dat de klassen *1 t/m 7 uur online*, *22 t/m 28 uur online* en *29 uur of meer online* (de op één na kleinste en de twee grootste klassen) bijna even groot zijn.
Eén respondent vulde in minder dan 1 uur per week online te zijn en voldoet derhalve niet aan de criteria voor de onderzoekselementen (minimaal 1 uur per week online). Diens resultaten worden derhalve samen met die van de ene respondent die niets invulde bij deze vraag, niet meegenomen bij de conclusies in dit onderzoek.

6.6 Soort gebruik

Er werd de respondenten gevraagd naar de activiteiten die online worden uitgevoerd. Mogelijke antwoorden daarvoor waren de antwoordklassen *surfen en websites bezoeken, lezen en versturen van e-mail, chatten in een chatbox, MSN Messenger/Live Messenger/ICQ/etc.* of *anders, namelijk*…. Er waren voor deze vraag meerdere antwoorden mogelijk voor de respondent. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.6.1 Resultaten

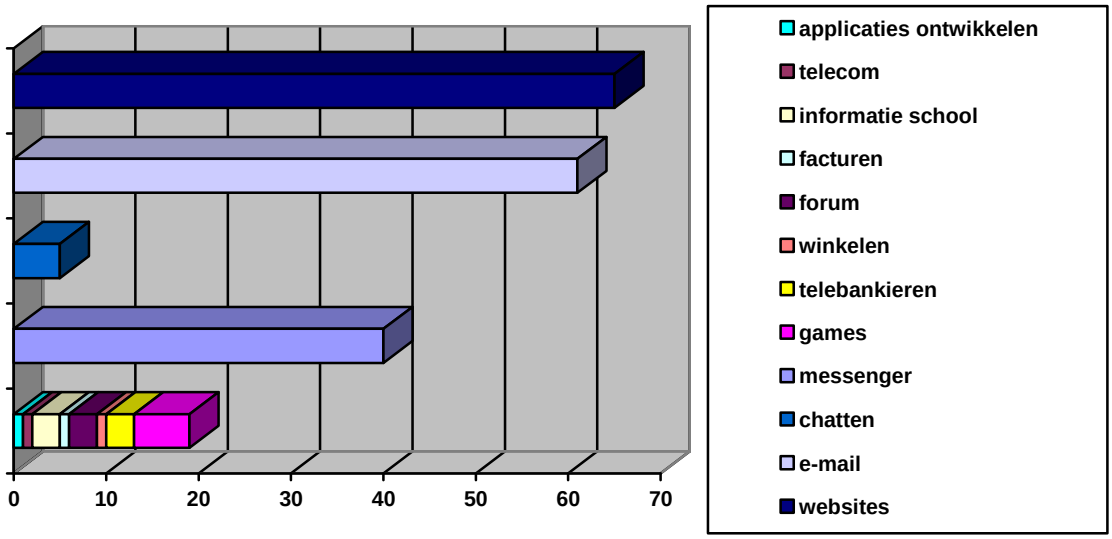
De respondenten heb ik opgedeeld naar de activiteiten die worden uitgevoerd op het Internet.

surfen en websites bezoeken	65
lezen en versturen van e-mail	61
chatten in een chatbox	5
messenger	40
anders	16

Antwoorden die werden gegeven in de categorie *Anders*, waren:

online games spelen	6
telebankieren, bankzaken	3
online winkelen/kopen	1
forum bezoeken	3
lezen van facturen	1
informatie opvragen voor school, huiswerk	3
telecomzaken	1
ontwikkelen van applicaties	1

Grafische representatie:



6.6.2 Analyse

Het is niet mogelijk om de antwoorden bij elkaar op te tellen en zo het aantal respondenten te bepalen, omdat er meerdere antwoorden mogelijk zijn op deze vraag.
Surfen en het bezoeken van websites is samen met e-mailen de meest uitgevoerde activiteit op het Internet. Chatten blijft ver achter bij de overige activiteiten. Dat is wellicht te wijten aan een enorme opkomst van de Messengers de afgelopen jaren, maar een dergelijke analyse valt buiten het kader van dit onderzoek.

Deze vraag was bedoeld om de respondenten eruit te filteren die geen van de reeds genoemde activiteiten op het Internet uitvoeren (maar bijvoorbeeld wel iets anders). De volgende vragen gaan immers over de bereidheid om een stuk online privacy in te leveren, waarbij het stuk privacy reeds is gedefinieerd in termen van de reeds genoemde activiteiten (zie sectie 3). Respondenten die slechts andere activiteiten dan de reeds genoemde zouden uitvoeren, zouden dus buiten het onderzoek zijn gevallen. Echter, geen van de respondenten heeft alleen andere activiteiten.

Wat opvallend is, is dat een aantal respondenten in de categorie *Anders* activiteiten invulden, die wat mij betreft zouden worden ingedeeld in een van de reeds genoemde antwoordcategorieën. Telebankieren, forum bezoeken, informatie opvragen voor school en online winkelen zijn vormen van een website bezoeken.

6.7 Bereidheid

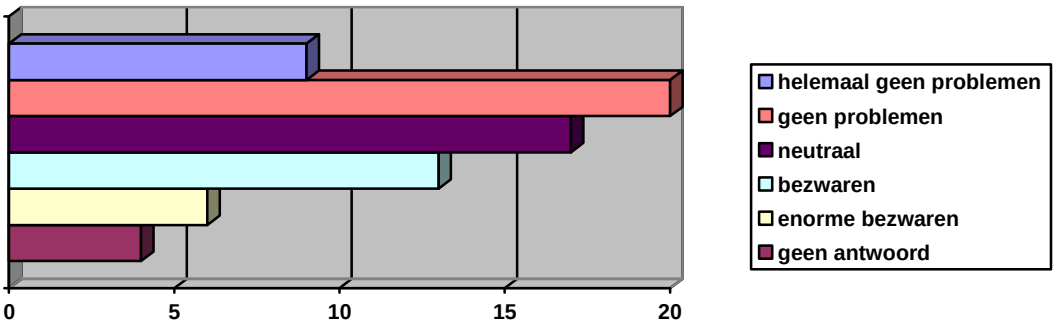
Deze vraag is opgesplitst in twee vragen en gaat over de bereidheid om een stukje privacy in te leveren zonder vermelding van de doeleinden (met een vraag voor een motivatie).
Er werd de respondenten gevraagd naar hun mening wanneer hun surfdata, e-mailverkeer, chatdata en Messengerdata zou worden opgeslagen bij de Internet Service Providers. Er was een antwoord mogelijk op een schaal van vijf, die liep van *helemaal geen problemen mee* tot *enorme bezwaren tegen*. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.7.1 Resultaten

De respondenten heb ik opgedeeld naar de bereidheid om een stukje privacy in te leveren (zonder dat het doeleinde is vermeld).

helemaal geen problemen mee	9
geen problemen mee	20
neutraal	17
bezwaren tegen	13
enorme bezwaren tegen	6
geen antwoord	4
totaal respondenten	69

Grafische representatie:



6.7.2 Analyse

In de vraag was niet aangegeven voor welke doeleinden de opgeslagen informatie zou worden opgeslagen. De meeste respondenten hebben deze vraag neutraal beantwoord (wellicht omdat ze onzeker zijn over de doeleinden), waarbij het uiteindelijk licht doorslaat naar de kant van geen problemen.
Vier respondenten hebben deze vraag niet ingevuld, waardoor over hun mening logischerwijs geen conclusie kan worden getrokken.

