Radboud Universiteit Nijmegen

Masteropleiding Informatiekunde

Onderzoeksplan

Geautomatiseerde privacyonderhandeling tussen gebruiker en applicaties

Versie	1.1
Student	Leon Krol (0333700)
Datum	15-05-2006, Nijmegen

“Privacy is not something that I’m merely entitled to, it’s an absolute prerequisite.”
Marlon Brando

“The right to be let alone is indeed the beginning of all freedom.”
Justice William O. Douglas

Inhoud

Inleiding

In dit hoofdstuk zal ingegaan worden op de op opzet van dit document en zal tevens een verantwoording hiervoor bieden door in te gaan op de gebruikte methode. Dit document is het plan van aanpak voor mijn afstudeeronderzoek. Hoewel dit plan van aanpak op eerdere voorstellen en de daarop verkregen feedback gebaseerd is, was ik niet tevreden over de oorspronkelijke richting van het onderzoek, daar het concept ingehaald is door de actualiteit en ik niet meer overtuigd was van het nut van het uitvoeren van nog een dergelijk onderzoek. Aanvankelijk was het idee opgevat om de privacyrisico's van adware en spyware te inventariseren met als doel een schaal te ontwikkelen waarmee de mate van privacyschending door applicaties gemeten kan worden. Bijkomend doel was het eenduidig en objectief definiëren van begrippen als spyware en adware. Dit plan was opgezet omdat niet altijd duidelijk was wat de criteria waren van anti-adware producenten om software als adware te classificeren, daarbij zorgde de ambiguïteit van begrippen als spyware voor onbegrip bij de doorsnee computergebruiker. Gevolgen hiervan zijn terug te vinden in [Borland 2004] [Jacobsson 2004][SpywareInfo] en [Nu.nl]. Inmiddels heeft Lavasoft, producent van anti-adware programmatuur, hun Threat Assessment Chart (TAC) [Lavasoft] gepubliceerd op de bedrijfssite. Bovendien is het Anti Spyware Coalition gekomen met een definitie van het begrip spyware die een industriebreed draagvlak beoogd [ASC2005 1] en een categoriseringsschema [ASC2005 2]. Deze ontwikkelingen maakten het noodzakelijk om met het onderzoek een nieuwe weg in te slaan om alsnog iets nieuws bij te kunnen dragen. De nieuwe vraagstelling is gericht op het afstemmen van de privacybehoeftes van gebruikers met de privacypolicies van software. In het volgend hoofdstuk zal ingegaan worden op de centrale probleemstelling.

Dit onderzoek zal worden verricht in het kader van de masteropleiding Informatiekunde aan de Radboud Universiteit Nijmegen en dient derhalve aan de door deze instelling opgelegde eisen te voldoen. Op de website van het Master Thesis lab van het Nijmeegs instituut voor Informatica en Informatiekunde (NIII) [MTL] staan de volgende eisen vermeld:

Procesgerichte eisen

De student moet laten zien zelfstandig in staat te zijn de volgende taken uit te voeren:

1. een complex probleem te analyseren en te modelleren,
2. literatuur te bestuderen en toe te passen,
3. een innovatieve oplossing te formuleren en te onderbouwen,
4. eventueel deze oplossing te realiseren, en
5. het verworven inzicht in een scriptie te beschrijven en dit mondeling te presenteren.

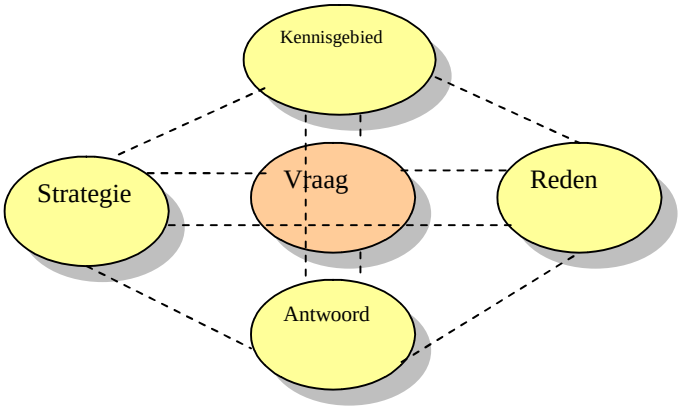
Productgericht

Bij de beoordeling van de scriptie wordt gelet op de volgende punten:

a. een samenvatting in de vorm van een abstract,
b. een goede formulering van de probleemstelling,
c. een heldere en goede inhoudelijke beschrijving van het verrichte werk,
d. een duidelijke conclusie,
e. een overzichtelijke literatuurlijst,
f. een goede schrijfstijl en correct taalgebruik,
g. een goede mondelinge presentatie.

Het uitvoeren van het afstudeeronderzoek wordt gewaardeerd op 18 european credits (EC). Uitgaande van een studiebelasting van ongeveer 28 uur per EC is de totale belasting (18 * 28 =) 504 uur, wat neerkomt op ruim 12 weken bij een fulltime tijdsbesteding. Bij de planning is er daarom uitgegaan van een tijdsbestek van drie maanden voor de uitvoering van het onderzoek en het schrijven van de scriptie, hierbij de tijd voor het opstellen van dit plan van aanpak niet meegerekend. Dit onderzoek zal begeleid worden door dr. Jaap-Henk Hoepman en dr. Martijn Oostdijk, beiden verbonden aan de onderzoeksgroep Security of Systems (SOS) binnen het NIII.

Gedurende het opstellen van dit Plan van Aanpak is er langzaam gegroeid naar de huidige vorm en invulling. Getracht is om aan alle academische eisen aan onderzoeksplannen te voldoen door de meest gangbare notatiewijze en indeling aan te houden zoals gevonden bij andere onderzoeksplannen. Verder valt te vermelden dat de huidige invulling is gedaan volgens het model van [Oost 2003]. Onderstaand schema geeft de positie van de onderzoeksvraag weer in dit model.



Figuur 1: Positionering onderzoeksvraag

Door de vraagstelling vanuit de domeinen: Kennisgebied, Strategie, Reden en Antwoord te bekijken wordt ervoor gezorgd dat de vraagstelling voldoende verankerd, relevant, precies, functioneel en consistent is. Doordat de genoemde domeinen elkaar ook onderling beïnvloeden is dit document iteratief tot stand gekomen door steeds een domein toe te voegen aan het plan en vervolgens het geheel consistent te maken.

