

My secret life as an average person

anonieme gegevensverzamelingen en informationele privacy

door Tijmen Wisman en Tina van der Linden.¹

§ 1. Inleiding

Het gebeurt dagelijks: of iemand nu meedoet aan een prijsvraag of een spel, iets wil bekijken, downloaden of insturen. Steeds vaker is registratie verplicht, moet een account aangemaakt worden of wordt er een klantenkaart uitgegeven. Soms moeten, bij wijze van met een sterretje aangegeven ‘verplichte’ velden, naam en adres (NAW-gegevens) opgegeven worden. Maar vaak ook zijn een zelfgekozen gebruikersnaam en wachtwoord voldoende, die ter verificatie gekoppeld zijn aan een emailadres. Een ‘anoniem’ account dus, want hoewel theoretisch misschien mogelijk, is het praktisch, zeker voor private partijen, ondoenlijk om daarbij NAW-gegevens te achterhalen.²

Ook zonder dat iemand zichzelf ergens voor opgeeft of registreert, worden ieders gangen vastgelegd: door beveiligingscamera’s, door spyware op de computer, door pasjes die nodig zijn om door deuren te komen, door mobiele telefoons. Natuurlijk worden daarbij gegevens over de betrokken persoon verzameld: waar is hij/zij, met wie heeft hij contact, waarin is hij geïnteresseerd, wat koopt hij, hoe betaalt hij, etc. etc. Die gegevens worden opgehangen aan een unieke code, en zo ontstaat een *digitale identiteit*: een setje gegevens die bij een persoon horen, en die middels een unieke code aan die persoon verbonden zijn.

Die gegevens zeggen dus iets over die persoon, en kunnen daarmee waardevol zijn voor bedrijven die hem iets willen aansmeren, voor potentiële werkgevers, voor verstrekkers van uitkeringen en leningen, etc. Ook kunnen ze worden gebruikt om iemand in een bepaald profiel te stoppen, waarbij de impliciete veronderstelling is dat de andere kenmerken die bij zo’n profiel horen, dan ook wel op die persoon van toepassing zullen zijn. Met andere woorden: geautomatiseerde vooroordelen.³

Als de NAW-gegevens ook bij die digitale identiteit opgeslagen worden, is het duidelijk dat het om een geïdentificeerd natuurlijk persoon in de zin van de Wet bescherming persoonsgegevens (hierna: Wbp) gaat, en dus de Wbp van toepassing is. De verwerking van de gegevens moet dan in overeenstemming zijn met de wet, hetgeen onder meer wil zeggen dat ze alleen voor een welbepaald doel verzameld mogen worden etc.

Maar wat als er geen NAW-gegevens bij de digitale identiteit bekend zijn? Is er dan überhaupt sprake van een privacyprobleem? Wat wordt eigenlijk bedoeld met (informationele) privacy?

¹ Tijmen Wisman is adviseur bij ecp.nl; Tina van der Linden is docent IT en Recht aan de Universiteit Utrecht en redacteur van dit blad.

² In theorie zou dit mogelijk zijn via de stappentoets uit Pessers – Lycos, Hoge Raad 25 november 2005 (Pessers/Lycos), LJN [AU4019](#).

³ Dit is precies ook de gevangenis waar Dommering het in zijn afscheidsrede over heeft – zie de boekbespreking elders in dit nummer. Egbert Dommering, *Gevangen in de waarneming*, Otto Cramwinckel Uitgever, 2008.

In dit artikel willen wij de stelling verdedigen dat ook bij anonieme gegevensverzamelingen de privacyregels van toepassing zouden moeten zijn.⁴ Daartoe zullen we eerst, in § 2, het begrip informationele privacy onder de loupe nemen en proberen duidelijk te maken wat we nu onder de noemer van privacy zouden willen beschermen. In § 3 geven we een tweetal voorbeelden waarmee we willen laten zien hoe door anonieme gegevensverzameling de informationele privacy aangetast kan worden. In § 4 leggen we uit hoe naar onze mening de Wbp zo geïnterpreteerd zou kunnen worden dat ook het anoniem verzamelen van gegevens onder het bereik van de wet gebracht kan worden. En we eindigen met een conclusie.