6.8 Bereidheid motivatie

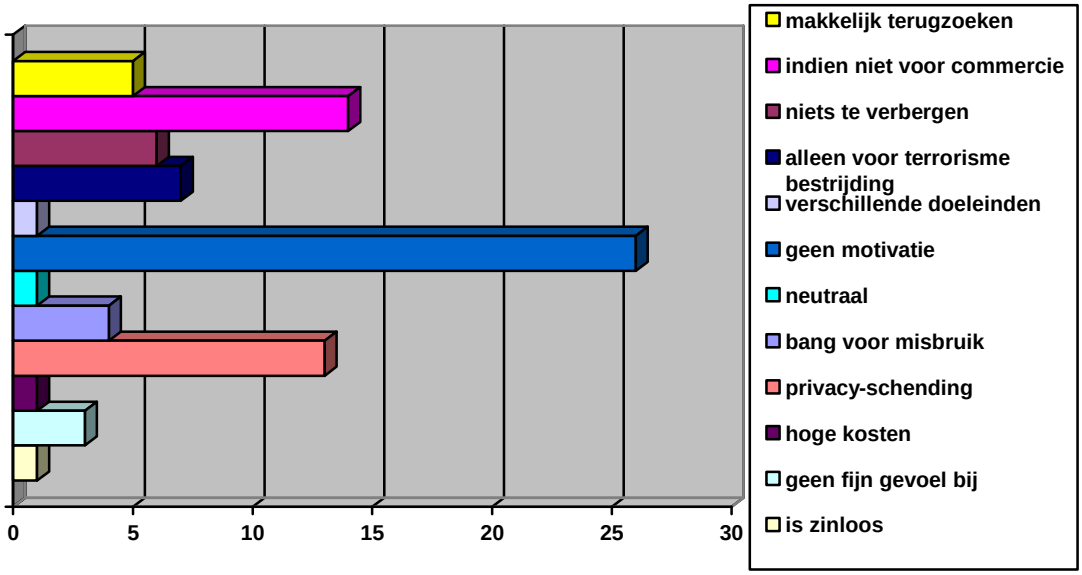
Er werd bij deze vraag ook gevraagd naar een motivatie voor het geselecteerde antwoord. Deze motivatie kon vrij door de respondent worden getypt en is door mij in klassen ingedeeld. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.8.1 Resultaten

De respondenten heb ik opgedeeld naar hun motivatie voor hun bereidheid voor het inleveren van een stukje privacy (zonder dat het doeleinde is vermeld).

makkelijk bij terugzoeken	5
indien niet voor commerciële doeleinden, geen misbruik en goed beveiligd	14
niets te verbergen	6
alléén voor terrorismebestrijding, veiligheid of als bewijsmateriaal	7
goed voor verschillende doeleinden	1
ik ben hier neutraal in	1
geen motivatie	26
bang voor misbruik van de gegevens	4
wil geen privacy inleveren, schending van privacy	13
hoge kosten	1
geen fijn gevoel bij, geen fijne gedachte	3
is zinloos	1

Grafische representatie:



6.8.2 Analyse

Het is niet mogelijk om de antwoorden bij elkaar op te tellen en zo het aantal respondenten te bepalen, omdat er meerdere antwoorden mogelijk zijn op deze vraag. Het valt op dat er veel respondenten geen motivatie hebben gegeven voor het geselecteerde antwoord op de vorige vraag. Ik denk dat dat een gevolg is van mijn keuze om deze vraag open te laten en respondenten niet de behoefte hebben om zelf hun motivatie te typen. Als er antwoordcategorieën waren geweest waaruit de respondent had kunnen kiezen, was de non-respons op deze vraag wellicht veel kleiner geweest.
Een ander punt is dat een aantal respondenten een motivatie gaven als: *als mijn gegevens worden opgeslagen op mijn computer kan ik deze gemakkelijk terugvinden*. Dat is een fout in de vraagstelling vind ik, omdat ik daar duidelijk had moeten vermelden dat de gegevens zouden worden opgeslagen bij de Internet Service Providers.

De twee motivaties die er verder uitspringen zijn:

- aan de *positieve* kant *prima, als het niet voor commerciële doeleinden wordt gebruikt, er geen misbruik van kan worden gemaakt of als de gegevens goed beveiligd zijn.*
- aan de *negatieve* kant *bang voor misbruik van mijn gegevens.*

6.9 Bereidheid terrorismebestrijding

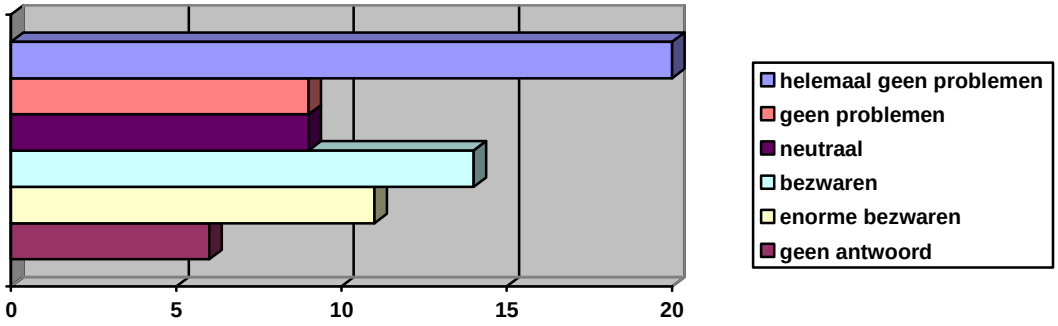
Deze vraag is opgesplitst in twee vragen en gaat over de bereidheid om een stukje privacy in te leveren voor terrorismebestrijding.
Er werd de respondenten gevraagd naar hun mening wanneer hun surfdata, e-mailverkeer, chatdata en Messengerdata zou worden opgeslagen bij de Internet Service Providers, wanneer deze gegevens zouden kunnen worden opgevraagd en gebruikt voor terrorismebestrijding. Er was een antwoord mogelijk op een schaal van vijf, die liep van *helemaal geen problemen mee* tot *enorme bezwaren tegen*. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.9.1 Resultaten