Probleemstelling

In deze paragraaf wordt de centrale probleemstelling besproken. Een van de zegeningen van het Internet is de eenvoud waarmee gebruikers een grote hoeveelheid aan informatie en software tot hun beschikking hebben. Softwareproducenten hebben een direct kanaal tot de eindgebruiker. Gebruikers kunnen eenvoudig software downloaden en installeren. De software die aangeboden wordt (via het Internet) valt in een vijftal categorieën op te delen:

- *Commerciële software*
  Voor commerciële software dient de gebruiker eerst een aankoopprijs te betalen alvorens hij de applicatie mag gebruiken. Deze vorm van software kan via het Internet goedkoper zijn omdat op diverse overheadkosten bespaard kan worden. Dat ook commerciële software niet altijd rekening houdt met de privacy van zijn gebruikers komt af en toe in de actualiteit [Byers 2003], [Webwereld].

- *Shareware*
  Bij shareware wordt de gebruiker in staat gesteld om de functionaliteit van een applicatie te benutten en beoordelen. Indien deze de beproefde functionaliteit na de proeftijd wenst te gebruiken dient er tot aanschaf over gegaan te worden. Veelal weigert de applicatie te functioneren zonder een activatiecode. Dit wordt ook wel eens ‘try-before-you-buy software genoemd’.

- *Adware*
  Adware is voortgekomen uit de shareware gedachte. Waar shareware-producenten hun inkomsten krijgen van de gebruiker zelf, krijgen adware producenten hun inkomsten van adverteerders. De producenten bouwen in hun programmatuur features in voor het weergeven van diverse reclame-uitingen. Deze reclameruimte wordt vervolgens verkocht aan adverteerders. Dat adverteerders hier geld voor over hebben komt mede doordat er gericht geadverteerd kan worden. Dat kan omdat vaak informatie van gebruikers als hun locatie, leeftijd en surf gedrag wordt verzameld. Voor deze privacyinbreuk en advertentieruimte krijgt de gebruiker de beschikking over de programmafunctionaliteit.

- *Malware*
  Malware is de verzamelnaam van alle software dat zich onethisch/illegaal gedraagt. Dit uit zich veelal in installaties zonder medeweten van de gebruiker en verborgen functionaliteit zoals het analyseren en het verzenden van het surfgedrag van de gebruiker. Op deze manier kan adware ook malware zijn. Producenten gaan dan voor het verkopen van zoveel mogelijk advertentieruimte waardoor deze ongemerkt hun applicaties willen laten gebruiken.

- *Open Source Software*
  Open Source software is software waarvan de broncode vrij verkrijgbaar. Hierdoor is het mogelijk om software ontwikkelaars over de wereld mee te laten werken aan het ontwikkelen, testen en verbeteren van software. Een voordeel van het vrij inzichtelijk maken van de broncode is het vergroten van het vertrouwen erin daar er geen verborgen functionaliteit aanwezig kan zijn. Elke potentiële privacyschending is af te leiden uit de specificatie.

Dat adware en met name malware een blijvend probleem vormen valt onder meer af te leiden uit de bedragen die er mee gemoeid zijn. Op de websites van enkele ‘advertentieruimte verkopende’ bedrijven wordt aan potentiële adverteerders een indicatie gevraagd van het advertentiebudget. WhenU.com [WhenU] gaat uit van een minimum van 5000 dollar voor binnenlandse en 2000 dollar voor buitenlandse reclames en Claria [Claria] gaat zelfs uit van een minimum van 25.000 dollar. De omzet van laatstgenoemde is 90,5 miljoen dollar met een winst van 34,8 miljoen dollar in 2003 [Klang 2004] geeft een indicatie van de volwassenheid van deze tak van marketing. Deze cijfers geven voldoende reden om aan te nemen dat het gebruik van gepersonaliseerde reclame voldoende effectief wordt beschouwd door adverteerder om te blijven toepassen.

Dit onderzoek zal zich met name richten op adware en malware, waarbij ook commerciële software meegenomen wordt omdat deze eveneens de privacy kunnen schenden. Het grootste probleem is ongewenste privacyschending ten gevolge van onvolledige informatie over de werking van een programma. Gebruikers willen vaak wel persoonlijke informatie vrijgeven voor bepaalde functionaliteit, maar zodra dit zonder kennisgeving/goedkeuring gebeurt, wordt er een inbreuk gedaan op de privacy van de gebruiker. Extra aandacht zal besteed worden aan het opstellen van een privacypolicy van de gebruiker. Alle huidige middelen die tot de beschikking staan van gebruikers richten zich op de huidige technologie. Het is beter als de gebruiker kan stellen dat hij niet wenst dat verzamelde informatie tot hem te herleiden is in plaats van dat hij moet aangeven dat hij niet wenst dat zijn NAW gegevens verzameld worden. Wanneer geautomatiseerd gecontroleerd kan worden of software voldoet aan de eisen van de gebruiker ontstaat er een omgeving waarin de gebruiker een hogere mate van bescherming geniet.

De kernproblematiek is dat de gebruiker niet volledige zeggenschap heeft over zijn gegevens omdat de gebruiker zijn beslissing om een applicatie al dan niet te installeren baseert op onvolledige gegevens. De gebrekkige informatieverschaffing, betreffende de werking van een programma, is niet opgelost door het wettelijk verplicht stellen van een End User License Agreement (EULA), omdat deze te lang en onleesbaar zijn. [Good 2005]

Met het probleem inzichtelijk kan de volgende onderzoeksvraag geformuleerd worden:

“Hoe kunnen de privacybehoeftes van thuisgebruikers vertaald worden naar een geformaliseerde privacypolicy om deze te vergelijken met een geformaliseerde privacypolicy van computerapplicaties in een geautomatiseerd systeem ter bescherming van de privacy van de gebruiker.”

Iets uitgebreider verwoord omhelst deze onderzoeksvraag het verrichten van onderzoek naar de mogelijkheid tot het maken van een privacypolicy voor gebruikers en een privacypolicy voor software(producenten) teneinde deze te kunnen vergelijken in een geautomatiseerd systeem met als doel het automatisch bewaken van de privacy van de gebruiker.

Verantwoording

In deze paragraaf zal ingegaan worden op de nieuwswaarde, nut en noodzaak van het beantwoorden van de onderzoeksvraag. Bovendien zal gekeken worden naar reeds verricht relevant onderzoek en zullen gebruikte begrippen geoperationaliseerd worden.