§ 2. Informationele privacy

Informationele privacy is een species van privacy, een notoir glibberig begrip.⁵ Het heeft in ieder geval iets met menselijke waardigheid en met respect te maken. Dat iemand zeggenschap heeft over zijn eigen lichaam, zijn huis, zijn gedachten, zijn contacten met anderen. Waar het bij informationele privacy vooral om gaat, is dat iemand zelf bepaalt wie wat over hem weet; inclusief de mogelijkheid om, al naar gelang de omstandigheden, een heel eenzijdig of onjuist beeld van zichzelf te schetsen.⁶

Beeldvorming is enorm belangrijk voor de manier waarop mensen met elkaar omgaan, denk maar aan uiterlijk en omgangsvormen. Eigenlijk komt dat op hetzelfde neer als bovengenoemde profielen: aan de hand van een paar kenmerken/gegevens ontstaat een beeld van iemand, en op basis van dat beeld wordt iemand op een bepaalde manier behandeld.

Informationele privacy draait erom, dat een mens zelf medeweten heeft van *en* zeggenschap heeft over het beeld dat van hem bestaat in een bepaalde context. Zo wil iemand misschien dat op zijn werk niet bekend is dat hij een of andere rare hobby heeft, omdat mensen dan anders tegen hem aankijken. Dus: dat gegevens die op iemand betrekking hebben, alleen met diens medeweten *en* toestemming verzameld en verwerkt mogen worden. Dommering omschrijft informationele privacy als: “De rechten van het individu om de opslag van informatie, die tot de persoon herleidbaar is, te verhinderen, te beperken of te veranderen.”⁷ De persoon die als eerste informationele privacy heeft gedefinieerd is Alan F. Westin, hij sprak over: “Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”⁸

⁴ Een zelfde punt wordt gemaakt door Steve Gibson in ‘The Ethics of Anonymous Surveillance for Profit’, in: OptOut, Subliminal Persuasion is Against the Law, 2003, <http://www.grc.com/oo/ethics.htm>, waarin hij nogal tekeer gaat tegen het zonder toestemming via internet verzamelen van persoonsgegevens.

⁵ “Privacy is een dynamisch rechtsgoed. Wel aan te duiden nauwelijks te definiëren.” aldus voormalig Minister van Justitie Hirsch Ballin in zijn rede op het vijfde nationaal privacy-symposium, Stc. 17.01.1990, nr. 12.

⁶ Zie Alberdingk Thijm, C., ‘Privacy vs. auteursrecht in een digitale omgeving’, ITeR reeks nr. 49, Den Haag: Sdu Uitgevers 2001, p. 43, die verwijst naar E. Schreuders, ‘Waarden en regels: over privacy en de Wet bescherming persoonsgegevens’ in Privacy & Informatie 1998/1, p. 24.

⁷ E. Dommering e.a., Informatierecht: fundamentele rechten voor de informatiesamenleving, Amsterdam, 2000, p. 50.

⁸ A.F. Westin, Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure and Surveillance, in: Columbia Law Review 1966, p. 7.

§ 3. Voorbeelden

Door de enorm toegenomen technische mogelijkheden is het risico op aantasting van informationele privacy toegenomen, ook bij anonieme gegevensverzamelingen. Twee voorbeelden illustreren deze stelling.

In het eerste voorbeeld speelt gebruik van radio frequency identification (RFID) een cruciale rol. Een zgn. RFID-tag is een chip, die op allerlei producten bevestigd kan worden (of geïntegreerd kan worden in een pas). Het bijzondere is, dat de gegevens op de chip op afstand uitgelezen kunnen worden door een apparaat (lezer of transponder), zonder dat degene die de chip bij zich draagt zich daar bewust van hoeft te zijn: het kan gemakkelijk ongemerkt gebeuren.