De respondenten heb ik opgedeeld naar de bereidheid om een stukje privacy in te leveren voor terrorismebestrijding.

helemaal geen problemen mee	20
geen problemen mee	9
neutraal	9
bezwaren tegen	14
enorme bezwaren tegen	11
geen antwoord	6
totaal respondenten	69

Grafische representatie:



6.9.2 Analyse

Als is vermeld dat de gegevens worden opgeslagen ten behoeve van terrorismebestrijding, blijkt het merendeel van de respondenten helemaal geen problemen ermee te hebben om een stukje van hun privacy in te leveren. Toch heeft 20% er ook dan bezwaren tegen en 16% zelfs enorme bezwaren tegen.
Zes respondenten hebben deze vraag niet ingevuld, waardoor over hun mening logischerwijs geen conclusie kan worden getrokken.

6.10 Bereidheid terrorismebestrijding motivatie

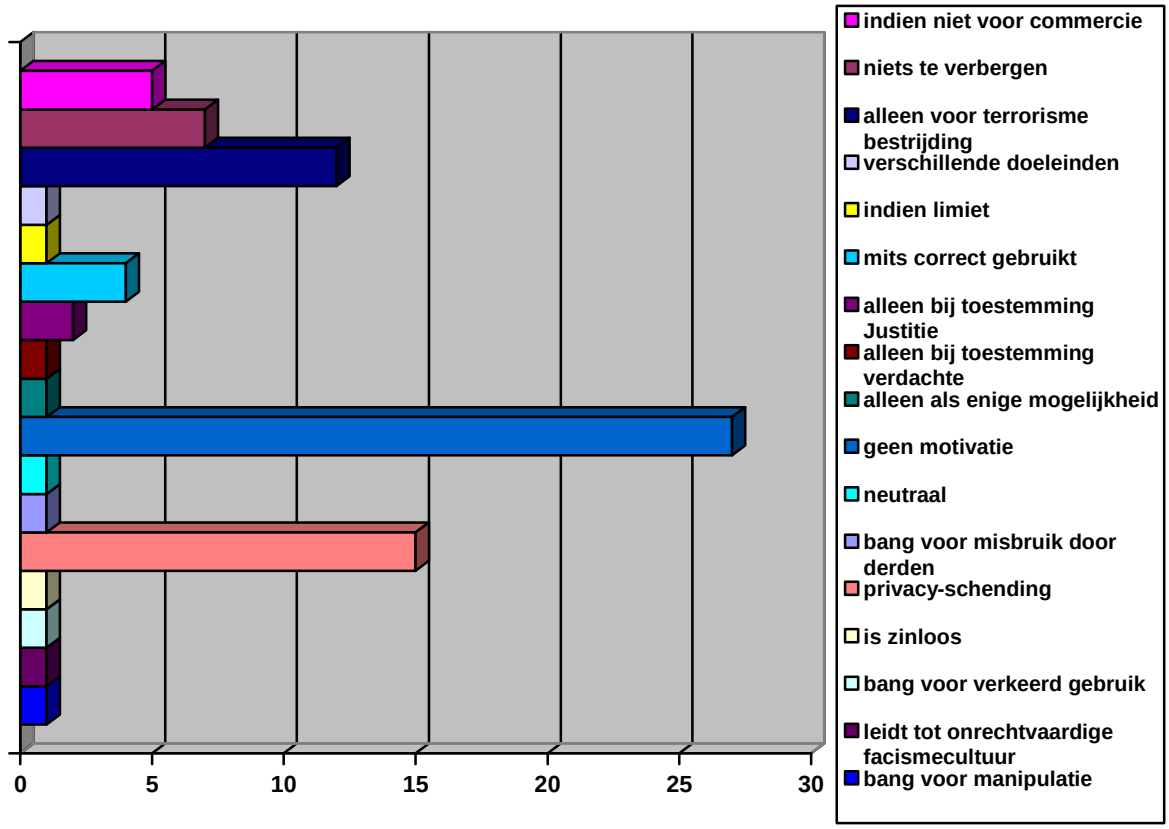
Er werd bij deze vraag ook gevraagd naar een motivatie voor het geselecteerde antwoord. Deze motivatie kon vrij door de respondent worden getypt en is door mij in klassen ingedeeld. Allereerst geef ik de resultaten weer, gevolgd door een analyse daarvan.

6.10.1 Resultaten

De respondenten heb ik opgedeeld naar hun motivatie voor hun bereidheid voor het inleveren van een stukje privacy voor terrorismebestrijding.

indien niet voor commerciële doeleinden, geen misbruik en goed beveiligd	5
niets te verbergen	7
alléén voor terrorismebestrijding, veiligheid of als bewijsmateriaal	12
goed voor verschillende doeleinden	1
indien limiet op aantal dagen dat de gegevens worden opgeslagen	1
mits correct gebruikt door opsporingsinstanties of aantoonbaar nuttig kan zijn	4
alléén bij toestemming van Justitie	2
alléén bij toestemming van de verdachte	1
alléén als dit de enige mogelijkheid is	1
ik ben hier neutraal in	1
geen motivatie	27
bang voor misbruik van de gegevens door andere organisaties/bedrijven	1
wil geen privacy inleveren, schending van privacy	15
is zinloos	1
bang voor verkeerd gebruik door de opsporingsinstanties	1
leidt tot een onrechtvaardige propaganda liefhebbende facismecultuur	1
bang voor manipulatie of het verkeerde uit de context halen van woorden	1

Grafische representatie:



6.10.2 Analyse

Het is niet mogelijk om de antwoorden bij elkaar op te tellen en zo het aantal respondenten te bepalen, omdat er meerdere antwoorden mogelijk zijn op deze vraag. Het valt op dat er veel respondenten geen motivatie hebben gegeven voor het geselecteerde antwoord op de vorige vraag. Ik denk dat dat een gevolg is van mijn keuze om deze vraag open te laten en respondenten niet de behoefte hebben om zelf hun motivatie te typen. Als er antwoordcategorieën waren geweest waaruit de respondent had kunnen kiezen, was de non-respons op deze vraag wellicht veel kleiner geweest.

Er zijn vrij veel respondenten die nog altijd vinden dat het opslaan van de gegevens een schending van de privacy is (15 respondenten). Echter, dat is de enige antwoordklasse aan de *negatieve* kant waarin meer dan één antwoord is ingedeeld.
De *positieve* kant heeft verschillende kleinere antwoordklassen met meer dan één antwoord. De motivatie *prima, als het wordt gebruikt voor terrorismebestrijding of veiligheid* (12) en *ik heb niets te verbergen* (7) springen eruit.