De laatste tijd wordt er veel aandacht aan adware en spyware geschonken in de media. Veel bladen geven ook tips hoe men deze categorieën software kunnen verwijderen. Deze artikelen gaan echter meer over genezing dan preventie. Bovendien wordt er veelal voorbij gegaan aan het feit dat adware niet per definitie kwaadaardig is. Denk hierbij aan googles gMail waarbij advertenties gepresenteerd worden na een analyse van trefwoorden in persoonlijke e-mail. Ondanks deze privacyschending is de e-mail dienst erg populair zoals uit cijfers blijkt [gMail 1]. Het verhogen van het privacybewustzijn onder gebruikers is een positieve ontwikkeling, echter er wordt niet altijd rekening mee gehouden dat commerciële software eveneens een inbreuk op de privacy op kunnen leveren. Bijvoorbeeld messenger applicaties bieden de mogelijkheid om gehouden gesprekken te archiveren zonder medeweten van alle gesprekspartners. Dit onderzoek zal een mogelijkheid ter preventie van elke vorm van ongewenste/onbewuste privacyschending aandragen door middel van informering van de gebruiker.

Het verworden van computers tot gemeengoed heeft tot gevolg dat gebruikers niet per definitie computervaardig zijn. Begrippen als ‘firewall’ en ‘spyware’ blijken amper bekend [Blue Coat 2005]. Die onwetendheid heeft paradoxaal genoeg tot gevolg dat gebruikers tegenwoordig ook meer angst hebben om besmet te raken. [Nu.nl]. Het is één van de doelen van dit onderzoek om het onderscheid tussen adware en spyware en allerhande begrippen niet meer relevant te maken voor de gebruiker. Concrete informatie over de werking van software met betrekking tot persoonlijke informatie moeten hen voldoende inzicht bieden zonder dat het gebruik van verwarrende termen nodig is.

De Anti Spyware Coalitie is inmiddels gekomen met een definitie van spyware die door alle producenten van Privacy Enhancing Technology (PET) [ASC2005] overgenomen kan worden waardoor getracht is de vaagheid rond het begrip weg te nemen. Dit is echter geen goede oplossing, omdat adware met privacyschendende eigenschappen nog steeds nuttig kan zijn voor de gebruiker. Dit is zeker het geval wanneer gebruikers niet kunnen of willen kiezen voor een commerciële applicatie met de gewenste functionaliteit. Gebruikers zijn doorgaans al helemaal niet op de hoogte van privacyschendende eigenschappen van commerciële software, wat tot een vals gevoel van veiligheid kan leiden bij de gebruiker ten aanzien van de commerciële varianten. Kort gezegd: er is niet zozeer behoefte aan een duidelijke beschrijving van spyware, maar naar een betere informatieverschaffing naar de gebruiker toe over de werking van een programma. Als het aankomt op potentiële privacyschending is de scheidslijn tussen spyware/adware en commerciële software niet duidelijk te trekken.

Met de introductie van service pack 2 voor MS Windows XP zijn er diverse functies aan het besturingssysteem toegevoegd die de veiligheid zouden moeten verbeteren, ook met betrekking tot malware. Een van deze functies is het geven van waarschuwingen wanneer een uitvoerbaar bestand dat gedownload is voor het eerst uitgevoerd wordt. Deze waarschuwing geeft weer wie de uitgever van het bestand is, indien deze bekend is. Deze uitgever dient zich aangemeld te hebben bij het certificeringbedrijf Verisign. Dit is relevant voor dit onderzoek op twee niveau’s. Deze functie faciliteert het a-priori waarschuwen van de gebruiker over de mogelijke gevolgen van het installeren

van een applicatie. Ten tweede kan het gebruik maken van een certificeringsysteem helpen om de betrouwbaarheid van een ingevulde eigenschappenlijst te waarborgen met behulp van certificering.

Het Platform for Privacy Preferences (P3P) is een project van het World Wide Web Consortium (W3C) en is bedoeld om een geautomatiseerde afstemming te maken tussen de privacybehoefte van de websurfer en de privacypolicy van de te bezoeken website. In de privacypolicy staat in een standaardformaat vermeld welke informatie van een gebruiker bijgehouden wordt c.q. gevraagd en voor welke doeleinden. De gebruiker geeft aan welke informatie hij eventueel vrij wilt geven. Indien er geen afstemming plaats kan vinden zal er geen cookie geplaatst worden. Hoewel dit systeem enkele nadelen kent [Coyle 1999] is de kern van het idee, preventie van ongewenste privacyschending door websites, goed en mutatis mutandis toepasbaar op software applicaties in de breedste zin van het woord.

Nut

Na de centrale probleemstelling en verantwoording behandeld te hebben kan er gekeken worden naar de verwachte opbrengsten van het onderzoek. Welk nut valt er te verwachten? Er is een aantal winstpunten te noemen:

- Privacybehoeftes van gebruikers in kaart brengen
  In de literatuur is weinig informatie te vinden over de privacybehoeftes die er onder computergebruikers bestaat. Met het onderzoek zal inzichtelijk worden gemaakt welke behoeftes er bestaan en in welke mate deze te veralgemeniseren zijn. Door niet direct te kijken naar de huidige technische mogelijkheden, maar naar de behoeftes van de gebruiker zal de inventarisatie zodanig opgesteld zijn dat deze lange tijd nagenoeg constant zal blijven.

- Vergroting van gebruikersvertrouwen
  Wanneer gebruikers preventief gewaarschuwd worden over gevolgen van het installeren van een applicatie zal deze niet/minder geconfronteerd worden met nare gevolgen achteraf.

- Verhoogd privacybewustzijn onder gebruikers
  Indien van een applicatie de privacyschendingen niet bekend zijn, of de schendingen overtreffen de standaardvoorkeuren van de gebruiker, dan wordt de gebruiker gewaarschuwd. Hierna kan deze zelf kiezen om het programma al dan niet te gebruiken. De waarschuwing die er aan vooraf gaat maakt de gebruiker alert op eventuele privacyschendingen, waardoor deze een bewust risico loopt.

- Verhoogd privacybewustzijn onder producenten
  Veelal lijken softwarebouwers zich niet bewust te zijn van de privacygevoeligheid van de informatie, die ze verwerken en gebruiken, van de gebruikers. Denk hierbij aan populaire tekstverwerkers die o.a. de diverse auteurs van een document opslaan. Dit kan tot privacycompromitterende situaties leiden. Door fabrikanten een maatstaf te geven waarlang hun software gelegd kan worden zijn ze op voorhand bewust van de privacygevoeligheid van hun software. Dit kan leiden tot vragen over de noodzaak van dergelijk eigenschappen, aangezien gebruikers met deze informatie inzichtelijke wellicht de installatie van een ander pakket overwegen.