Henk de Vries is al jaren klant van een supermarktketen waarvan hij een anonieme klantenkaart heeft, omdat Henk geen kortingen wil mislopen. Oorspronkelijk had Henk een klantenkaart met NAW-gegevens. Toen hij geadresseerde reclame thuis ontving, heeft hij zijn kaart vervangen door een anonieme klantenkaart. De supermarkt waar Henk altijd zijn boodschappen doet, introduceert klantenkaarten met RFID. Hierdoor worden de conventionele klantenkaarten ongeldig. Henk verruilt zijn conventionele klantenkaart voor eentje met RFID, maar blijft anoniem. Op een dag komt Henk de supermarkt ingelopen en het valt hem op dat er meerdere schermen in de winkel zijn geplaatst die filmpjes van aanbiedingen afspelen. Wanneer Henk er voorbij loopt start er een filmpje voor een aanbieding van een merk wijn dat Henk wel eens koopt. "Wat een toeval", denkt Henk en hij schaft een fles aan. Twee weken later gebeurt er precies hetzelfde, alleen ditmaal met 'zoenen' van Buys. Het kind van de moeder die langsloopt zegt duidelijk verstaanbaar tegen zijn moeder: "Die meneer is een snoeperd." Navraag bij de kassa bevestigt zijn vrees: de schermen reageren op de persoonlijke voorkeur van de klant. Die voorkeur blijkt uit zijn profiel, dat is opgeslagen in een achterliggende database. De unieke code van de RFID-tag van de anonieme klantenkaart wordt uitgelezen, het profiel van de klant opgehaald uit de database en op basis daarvan wordt één van de vele aanbiedingsfilmpjes vertoond. Henk tekent bezwaar aan bij de manager. Die zegt dat Henk dan zijn klantenkaart voortaan maar thuis moet laten, omdat de supermarkt dit gewoon mag doen. Henk is en blijft immers anoniem?

Het tweede voorbeeld heeft betrekking op internet. Een zekere Willem heeft seksuele voorkeuren die afwijken van wat algemeen als "normaal" beschouwd wordt. Vroeger kocht hij zijn vieze boekjes in een winkel aan de andere kant van de stad, tegenwoordig kan hij alles wat hij zoekt op internet vinden. Het blijft overigens bij fantasie; hij praktiseert niet. Met één van zijn downloads is spyware meegekomen. Als hij de algemene voorwaarden van die download gelezen had (hetgeen hij uiteraard niet gedaan heeft) dan had hij geweten dat die spyware informatie over zijn surfgedrag verzamelt en doorgeeft aan derden. Uit die informatie wordt zijn afwijkende smaak eenvoudig afgeleid. Op basis daarvan krijgt Willem op zijn scherm niet de reclame van een ziektekostenverzekeraar te zien, die stunt met een goedkope polis. Willem weet uiteraard niet dat hij die reclame niet te zien krijgt - maar hij wordt *wel* feitelijk uitgesloten op basis van een vooroordeel dat gebaseerd is op de door de spyware verzamelde gegevens.

§ 4. Identiteit in de Wbp

Zowel Henk als Willem zijn anoniem én adresseerbaar. Daarnaast is er van hen beiden een profiel voorhanden. In Henks geval ontstaat dit profiel aan de hand van zijn winkelgedrag dat wordt waargenomen door de RFID-lezer in de winkel. Dit profiel is opgeslagen in de achterliggende databank van het RFID-systeem. De code van zijn RFID-tag kan worden uitgelezen en hieraan kan betekenis worden toegekend door middel van de informatie die uit die achterliggende databank kan worden opgevraagd. Een klant uitgerust met een klantenkaart met RFID heeft niet alleen geen geheimen meer voor de supermarkt, maar kan ook individueel aangesproken worden, ook al is hij anoniem.

In Willems geval wordt zijn profiel bepaald aan de hand van zijn surfgedrag. Dit wordt doorgesluist naar databanken van derden door de spyware op zijn computer. Om maar eens een variant op een oud gezegde voor de privacykar te spannen: zeg mij welke internetpagina's je bezoekt en ik zeg wie je bent. En ook Willem kan, zonder dat hij dat noodzakelijkerwijs in de gaten heeft, individueel benaderd worden, terwijl ook hij anoniem is.