7 Conclusie

Om conclusies over de resultaten te kunnen trekken en daarmee de onderzoeksvraag te kunnen beantwoorden, moeten er eerst nog een aantal criteria worden verwerkt en relaties worden onderzocht:

- de bereidheid voor terrorismebestrijding gemeten voor Nederlandse gebruikers van het Internet, zoals is afgebakend in sectie 3;
- de relatie geslacht en de bereidheid tot inleveren privacy voor terrorismebestrijding;
- de relatie leeftijd en de bereidheid tot inleveren privacy voor terrorismebestrijding;
- de relatie mate van gebruik en de bereidheid tot inleveren privacy voor terrorismebestrijding.

Hierbij is het van belang dat respondenten die niet voldoen aan de gestelde criteria (op het gebied van leeftijd, nationaliteit, woonland, uren online en soort gebruik) of die een van de vragen (met uitzondering van de motivatievragen) niet hebben beantwoord, niet worden meegenomen in de conclusies. Er blijven daardoor 53 respondenten over voor de conclusie.

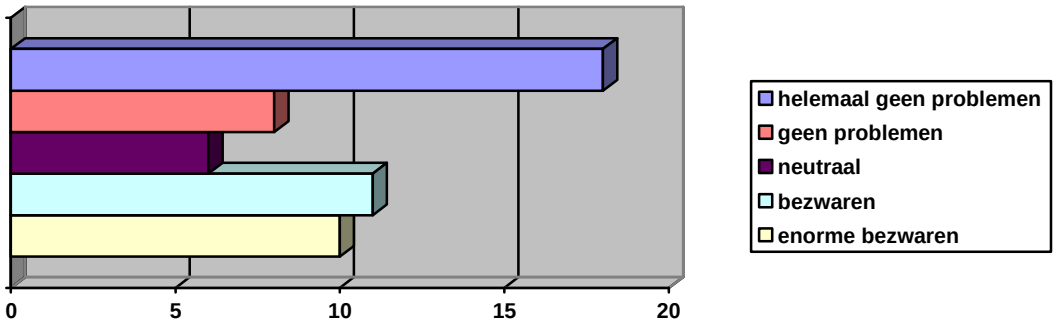
Ook kan er een conclusie worden getrokken of dat het een rol speelt dat mensen weten dat hun gegevens worden opgeslagen voor opsporingsinstanties of dat dat juist niets uitmaakt.

7.1 De bereidheid voor terrorismebestrijding

De 53 respondenten heb ik opgedeeld naar de bereidheid om een stukje privacy in te leveren voor terrorismebestrijding.

helemaal geen problemen mee	18
geen problemen mee	8
neutraal	6
bezwaren tegen	11
enorme bezwaren tegen	10
totaal respondenten	53

Grafische representatie:



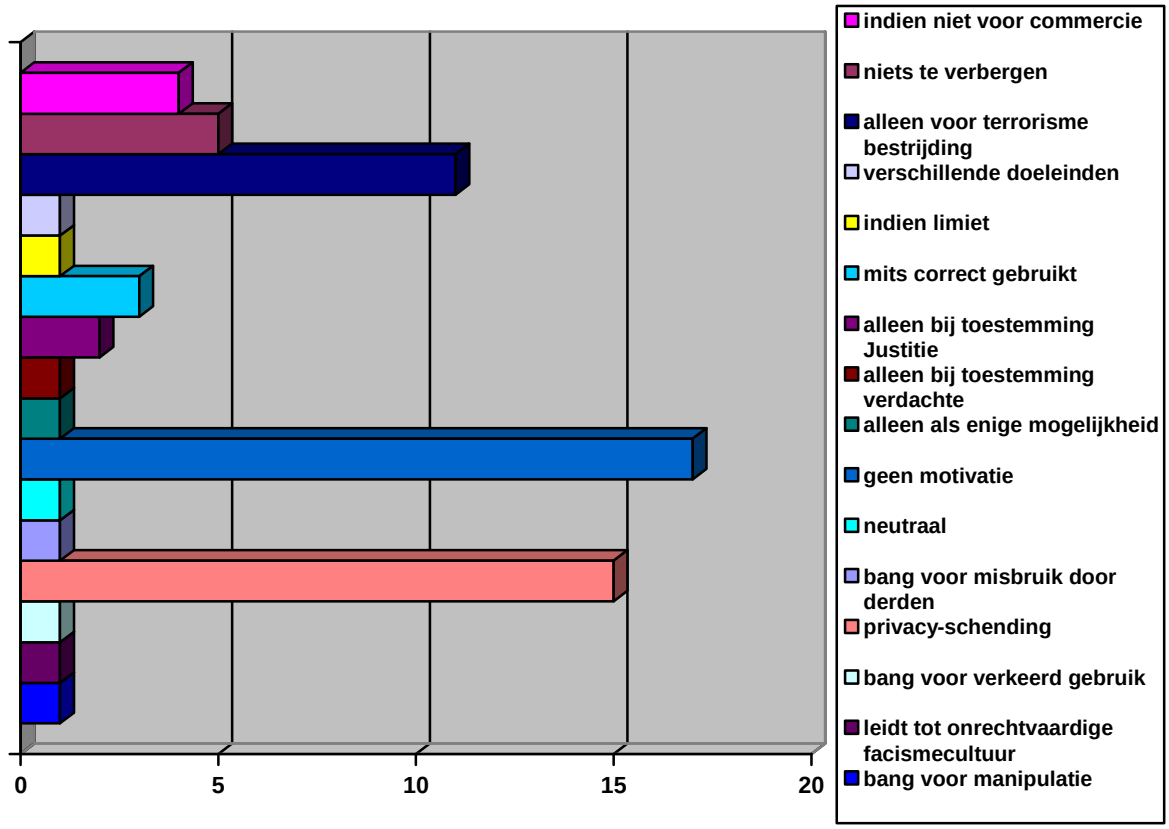
Na de correctie blijkt het merendeel van de respondenten nog altijd helemaal geen problemen ermee te hebben om een stukje van hun privacy in te leveren voor terrorismebestrijding. Als de twee klassen aan de "positieve" kant bij elkaar worden opgeteld en worden samengevat onder *bereid*, blijkt dat 18+8=26 respondenten / 53 = 49% bereid is om een stukje online privacy in te leveren voor terrorismebestrijding. Toch is de groep met (enorme) bezwaren nog altijd vrij groot: (11+10) / 53 = 40%.