- Verhoogde veiligheid
  De gebruiker maakt de keuze tot installatie op basis van volledige informatie voer de werking van het programma. Het uitoefenen van het recht op privacy kan alleen wanneer er voldoende informatie voorhanden is. Het voor te stellen systeem gaat goed samen met de andere standaard security software voor de thuiscomputer als de virusscanner, de adwarescanner en de ingebouwde waarschuwingen in Windows XP Service pack 2.

Theoretisch kader

Informatiekunde is de wetenschap die zich bezighoudt met de afstemming van mens, bedrijf en (informatie)technologie. Kenmerkend hierbij is het verwerken van zachte gegevens (behoeftes van de mens) tot concrete informatie voor het ontwerp van een informatiesysteem. Aan de opleiding informatiekunde aan de Radboud Universiteit wordt dit beschreven als: ‘de exacte vaagheid’.

Dit onderzoek raakt de domeinen: privacy, informatietechnologie en security. Privacyonderzoek in het kader van dit onderzoek houdt zich voornamelijk bezig met de gevolgen die het Internet met zich meebrengt voor persoonlijke informatie. Privacy Enhancing technologies (PET’s) is het soort technologie specifiek ontworpen om de privacy van de gebruiker te beschermen. Als zodanig zal het resultaat van dit onderzoek ook in deze categorie vallen.

Daar dit onderzoek zich zal richten op privacy zal hiervan een eenduidige definitie gegeven moeten worden. De definitie die in dit onderzoek gehanteerd zal worden is als volgt:

> *Privacy is het zelfbeschikkingsrecht van de gebruikers aangaande informatie over en van henzelf .Er is dus volledige zeggenschap over het vrijgeven en gebruik van de eigen informatie.*

Er zijn al vele initiatieven voor het beschermen van de privacy in de omgeving van het Internet. Deze gaan de kant op van wetgeving en de kant van technische beschermingsmiddelen. Op wetgevingsgebied zijn veelal aanpassingen gedaan aan de huidige privacy- en copyrightwetgeving en om deze geschikt te maken voor de digitale omgeving van het Internet. De wetgeving voorziet onder andere in een opt-in regeling voor spam en installatie van software en het gebruik van EULA’s. Doordat de huidige wetgeving de probleemstelling in het eerste hoofdstuk niet oplost en dus op zichzelf nog niet voldoende bescherming biedt zal hier geen verdere aandacht aan besteed worden in dit onderzoek.

Het al eerder genoemde P3P is een project van het World Wide Web Consortium (W3C) met als doel het mogelijk maken van het geautomatiseerd omgaan met privacy policies van websites. De gebruiker geeft aan onder welke omstandigheden hij een ‘cookie’ wil accepteren en wanneer niet, door een vragenlijst in te vullen. Dit wordt gedaan door websites in gestandaardiseerde vorm hun privacy policy te laten noteren. De nieuwste versies van Internet Explorer ondersteunen P3P. Een ander gebruik van P3P is terug te zien in de zoekfunctie van de website privacyfinder [Privacybird]. Deze site biedt een zoekmachine waarbij aangegeven wordt of websites al dan niet aan de privacybehoefte van de gebruiker voldoen. Er is echter divers commentaar op P3P met als voorbeeld: [Coyle 1999]. De kern van de kritiek houdt in dat dit systeem meer de belangen behartigt van de website exploitanten in plaats van die van de bezoeker.

Het op te leveren systeem moet een geautomatiseerde onderhandeling over privacy mogelijk maken. Dit moet dienen tot een betere informatieverschaffing naar de gebruiker toe, naast de End User License Agreement. Dit systeem dient zodanig transparant te zijn dat er enkel een waarschuwing gegeven dient te worden wanneer de privacybehoefte van de gebruiker en de eigenschappen van de software niet overeen komen.

De privacybehoefte zal voor elke gebruiker anders zijn. Het belangrijkste is dat de gebruiker een keus heeft op basis van voor hem begrijpbare informatie. In de meeste definities van het begrip privacy vormt het zelfbeschikkingsrecht over persoonlijke gegevens een onderdeel. Belangrijk is om te melden dat dit onderzoek zich zal richten op thuisgebruikers van software. Onder thuisgebruikers wordt verstaan de groep gebruikers die voor persoonlijke doeleinden op een computer waar zij de beheerder van zijn software installeren en gebruiken. De gebruikers hebben dus zelf de bevoegdheid (rechten) om applicaties te installeren. In een bedrijfsomgeving vallen de beheersrechten onder de bevoegdheid van de automatiseringsafdeling van het bedrijf zelf. Daarom wordt er gekeken naar de thuisgebruikers, aangezien daar veelal onbewust de privacy geschonden wordt. In dienst van een bedrijf zullen werknemers niet werken met persoonlijke informatie waardoor het privacyvraagstuk daar minder relevant is.

Wanneer er over softwareapplicaties gesproken wordt dan dient dit in de breedste zin van het woord begrepen te worden, mits geschikt voor thuisgebruik. Bijna elk programma vraagt/verzamelt persoonlijke informatie, al dient dit niet altijd een commercieel doel zoals wel het geval is bij adware. Denk hierbij aan applicaties als MSN Messenger waarbij logboeken bijgehouden kunnen worden met transcripties van een gesprek zonder medeweten van een gesprekspartner. Het onderzoek is dus niet beperkt tot adware en malware-varianten. Deze varianten zullen eveneens bestudeerd worden omdat daar juist een grote hoeveelheid verschillende privacyschendingen voorkomen. Wanneer Adware zich installeert zonder medeweten van de gebruiker wordt dit gezien als een vorm van malware.

Zoals al gemeld, neemt Adware een prominente plaats in, in dit onderzoek. Adware is een soort software die advertenties toont op de computer in ruil voor functionaliteit. Veelal zullen de getoonde reclame-uitingen, vaak *banners* genoemd, zo veel mogelijk persoonsgericht zijn, aangezien adverteerders hier meer geld voor overhebben. Om persoonsgericht te werk te kunnen gaan is informatie over, en van de gebruiker nodig. Voorbeelden hiervan zijn interesses en demografische gegevens. Deze kunnen gevraagd worden aan de gebruiker direct, of automatisch opgezocht in persoonlijke bestanden of bepaald worden aan bijvoorbeeld het surfgedrag van de gebruikers. Het automatisch verzamelen van informatie van de gebruiker maakt een applicatie tot spyware. Verder bestaat er handel in dergelijke informatie over mensen, waarvan het verkopen van databestanden met e-mail adressen aan adverteerders een voorbeeld is. Deze korte opsomming geeft al aan dat er op verschillende niveaus de privacy van gebruikers aangetast kunnen worden. Voor veel gebruikers is dit geen groot probleem als de geleverde functionaliteit van een hoog genoeg kwaliteit is, waarbij te denken valt aan de Albert Heijn klantenkaart en de e-mail dienst van Google die technisch gesproken ook een vorm van adware is [gMail 1] en desalniettemin zeer populair is [gMail 2] Het te ontwerpen systeem zal ervoor zorgdragen dat een eventuele inbreuk niet zonder medeweten van de gebruiker kan gebeuren.

Veel valt er te leren van PET’s met betrekking tot online informatie privacy. Initiatieven als P3P, firewalls en certificaten zijn allen onder andere bedoeld om gebruikers/websurfers meer zeggenschap te geven over hun persoonlijke informatie. Helaas is de technische aard van applicaties als adware anders dan van websites waardoor er met verschillen in soorten privacyschending rekening gehouden dient te worden. Groot verschil is dat websites simpelweg geen spyware kunnen zijn want het is onmogelijk om actief informatie te kunnen verzamelen. Er zijn wel technieken om bezoekers te verlokken om spyware te installeren (drive by downloads) maar daar zou het voorgestelde systeem weer rekening mee kunnen houden.

Er is al enkele malen geschreven over P3P. Dit onderzoek zal voortborduren op de kerngedachte van P3P waarbij er sprake is van het vergelijken van privacypolicys van aan de ene kant gebruikers en aan de andere kant van software. Deze specificatie is echter niet een op een over te nemen daar P3P uitgaat van technische mogelijkheden, terwijl dit onderzoek zich vooral zal richten op de eigenlijke privacybehoeftes van de gebruiker. Bovendien richt P3P zich op websites en dit onderzoek op applicaties. Dit brengt de volgende consequenties met zich mee:

Waar bezoekers van websites er zelf voor kunnen kiezen om informatie in te vullen die niet te herleiden zijn tot henzelf is het mogelijk om zelf je anonimiteit te beschermen. Veelal maken mensen aparte E-mail accounts aan speciaal voor webbezoek bij een van de vele gratis e-mail diensten. Zo creëren mensen veelal alter-ego's die gebruikt worden bij het bezoeken van onbetrouwbaar geachte websites. Bij applicaties die thuisgebruikers installeren is er toegang mogelijk tot praktisch alle informatie die lokaal opgeslagen is en de potentiële privacyinbreuk kan dan ook vele malen groter zijn zonder dat de gebruiker zich hier bewust van is. De thuiscomputer staat het dichtst bij de gebruiker in termen van informatieopslag.

De verschillen tussen applicaties en websites zijn niet enkel te vinden op het gebied van technische mogelijkheden, maar ook op het gebied van functie, de transparantie van de werking van de applicatie, en de wijze van matching. Per genoemd punt zal in het kort aangegeven worden welke complicaties/aanpassingen te verwachten zijn. Hiermee wordt ingehaakt op de opmerking zoals gegeven in de P3P specificatie versie 1.0 dat de specificatie uitsluitend gericht is op websites en aangepast moet worden wil dit vertaald worden naar een privacysysteem gericht op applicaties.

- Functie

Waar P3P voor websites met name een geformaliseerde samenvatting is van de privacy policy zou een dergelijk systeem dat gericht is op applicaties op een vergelijkbare wijze de End Users License Agreement (EULA) moeten gebruiken. Het feit dat een EULA meer informatie en andersoortige informatie (zoals het installeren van software van derden en juridische informatie) betekent dat er meer zaken zijn om rekening mee te houden.

- Transparantie

Daar voor websites het zetten van cookies en invoervelden, waar P3P zich op richt, eenvoudig te controleren zijn is de controleerbaarheid van de werking van applicaties een stuk minder transparant. Een privacysysteem op een computerplatform is vele malen onbetrouwbaarder gezien de zwaktes van software zoals uitgebreid door virusschrijvers en adware producenten is gedemonstreerd. Specificaties zijn doorgaans niet vrij beschikbaar. Er zal een heel andere wijze van toezicht hierop gehanteerd moeten worden. De invulling hiervan zal verder onderzoek vereisen.

- Matching

Het vergelijken van privacypolicy van de gebruiker met de privacypolicy van de applicatie kan op diverse wijze ingevuld worden. Er kan gedacht worden aan een losse matchingagent die los te installeren is door de gebruiker, maar opties als online matchingdiensten zijn ook mogelijk. Aangezien P3P gericht is op websites en dus veel meer specificaties, die ook nog eens per dag kunnen wisselen, oplevert dan wanneer het gericht zou zijn op applicaties is het niet mogelijk om deze centraal op te slaan. Zodra een applicatie uitgebracht wordt heeft deze een versienummer en

een eigen specificatie. Het behoort tot de mogelijkheden om dit centraal op te slaan. of dit nuttig is dient nader onderzocht te worden.

De voornoemde verschillen tussen websites en applicaties geven een beeld van de mogelijke resultaten van het onderzoek. Het dient benadrukt te worden dat het principe van P3P, privacyafstemming, gehanteerd blijft, maar gepoogd is om aan te geven dat de invulling sterk kan afwijken wanneer niet websites maar applicaties het onderwerp van specificatie zijn. Bovendien dient benadrukt te worden dat bij P3P privacypolicies van websites centraal staat terwijl voor dit onderzoek de privacypolicy van de gebruiker centraal staat.

Methode

Domein

Dit onderzoek zal zich bezighouden met privacyrisico's voor mensen die thuis applicaties gebruiken. De thuisgebruiker heeft doorgaans andere applicaties tot zijn beschikking dat de professionele gebruiker. Daarom zal het domein afgebakend worden tot de groep van softwareproducten bedoeld voor thuisgebruik. Tevens zullen bekende vormen van adware en spyware meegenomen worden. In dit onderzoek wordt gekeken hoe de privacybehoeftes van een gebruiker geëxpliciteerd kunnen worden. Dit moet gelden voor het universele domein van thuisgebruikers van computerapplicaties.