De klasse “neutraal” is beduidend kleiner geworden (6 / 53 = 11%). Wellicht is dit te verklaren doordat de respondenten die niet echt een mening hebben betreffende het onderwerp, ook niet gemotiveerd zijn om alle vragen goed in te vullen en daardoor niet mee kunnen worden genomen in dit onderzoek.

Ook de motivatie is bijgesteld voor de 53 respondenten:

indien niet voor commerciële doeleinden, geen misbruik en goed beveiligd	4
niets te verbergen	5
alléén voor terrorismebestrijding, veiligheid of als bewijsmateriaal	11
goed voor verschillende doeleinden	1
indien limiet op aantal dagen dat de gegevens worden opgeslagen	1
mits correct gebruikt door opsporingsinstanties of aantoonbaar nuttig kan zijn	3
alléén bij toestemming van Justitie	2
alléén bij toestemming van de verdachte	1
alléén als dit de enige mogelijkheid is	1
ik ben hier neutraal in	1
geen motivatie	17
bang voor misbruik van de gegevens door andere organisaties/bedrijven	1
wil geen privacy inleveren, schending van privacy	15
bang voor verkeerd gebruik door de opsporingsinstanties	1
leidt tot een onrechtvaardige propaganda liefhebbende facismecultuur	1
bang voor manipulatie of het verkeerde uit de context halen van woorden	1

De motivatie *is zinloos* is hiermee verdwenen.
Grafische representatie:



Er is door de correctie weinig veranderd in de verhouding tussen de klassen onderling.

Er zijn vrij veel respondenten die nog altijd vinden dat het opslaan van de gegevens een schending van de privacy is (15 respondenten). Echter, dat is de enige antwoordklasse aan de "negatieve" kant waarin meer dan één antwoord is ingedeeld.
De "positieve" kant heeft verschillende kleinere antwoordklassen met meer dan één antwoord. De motivatie *prima, als het wordt gebruikt voor terrorismebestrijding of veiligheid* (11). Wel is de klasse *ik heb niets te verbergen* kleiner geworden.

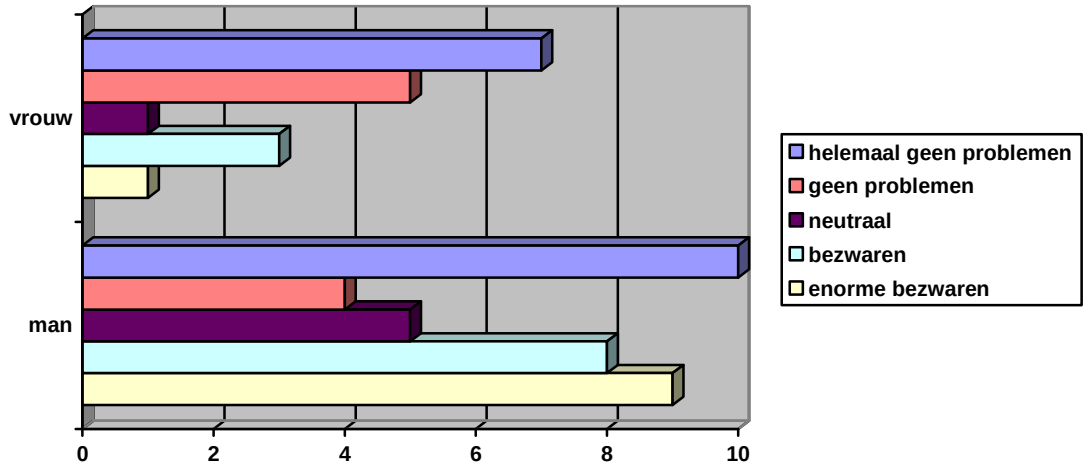
7.2 Relatie geslacht en bereidheid terrorismebestrijding

Met behulp van deze relatie kan worden bepaald of het geslacht een rol speelt in de bereidheid van mensen om een stukje van hun online privacy op te geven voor terrorismebestrijding. Ik geef eerst een overzicht van de resultaten van de relatie, gevolgd door een analyse ervan.
Respondenten die niet voldoen aan de gestelde criteria voor de onderzoekselementen (zoals is afgebakend in sectie 3), worden niet meegenomen in deze relatie. Datzelfde geldt voor respondenten die geen antwoord gaven op de vraag naar hun bereidheid voor terrorismebestrijding.

De respondenten zijn opgedeeld naar geslacht en de bijbehorende bereidheid om een stukje online privacy op te offeren voor terrorismebestrijding.

	man	vrouw	totaal
helemaal geen problemen mee	10	7	17
geen problemen mee	4	5	9
neutraal	5	1	6
bezwaren tegen	8	3	11
enorme bezwaren tegen	9	1	10
totaal respondenten	36	17	53

Grafische representatie:



Het valt af te lezen dat vrouwen over het algemeen geen of helemaal geen problemen hebben om privacy in te leveren voor terrorismebestrijding: (7+5) / 17 = 71%. Het merendeel van de vrouwelijke respondenten valt in een van deze twee *positieve* antwoordcategorieën. Aan de "negatieve" kant vallen slechts (3+1) / 17 = 24% respondenten. Verder zijn 1 / 17 = 5% van de vrouwelijke respondenten "neutraal".
Bij de mannelijke respondenten is de bereidheid veel meer verdeeld. De meeste mannen hebben helemaal geen problemen met het inleveren van een stukje privacy voor terrorismebestrijding,

maar de tweede en derde grootste klasse zitten juist helemaal aan de andere – "negatieve" – kant. Aan de "positieve" kant zit (10+4) / 36 = 39% van de mannen, (8+9) / 36 = 47% van de mannelijke respondenten zit aan de "negatieve" kant. Bij de mannen is 5 / 36 = 14% "neutraal".

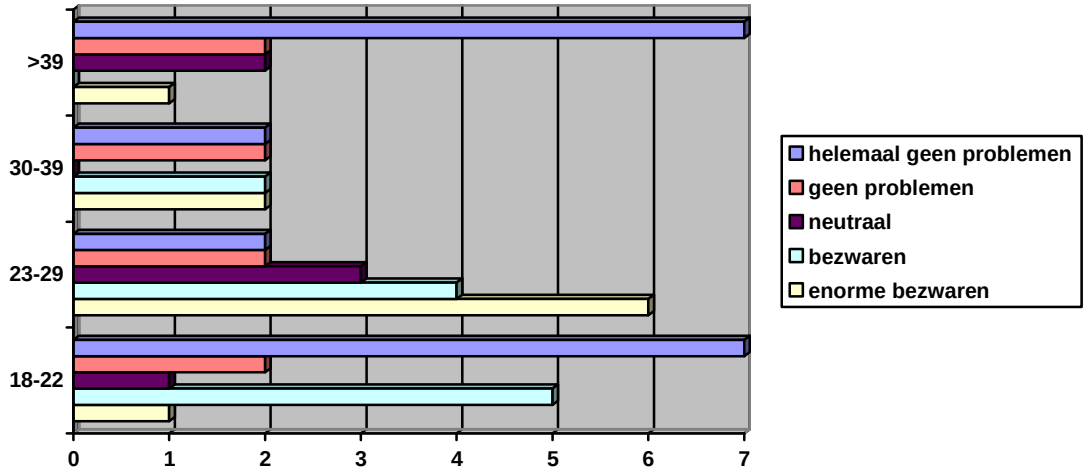
7.3 Relatie leeftijd en bereidheid terrorismebestrijding