Privacyschendende eigenschappen kunnen verschillende vormen aannemen:

- Informatie scannen op trefwoorden
- Informatie verzamelen
- Informatie verzamelen en interpreteren
- Informatie verzamelen en doorspelen aan derden

Andere eigenschappen zijn ook van belang zoals de integriteit van de dataopslag. Hoe veilig zijn de gegevens en is het zeker dat de gegevens niet eenvoudig verkregen kunnen worden. Dit is slechts een kleine opsomming van het totale aantal mogelijke privacyschendingen. Daarom is het noodzakelijk om tijd te besteden aan een grondige inventarisatie.

Onderzoeksfunctie

Dit onderzoek heeft een ontwerpfunctie. Het beoogde eindresultaat is een model/ontwerp van een geautomatiseerd systeem om gebruikers om te laten gaan met privacyrisico's van thuissoftware. Dit ontwerp is gebaseerd op een inventarisatie van software-eigenschappen, een inventarisatie van gebruikersvoorkeuren en op de voor- en nadelen van vergelijkbare systemen.

Onderzoeksvragen

Hieronder staat een overzicht van de deelvragen en de gewenste vorm van het antwoord, om de samenhang tussen de vragen inzichtelijk te maken:

Deelvraag	Resultaat
Op welke wijze kunnen de privacybe-hoeftes van een gebruiker geëxpliciteerd worden?	Een vragenlijst waarmee gebruikers hun privacybehoefte kunnen expliciteren
Welke privacyrisico's kunnen zich voor-doen bij het thuisgebruik van software-applicaties?	Een lijst van software-eigenschappen die betrekking hebben op informatie van/over de gebruiker
Wat valt er te leren van vergelijkbare systemen en relevante standaarden?	Mogelijkheden tot voorkoming van genoemde tekortkomingen (eisen aan nieuw systeem)
Hoe kan het ontwerp zo goed mogelijk organisatorisch ingebed worden?	Beschrijving van de organisatorische aspecten rond het systeem waarbij de voornoemde vragen beant-woord zijn.
Hoe ziet het model er uit?	Het ontwerpdocument
Op welke wijze kan dit systeem geschikt gemaakt worden voor een bedrijfsomge-ving	Lijst met aanpassingen aan het systeem

Deelvraag	Resultaat
Hoe zien diverse scenario's er uit gebruik-makend van het privacybescherming-systeem?	Overzicht van ingevulde scenario's met geïnventariseerde problemen

Per (deel)vraag zal besproken worden welke informatie benodigd is voor een bevredigend antwoord, waar en hoe die informatie verkregen wordt (de strategie) en hoe de informatie verwerkt en gepresenteerd zal worden.

Op welke wijze kunnen de privacybehoeftes van een gebruiker geëxpliciteerd worden?	
Gebruikers hebben verschillende behoeftes als het aankomt op hun privacy. Welke mogelijke behoeftes aan privacy bestaan er en zijn deze te veralgemeniseren naar categorieën? Het uitgangspunt zijn niet de technische eigenschappen waarbij de gebruiker aan dient te geven of deze al dan niet wenselijk zijn, maar de fundamentele privacybehoefte van de gebruiker waarna er gekeken welke technische eigenschappen daarmee in overeenstemming zijn.	
Benodigde informatie:	Een vragenlijst waarmee gebruikers hun privacybehoefte kunnen expliciteren in een geformaliseerde privacypolicy.
Informatieverzameling:	Om de privacybehoeftes te achterhalen zijn er diverse mogelijkheden. Ten eerste zal er in de literatuur gekeken moeten worden welke inventarisaties van privacybehoeftes reeds bestaan. Ten tweede zal er gekeken moeten worden naar reeds bestaande middelen ter bescherming van de privacy. Hierbij valt te denken aan P3P waarbij er reeds een mogelijkheid is om de privacybehoeftes te inventariseren. Zo zal er gekeken moeten worden welke op welke wijze deze de privacy beschermt. Nu zullen de meeste resultaten gericht zijn op technische eigenschappen, waardoor er meer tijd gestoken dient te worden in het achterhalen van de achterliggende privacybehoefte. Hiertoe dienen de intenties van de systeemontwerpers en de gebruikersmotieven achterhaalt worden. Andere systemen waar naar gekeken kan worden zijn onder andere: PGP, firewalls, freenet, anonymous proxys en anti-adaware programmatuur.
Informatieverwerking	De bovenstaande activiteiten leiden tot een lijst van privacybehoeftes samen met technische middelen. Deze moeten verwerkt worden tot een lijst van vragen waarmee de gebruiker zelf een privacypolicy op kan stellen.

Welke privacyrisico's kunnen zich voordoen bij het thuisgebruik van softwareapplicaties?	
Om te achterhalen welke privacyrisico's zich voordoen bij het gebruik van software kan er gekeken worden naar diverse bronnen, zoals literatuur over spyware en adware en security-reports van commerciële software. Concreet is de bronnenverzameling als volgt: - Spywareguide.net - Lavasoft Threat assessment chart - EPIC.org - P3P Characteristics summary	
Benodigde informatie:	Een lijst van software-eigenschappen die betrekking hebben op informatie van/over de gebruiker.
Informatieverzameling:	Aanpak: Literatuuronderzoek Domein: Softwareapplicaties bedoeld voor thuisgebruik Variabele: Softwarefunctie verbonden aan persoonlijke informatie Score: Lijst van softwarefuncties die werken persoonlijke gegevens
Informatieverwerking:	Tegengekomen risico's in het literatuuronderzoek worden, voor zover relevant, voor software, opnemen in een lijst. Per eigenschap of combinatie van eigenschappen zal aangegeven worden bij welke categorieën van privacybehoeftes deze nog toegestaan zijn.

Wat valt er te leren van vergelijkbare systemen en relevante standaarden?	
Initiatieven als P3P zijn niet zonder kritiek ontvangen. Om het onderzoek effectief te laten zijn dient er gekeken te worden naar de tekortkomingen van vergelijkbare systemen. P3P is niet het enige systeem waar naar gekeken kan worden. Er zal daarom een overzicht moeten komen van PET's en standaarden die een vergelijkbare functionaliteit hebben. De lijst van kritieken (positief en negatief) moet vertaald worden naar een document van eisen voor het voor te stellen systeem.	
Benodigde informatie:	Mogelijkheden tot voorkoming van genoemde tekortkomingen geformuleerd in termen van eisen aan het te ontwerpen systeem
Informatieverzameling:	Aanpak: Literatuuronderzoek Domein: Privacybeschermende systemen Variabele: Tekortkomingen
Informatieverwerking:	Kritieken op P3P en relevante standaarden worden verzameld en verwerkt tot een lijst van 'bad practices'. Per 'bad practice' zal een aanbeveling worden geformuleerd voor het te ontwerpen systeem.