Met behulp van deze relatie kan worden bepaald of de leeftijd een rol speelt in de bereidheid van mensen om een stukje van hun online privacy op te geven voor terrorismebestrijding. Ik geef eerst een overzicht van de resultaten van de relatie, gevolgd door een analyse ervan.
Respondenten die niet voldoen aan de gestelde criteria voor de onderzoekselementen (zoals is afgebakend in sectie 3), worden niet meegenomen in deze relatie. Datzelfde geldt voor respondenten die geen antwoord gaven op de vraag naar hun bereidheid voor terrorismebestrijding.

De respondenten zijn opgedeeld naar leeftijd en de bijbehorende bereidheid om een stukje online privacy op te offeren voor terrorismebestrijding.

	18-22	23-29	30-39	>39	totaal
helemaal geen problemen mee	7	2	2	7	18
geen problemen mee	2	2	2	2	8
neutraal	1	3	0	2	6
bezwaren tegen	5	4	2	0	11
enorme bezwaren tegen	1	6	2	1	10
totaal respondenten	16	17	8	12	53

Grafische representatie:



Uit de resultaten van de relatie kan worden afgelezen dat de respondenten die er helemaal geen problemen mee hebben om een stukje privacy in te leveren voor terrorismebestrijding, vooral ouder zijn dan 39 jaar of vallen in de klasse 18 t/m 22 jaar.
Geen problemen ("gematigd positief") is voor alle leeftijdsklassen ongeveer gelijk.
In de klasse 18 t/m 22 jaar zit (7+2) / 16 = 56% aan de "positieve" kant, in de klasse ouder dan 39 jaar is dat (7+2) / 12 = 75%, in de klasse 23 t/m 29 jaar is dat slechts (2+2) / 17 = 24 % en in de klasse 30 t/m 39 jaar is dat (2+2) / 8 = 50%.
Enorme bezwaren zijn er vooral onder respondenten in de leeftijd van 23 t/m 29 jaar.
Bezwaren ("gematigd negatief") tegen het inleveren van online privacy blijken vooral onder respondenten uit de twee *jongste* leeftijdsklassen te zijn.

In de klasse 23 t/m 29 jaar zit (4+6) / 17 = 59% aan de "negatieve" kant, in de klasse 18 t/m 22 jaar is dat (5+1) / 16 = 38%, in de klasse 30 t/m 39 jaar is dat (2+2) / 8 = 50 % en in de klasse ouder dan 39 jaar is dat slechts (0+1) / 12 = 8%.

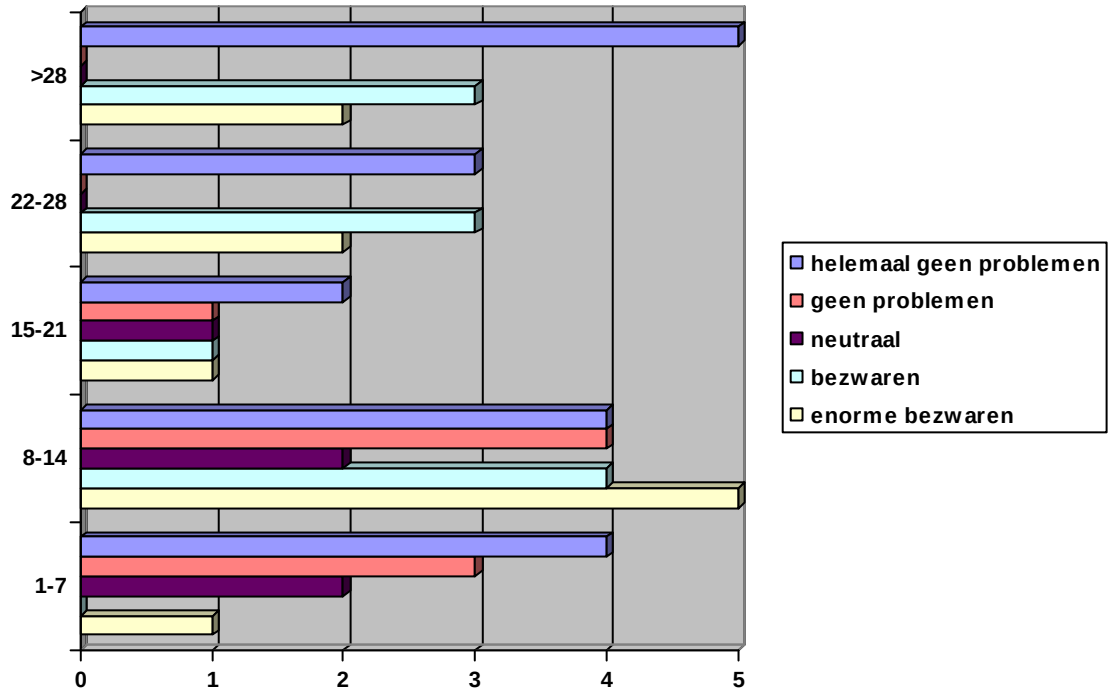
7.4 Relatie mate van gebruik en bereidheid terrorismebestrijding

Met behulp van deze relatie kan worden bepaald of de mate van gebruik een rol speelt in de bereidheid van mensen om een stukje van hun online privacy op te geven voor terrorismebestrijding. Ik geef eerst een overzicht van de resultaten van de relatie, gevolgd door een analyse ervan. Respondenten die niet voldoen aan de gestelde criteria voor de onderzoekselementen (zoals is afgebakend in sectie 3), worden niet meegenomen in deze relatie. Datzelfde geldt voor respondenten die geen antwoord gaven op de vraag naar hun bereidheid voor terrorismebestrijding.

De respondenten zijn opgedeeld naar mate van gebruik als uren online per week en de bijbehorende bereidheid om een stukje online privacy op te offeren voor terrorismebestrijding.