Hoe kan het ontwerp zo goed mogelijk organisatorisch ingebed worden?	
Het systeem zoals voorgesteld bestaat uit een vragenlijst voor de gebruiker een eigenschappenlijst van de applicatie en de mogelijkheid tot het vergelijken daarvan. Bij een systeembeschrijving dient vermeld te staan hoe het systeem daadwerkelijk gebruikt dient te worden. De aspecten waar nog op ingegaan dient te worden zijn: - Hoe wordt de eigenschappenlijst ingevuld? - Op welke wijze vult de gebruiker de vragenlijst in? - Hoe vindt de technische afstemming plaats tussen de twee lijsten? - Welke security risico's zijn er bij het gebruik van dit systeem?	
Benodigde informatie:	Beschrijving van de organisatorische aspecten rond het systeem waarbij de voornoemde vragen beantwoord zijn.
Informatieverzameling:	Aanpak: Literatuuronderzoek/ontwerp Domein: PET's Variabele: Organisatorische aspecten
Informatieverwerking:	Er zal een inventarisatie gedaan worden van de mogelijkheden ter beantwoording van de voornoemde vragen door naar vergelijkbare systemen te kijken als P3P, Pretty Good Privacy (PGP) en andere PET's. Per mogelijke oplossing zal gekeken worden naar de voor- en nadelen waarbij er een beslissing gemaakt wordt die in het ontwerpdocument terecht zal komen.

Hoe ziet het model eruit?	
De voorgaande onderzoeksvragen hebben allen een enkel aspect van het systeem beschreven. Wat rest is een totaal ontwerpdocument, waarin deze aspecten samenkomen en kan fungeren als een ontwerpdocument voor het implementeren van het systeem. Door alle voorgaande vragen te beantwoorden zijn er een document van eisen, een eigenschappenlijst, een vragenlijst en aanvullende eisen geformuleerd. Deze samen worden verwerkt in het ontwerpdocument waar de volgende elementen in opgenomen zijn: - Beschrijving systeem - Inventarisatie privacyschendende eigenschappen van software - Overzicht vragenlijsten - Beschrijving van de wijze waarop de vragenlijst van de gebruiker en de eigenschappenlijst gematcht worden - Voorstellen voor organisatorische inbedding	
Benodigde informatie:	Het ontwerpdocument
Informatieverzameling:	Voor het beantwoorden van deze onderzoeksvraag zullen de antwoorden op de voorgaande deelvragen samengevat worden in een document om een consistente beschrijving van privacybeschermings-programma te geven. Voor dit document worden de volgende hoofdstukken geschreven: • Functionele specificatie • Beschrijving vragenlijst gebruiker • Overzicht privacyschendende eigenschappen van software • Organisatorische aspecten De randvoorwaarden voor de invulling van deze hoofdstukken bestaan uit: - De lessons-learned van vergelijkbare initiatieven - De beschrijving dient platform-onfhankelijk te zijn
Informatieverwerking:	De lay-out van de applicatie hangt af van de organisatorische inbedding en de mogelijkheid tot het matchen van de gebruikerslijst en de producentenlijst. Er wordt dus voortgeborduurd op de vorige vragen. Waar nodig wordt wel ingegaan op te gebruiken protocollen in verband met de veiligheid

Op welke wijze kan dit systeem geschikt gemaakt worden voor een bedrijfsomgeving?	
Dit onderzoek richt zich in beginsel op thuisgebruikers wat tot gevolg heeft dat het systeem niet direct geschikt is voor toepassing in een bedrijfsomgeving. Door te kijken welke aanpassingen benodigd zijn om het systeem voor andere omgevingen geschikt te maken ontstaat er zicht op hoe generiek het systeem daadwerkelijk is alsmede welke privacyrisico's er in een bedrijfsomgeving bestaan.	
Benodigde informatie:	Lijst met aanpassingen aan het systeem
Informatieverzameling:	Als eerste dient inzichtelijk gemaakt te worden welke privacyrisico's en installatieoverwegingen in een bedrijfsomgeving bestaan. Hiertoe zal er gekeken worden naar applicaties bestemd voor professionele toepassingen en de daaraan verbonden informatieverzamelende eigenschappen. Verder dient er gekeken te worden naar de infrastructurele beperkingen en mogelijkheden een bedrijfsomgeving biedt. Een netwerkomgeving met vele gebruikers kunne gevolgen hebben voor de het systeemontwerp. Alle omstandigheden die een dergelijke omgeving met zich meebrengt dienen in kaart gebracht te worden.
Informatieverwerking:	Alle geïnventariseerde privacyrisico's dienen verwerkt te worden tot een aangepaste privacypolicy voor zowel de gebruiker als voor de softwarekant. Bovendien zal de systeemspecificatie geld moeten worden naar de infrastructuurbeschrijving om te komen tot een lijst van noodzakelijke aanpassingen.

Hoe zien diverse scenario's er uit gebruikmakend van het privacybeschermingsysteem?	
Diverse scenario's dienen opgesteld die allen de huidige problematiek van gebrekkige privacybescherming demonstreren. In de scenario's dient op een realistische wijze weergegeven te worden op welke wijze het nieuwe systeem gebruikt wordt en al dan niet de huidige problemen verhelpt. De scenario's dienen uit te gaan van thuisgebruikers én zakelijke gebruikers zoals gedefinieerd in de voorgaande onderzoeksvraag.	
Benodigde informatie:	Overzicht van ingevulde scenario's met geïnventariseerde problemen
Informatieverzameling:	De scenario's dienen zodanig opgesteld te worden dat ze een van de huidige problemen omtrent privacyschendende software illustreren. Kijkend naar de doelstellingen van dit onderzoek kan middels scenario's concreet aangegeven worden op welke wijze matching van privacypolicies hier verbetering in aanbrengt. Bovendien dient tenminste één van de scenario's in te gaan op de problematiek van privacyschendende software binnen een bedrijfsomgeving. Hiervoor zal gekeken worden naar de problematiek en de aangegeven wijzigingen aan het systeem zoals voortgekomen uit de voorgaande deelvraag.
Informatieverwerking:	Na het opstellen van de scenario's zal er gekeken worden naar de eventuele tekortkomingen in het systeem. Blijven enkele aspecten van de huidige problematiek bestaan, dan moeten deze geïnventariseerd worden om een realistische inschatting te kunnen maken van de effectiviteit van het systeem.

Tijd- en faseringsschema

In deze paragraaf zal de planning voor dit onderzoek besproken worden. Hierbij is uitgegaan van een studiebelasting van 18 EC wat neerkomt op ongeveer 12 weken bij een full-time tijdsinvestering.

De activiteiten die per fase worden uitgevoerd zijn als volgt:

Voorbereiding
In deze fase wordt het plan van aanpak afgerond en worden diverse formaliteiten rond het afstuderen geregeld.

Materiaalverzameling;
In deze fase worden de deelvragen beantwoord dit noodzakelijk zijn voor het samenstellen van een ontwerpdocument. De vragen in kwestie zijn de eerste 4 deelvragen genoemd in de vorige paragraaf.

Materiaalanalyse;
In deze fase wordt het ontwerpdocument opgeleverd evenals het prototype voor de testfase.

Test;
In de testfase wordt de laatste deelvraag beantwoordt waarin gekeken werd naar de bruikbaarheid en effectiviteit van het systeem.

Rapportage.
In de rapportagefase worden de verkregen onderzoeksresultaten verwerkt in de scriptie.

De onderstaande strokenplanning geeft de tijdbesteding per deelvraag aan in het tijdsbestek van de genoemde 12 weken, lopend van 6 maart tot en met 5 juni 2006. Week 1 loopt dus van 6 tot en met 13 maart. Indien nodig blijkt zal er per fase een gedetailleerdere planning gemaakt worden.

Week / Fase	1	2	3	4	5	6	7	8	9	10	11	12
Voorbereiding												
Deelonderzoek 1												
Deelonderzoek 2												
Deelonderzoek 3												
Deelonderzoek 4												
Deelonderzoek 5												
Deelonderzoek 6												
Deelonderzoek 7												
Rapportage & presentatie												

Literatuur

Hieronder staat een overzicht van alle artikelen en websites waarnaar verwezen wordt in dit document.

[ASC 2005 1] *Anti Spyware coalition risk model*
http://www.antispywarecoalition.org/documents/riskmodel.htm
Website, Bezocht op 01-12-2005

[ASC 2005 2] *Anti Spyware coalition term definititions*
http://www.antispywarecoalition.org/documents/definitions.htm
Website, Bezocht op 01-12-2005

[Byers 2003] Byers, S
Scalable Exploitation of, and Response to Information Leakage Through Hidden Data in Published Documents
Ongepubliceerd artikel, AT&T Labs research 2003

[Blue Coat 2005] Survey on spyaware en adware by NOP on behalf of Blue Coat
http://www.bluecoat.com/downloads/datasheets/BCS_Spyware_Study.pdf
Website, Bezocht op 01-12-2005

[Borland 2004] Borland, J
News.com: Symantec sued for labeling product adware
Internet nieuwsartikel, News.com, 2004

[Claria] *Claria.com: Advertisers Rates and Information sheet*
http://www.claria.com/advertise/rates/
Website, Bezocht op 01-12-2005

[C|Net] C|net download.com FAQ: How do you test for adware and spyware
http://download.custhelp.com/cgi-in/download.cfg/php/enduser/std_adp.php?p_faqid=339&p_created=1108142543&p_sid=bHCkDaKh&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD00MSZwX3Byb2RzPSZwX2NhdHM9JnBfcHY9JnBfY3Y9JnBfc2VhcmNoX3R5cGU9YW5zd2Vycy5zZWFyY2hfZm5sJnBfcGFnZT0x&p_li=&p_topview=1
Website, Bezocht op 01-12-2005

[Coyle 1999] *Pretty poor privacy*
Karen Coyle
http://www.kcoyle.net/p3p.html
Website, Bezocht op 01-12-2005

[Epic] *Electronic privacy information center*
http://www.Epic.org
Website, Bezocht op 01-12-2005

[gMail 1] *Gmail privacy informatiepagina*
http://gmail.google.com/gmail/help/intl/nl/about_privacy.html
Organization website, Bezocht op 01-12-2005

[gMail 2] *Gmail Testimonials*
http://www.google.com/gmail/help/testimonials_more.html
Organization website, Bezocht op 01-12-2005

[Good 2005] Good,N et al.
Stopping Spyware at the Gate: A user study of Privacy, notice and Spyware
Proceedings of the 2005 symposium on Usable privacy and security: 43-52, 2005

[Jacobsson 2004] Jacobsson, A
Exploring Privacy Risks in Information Networks
Blekinge Institute of Technology, Licentiate series no. 2004:11

[Klang 2004] Klang, M
Spyware, the ethics of covert software
Ethics and Information Technology 6: 193-202, 2004

[Lavasoft] Lavasoft Threat Assesment Chart
http://www.lavasoftresearch.com/tac_main.php
Website, Bezocht op 01-12-2005

[MTL] NIII Master Thesis Lab
http://www.niii.ru.nl/onderwijs/afstudereninfo
Universitaire site, Bezocht op 01-12-2005

[Nu.nl] *Angst voor spyware beïnvloedt internetgedrag*
http://www.nu.nl/news.jsp?n=554530&c=50&rss
nieuwsartikel: Nu.nl 08-08-2005

[Oost 2003] Oost H., Markenhof A.
Een onderzoek voorbereiden
HB Uitgevers Baarn, 2003

[Post Gazette] Jesdanun, A
Post.Gazette nieuws artikel: Coalition hopes "spyware" definitions lead to better control of machines
http://www.post-gazette.com/pg/05193/536418.stm
Website, Bezocht op 01-12-2005

[Privacy] *Privacy.org*
http://www.privacy.org
Website, Bezocht op 01-12-2005

[Privacybird] *Privacyfinder*
http://search.privacybird.com
Website, Bezocht op 01-12-2005

[Sherman 2004] S. Sherman et al.
A generic Anti Spyware Solution
The journal of systems and software 75: 227-234, 2004

[SpywareInfo] *Complaint: Newnet vs Lavasoft*
http://www.spywareinfo.com/downloads/ls/newnet-v-lavasoft.pdf
Website, Bezocht op 01-12-2005

[W3C P3p] *P3P Public overview*
http://www.w3c.org/P3P
Website, Bezocht op 01-12-2005

[Webwereld] Nieuwsartikel: 'Sony-cd's installeren onzichtbare software
http://www.webwereld.nl/articles/38113
Website, Bezocht op 01-12-2005

[WhenU] *WhenU.com: Advertisers contact sheet*
http://app.whenu.com/LeadGen
Website, Bezocht op 01-12-2005