	1-7	8-14	15-21	22-28	>28	totaal
helemaal geen problemen mee	4	4	2	3	5	18
geen problemen mee	3	4	1	0	0	8
neutraal	2	2	1	0	0	5
bezwaren tegen	0	4	1	3	3	11
enorme bezwaren tegen	1	5	1	2	2	11
totaal respondenten	10	19	6	8	10	53

Grafische representatie:



Uit de resultaten van de relatie kan worden afgelezen dat onder de respondenten die meer dan 28 uur online per week zijn, het meest voorkomende antwoord *helemaal geen problemen* is. Opvallend is dat de tweede en derde grootste klasse daarbij aan de "negatieve" kant zitten. In deze klasse zit

(5+0) / 10 = 50% aan de "positieve" kant, en de andere (3+2) / 10 = 50% aan de "negatieve" kant.
Bij de categorie respondenten die 22 t/m 28 uur per week online zijn *helemaal geen problemen* en *bezwaren* even groot, gevolgd door *enorme bezwaren*. De "negatieve" kant is hier beduidend groter, namelijk (3+2) / 8 = 63%, dan de "positieve" kant met (3+0) / 8 = 37%.
In de categorie 15 t/m 21 uur per week online zijn alle klassen gelijk verdeeld, met als enige uitschieter de klasse *helemaal geen problemen*. Aan de "positieve" kant zitten (2+1) / 6 = 50% van de respondenten, tegenover (1+1) / 6 = 33% aan de "negatieve" kant.
Ook in de categorie 8 t/m 14 uur per week online is er sprake van een verdeling over de klassen. Daar is echter de klasse *enorme bezwaren* het grootst en is de klasse *neutraal* het kleinst. In deze categorie zit (4+4) / 19 = 42% van de respondenten aan de "positieve" kant, en (4+5) / 19 = 47% aan de "negatieve" kant. Ook de "neutrale" respondenten zijn hier in verhouding erg talrijk: 2 / 19 = 11%.
Tot slot de categorie 1 t/m 7 uur per week online. Daarin is een aflopende lijn te tekenen over de klassen. De klasse *helemaal geen problemen* is het grootst, gevolgd door *geen problemen, neutraal* en *enorme bezwaren*. Hier valt (4+3) / 10 = 70% van de respondenten aan de "negatieve" kant, tegenover (0+1) / 10 = 10% aan de "positieve" kant. De "neutrale" respondenten zijn hier groter dan de "positieve" kant met 2 / 10 = 20%.

7.5 Relatie bereidheid en bereidheid terrorismebestrijding

Dan is het ook nog interessant om te bekijken of het van invloed is geweest dat de respondenten ervan op de hoogte waren dat het inleveren van het stukje privacy gebruikt zou worden voor terrorismebestrijding, of dat ze hiervan niet op de hoogte waren. De resultaten hiervan zijn eerder besproken en geanalyseerd in sectie 6.9 en 6.10.

Deze relatie is eenvoudig te bepalen door de antwoorden op de antwoordschaal om te zetten naar cijfers, waarmee gerekend kan worden:

- helemaal geen problemen mee → 1
- geen problemen mee → 2
- neutraal → 3
- bezwaren tegen → 4
- enorme bezwaren tegen → 5

Door vervolgens de *antwoordcijfers* voor beide vragen afzonderlijk bij elkaar op te tellen (dus een som te nemen voor de bereidheid en de bereidheid voor terrorismebestrijding), kun je zien of er sprake is van een groot verschil in antwoorden op beide vragen.
Uiteraard worden ook hier respondenten die niet voldoen aan de gestelde criteria voor de onderzoekselementen (zoals is afgebakend in sectie 3), niet meegenomen in deze berekening. Datzelfde geldt voor respondenten die geen antwoord gaven op de vraag naar hun bereidheid en/of hun bereidheid voor terrorismebestrijding. Daarmee is tevens bepaald dat er voor beide vragen evenveel respondenten zijn en dat het dus eerlijk en verantwoord is om te vergelijken.

De som van de bereidheid komt bij 53 respondenten uit op 148, de som van de bereidheid voor terrorismebestrijding op 146. Er zit dus nauwelijks verschil tussen de antwoorden op beide vragen.

7.6 Conclusietrekking

Nu alle gegevens zijn verzameld, geordend en geanalyseerd en ook de relaties zijn blootgelegd, kan er een conclusie worden getrokken met betrekking tot de onderzoeksvraag. Voor de duidelijkheid zal ik deze nog eenmaal vermelden:

Zijn Nederlandse gebruikers van het Internet bereid om een deel van hun privacy op het Internet op te offeren in ruil voor meer veiligheid in de vorm van terrorismebestrijding? Waarom wel of waarom niet en hangt dit af van geslacht, leeftijd of mate van gebruik?

Nederlandse gebruikers van het Internet zijn bereid om een deel van hun privacy op het Internet op te geven voor terrorismebestrijding. Uit de onderzoeksresultaten blijkt dat bijna de helft (49%) van de Internetters er (helemaal) geen problemen mee heeft dat een stukje van hun online privacy wordt opgeslagen en kan worden opgevraagd door de opsporingsinstanties in de strijd tegen terrorisme.
Toch is een kleine kanttekening hier op zijn plaats, omdat er ook een groep van 40% is die (enorme) bezwaren heeft tegen inleveren van online privacy voor terrorismebestrijding. Deze mensen vinden het vooral een schending van het recht op privacy. Ik denk daarom dat dit onderzoek geen argument vóór mag zijn om over te gaan tot het invoeren van een wet die het opslaan van de online privacy vastlegt.

Hoewel de meeste respondenten aangaven dat ze er helemaal geen problemen mee hebben om een stukje online privacy in te leveren voor terrorismebestrijding, blijkt uit de motivaties dat er wel degelijk een voorwaarde wordt gesteld aan het opslaan en het gebruiken van deze gegevens. Zo willen de Nederlandse Internetters de zekerheid dat de opgeslagen gegevens alleen worden gebruikt voor terrorismebestrijding of het waarborgen van de veiligheid en absoluut niet voor commerciële doeleinden.

Geslacht speelt duidelijk een rol in de bereidheid van Nederlandse Internetters om online privacy in te leveren. Maar liefst 71% van de vrouwen is bereid om deze gegevens te laten opslaan, tegen slechts 39% van de mannen. Van de mannen geeft zelfs 47% geen toestemming, tegen 24% van de vrouwen. Vrouwelijke gebruikers van het Internet zijn dus meer bereid om online privacy op te offeren voor terrorismebestrijding dan mannelijk Interrnetters.

Ook de leeftijd is van invloed op de bereidheid. Uit het onderzoek blijkt dat vooral de Internetters ouder dan 39 jaar geen problemen hebben met het opslaan van hun online privacy voor terrorismebestrijding. In die leeftijdscategorie is slechts 8% negatief over het opslaan van hun gegevens. Ook in de leeftijd 18 tot en met 22 jaar is dit beeld te zien; 56% is positief tegenover 38% negatief. In de leeftijd 30 tot en met 39 jaar is het gelijk verdeeld en van 23 tot en met 29 jaar is het merendeel van de Internetters negatief (59%), tegen 24% positief.

Voorts blijkt uit de resultaten dat de mate van gebruik, gemeten in het aantal uren dat men online is per week, van invloed is op de bereidheid. Van de Internetters die 1 tot en met 7 uur per week online zijn, is 70% positief met betrekking tot het inleveren van online privacy voor terrorismebestrijding. Ook de Internetters die 15 tot en met 21 uur per week online zijn, zijn meer positief (50%) dan negatief (33%).
Alle andere soorten gebruikers geven over het algemeen geen toestemming voor het inleveren van hun online privacy voor terrorismebestrijding. Met name de groep gebruikers die 22 tot en 28 uur per week online is, is erg negatief. Uit deze groep Internetters is maar liefst 63% tegen het inleveren van de online privacy. Er kan dus worden geconcludeerd dat mensen die weinig tijd doorbrengen op het Internet minder waarde hechten aan hun online privacy (in het kader van terrorismebestrijding) dan fervente Internetters.

Tot slot kan worden geconcludeerd dat het voor de bereidheid van respondenten geen verschil maakt of het gaat om het inleveren van online privacy voor onbekende doeleinden, of voor specifieke antiterrorisme doeleinden. De motivaties verschillen echter wel sterk voor deze twee kwesties.

8 Slotwoord

De opkomst van terrorisme heeft de gebruiker van het Internet overtuigd om een stukje van zijn privacy op het Internet in te leveren. Een conclusie die ik op voorhand niet had durven te trekken, maar die me uiteindelijk ook niet verbaast. Veiligheid(sgevoel) wordt verkozen boven privacy.
Ik heb het afgelopen halfjaar meer inzicht gekregen in dit boeiende vraagstuk. Voorstanders proberen tegenstanders te overtuigen, en andersom. Beide kanten hebben duidelijke en goede argumenten en dat geeft aan hoe moeilijk de kwestie is.
Ook heb ik getracht een beeld te schetsen van hoe de Nederlandse internetter er tegenaan kijkt. Dat is in mijn ogen goed gelukt en ik wil via deze weg iedereen bedanken die heeft meegewerkt aan het totstandkomen van het onderzoek en deze scriptie. In het bijzonder bedank ik Dhr. Luca Consoli, voor zijn tijd en inzet tijdens de begeleiding van mijn onderzoek en scriptie.

John Akkermans, 21 januari 2007
J.Akkermans@student.ru.nl

9 Referenties

[1] C. Kruyskamp: *Van Dale, Groot Woordenboek der Nederlandse taal*, negende druk, 1970, Nijhoff Uitgeverij, p. 1580

[2] Wikipedia, de Vrije Encyclopedie : Privacy, http://nl.wikipedia.org/wiki/Privacy, bekeken op 20/12/2006.

[3] J. Turow: *Americans and online privacy*, University of Pennsylvania, 2003, pp. 3-4

[4] S. Asrani: *Security versus Liberty: Striking the Right Balance. A Comparison of Anti-Terror Provisions in India and the United States*, German Law Journal, Vol. 9, [13]-[14], [25]-[29]

[5] Wikipedia, de Vrije Encyclopedie : ECHELON, http://nl.wikipedia.org/wiki/ECHELON, bekeken op 2/1/2007.

[6] Andrea Foster: *Your E-Mail Message to a Colleague Could Be Tomorrow's Headline*, The Chronicle, http://chronicle.com/free/v48/i41/41a03101.htm, bekeken op 2/1/2007.

[7] *The Conference on Computers, Freedom and Privacy*, http://www.cfp.org/

[8] Gabriel Weimann: *How Modern Terrorism Uses The Internet*, Special Report USIP, Vol. 116

[9] M. France: *Privacy in the Age of Terror*, Business Week, 5 november 2001

[10] Bruce Schneier: *We're Giving Up Privacy and Getting Little in Return*, Minneapolis Star Tribune, 31 mei 2006

[11] Richard Morin: *Poll: Most Americans support NSA's Efforts*, Washington Post, 16 mei 2006

[12] D. Balz, C. Deane: *Differing Views on Terrorism*, Washington Post, 11 januari 2006

[13] *Americans Protect Civil Liberties*, Policy Brief The Institute for Public Policy and Social Research, Vol. 4, april 2002

[14] Jasper Koning: *Nederlanders vinden aftappen mail geen probleem*, http://www.zdnet.nl/News.cfm?id=14271, bekeken op 2/1/2007.

[15] *Nederlanders bang voor misbruik van internet*, http://www.sif.nl/?page=9&catid=6&object=142283, bekeken op 2/1/2007.

[16] *Nederlander verdeeld over uitbreiding bevoegdheden AIVD, niet bang voor privacyschending*, https://secure.mijnopinie.nl/index.php?pagina_id=2&nieuws_id=17&loginID=f535efab34ee99dc18eedb156267aace, bekeken op 2/1/2007.

[17] Peter Vermaas: *Angst alom*, De Groene Amsterdammer, 20 oktober 2001

[18] L.F. Asscher: *BVD heeft geen nieuwe bevoegdheden nodig*, NRC Handelsblad, 15 oktober 2001, p. 8

[19] Wieneke Gunneweg: *Geheimzinnige sluier rond aftappen*, Univers, 22 juni 2006

[20] Sander van Walsum, *Het gevaar van minder privacy,* De Volkskrant, 6 oktober 2001

[21] *Factor: privacy in oorlogstijd*, IKON, aflevering 2, 11 september 2004

[22] J. Segers: *Methoden voor de maatschappijwetenschappen*, Van Gorcum & Comp BV Assen, 1999, pp. 63, 67, 175-178

[23] *newrulez presenteert jongerenonderzoek*, http://www.sanoma-young.nl/Nieuws%20-%20homepage/2006/newrulez%20presenteert%20jongerenonderzoek.aspx, bekeken op 27/10/2006.

[24] Centraal Bureau voor de Statistiek: *Bevolking; kerncijfers*, http://statline.cbs.nl/StatWeb/Table.asp?STB=T&LA=nl&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,(l-1)-l&HDR=G1

[25] Centraal Bureau voor de Statistiek: *Onderzoek ICT gebruik bij personen*, http://statline.cbs.nl/StatWeb/table.asp?STB=T&LA=nl&DM=SLNL&PA=71098ned&D1=33-133&D2=0-2&HDR=G1

A Bijlagen

A.1. Vragenlijst