De hamvraag is nu, of bovengenoemde gegevensverzamelingen wel of niet onder de bescherming van de Wbp vallen. We nemen een duik in de geschiedenis. De informationele privacy is als grondrecht in de Grondwet verankerd in artikel 10 lid 2 en lid 3. In eerste instantie is aan dit artikel uitvoering gegeven in de Wet persoonsregistraties (WPR). In 1995 zijn de in Europa erkende privacybeginselen vastgelegd in de privacyrichtlijn 1995.⁹ Deze privacyrichtlijn is in Nederland uitgewerkt in de Wbp. De Wbp is tevens de opvolger en vervanger van de WPR.

Een belangrijk verschil tussen beide wetten is de herdefiniëring van het begrip 'persoonsgegeven'. In de WPR luidde de definitie als volgt: "Een gegeven dat *herleidbaar* is tot een individuele natuurlijke persoon." In de Wbp werd deze definitie gewijzigd: "Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon." Volgens de Memorie van Toelichting (hierna MvT) was deze wijziging noodzakelijk, omdat de definitie in de WPR tot misverstanden leidde.¹⁰ Welke misverstanden dit zijn, en hoe die opgelost zouden zijn door de definitie van de Wbp, is vooralsnog onduidelijk.

In de Wbp valt de vraag of er sprake is van een persoonsgegeven, uiteen in twee deelvragen:¹¹

1. Bevatten de gegevens informatie over een natuurlijke persoon?
2. Is deze persoon identificeerbaar?

Voor een positieve beantwoording van de eerste deelvraag zijn er meerdere mogelijkheden. In ieder geval is een vereiste dat de gegevens naar hun aard feitelijke informatie over een persoon geven. Hieronder vallen gegevens die betrekking hebben op handelingen van een persoon, waaronder bijvoorbeeld winkelgedrag en surfgedrag op het internet.

⁹ EU-privacyrichtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

¹⁰ Kamerstukken II 1997-1998, 25 892, nr. 3, p. 46.

¹¹ Handleiding Wet Bescherming Persoonsgegevens, p. 12.

De tweede deelvraag is een stuk complexer. In de MvT luidt het uitgangspunt dat een persoon identificeerbaar is indien zijn identiteit redelijkerwijs, zonder onevenredige inspanning, kan worden vastgesteld.¹² Met behulp van NAW-gegevens (naam, adres en woonplaats) is dit geen probleem. Deze gegevens worden direct-identificerende gegevens genoemd. In bepaalde gevallen kunnen gegevens die ontdaan zijn van een naam in combinatie met andere gegevens toch leiden tot een bepaalde persoon, dit zijn indirect-identificerende gegevens. In de handleiding van de Wbp¹³ luidt de conclusie dat identificeerbaarheid mede wordt bepaald aan de hand van de vraag of de verantwoordelijke feitelijk redelijkerwijs in staat is de 'identiteit' van een persoon vast te stellen.

Bij nadere bestudering van de MvT blijkt echter dat het begrip 'herleidbaar' nog een sluimerend bestaan leidt in het huidige begrippenkader. Op pagina 46 van de MvT staat met zoveel woorden dat de nieuwe definitie van een persoonsgegeven bestaat uit twee elementen. Het gaat om gegevens 'betreffende' een 'identificeerbare' persoon. Vervolgens vermeldt de MvT dat deze twee elementen besloten liggen in de term herleidbaar. Het is op z'n minst vreemd te noemen dat een criterium dat in de praktijk tot misverstanden leidde, wordt vervangen door twee, naar ons idee complexere, elementen en dat deze elementen vervolgens op precies hetzelfde neerkomen. Op pagina 49 van de MvT staat het volgende: "Wat dus bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding." Met deze zin wordt niet alleen bevestigd dat herleidbaarheid het criterium is voor een persoonsgegeven. Daarnaast wordt anonimiteit lijnrecht tegenover het begrip herleidbaarheid geplaatst: iets is anoniem zolang het niet op een persoon herleidbaar is. Op grond hiervan zou je zeggen dat de gegevensverzamelingen uit de voorbeelden niet herleidbaar zijn, omdat ze anoniem geschieden en dus niet onder de Wbp vallen.

Echter, de MvT zegt ook nog iets anders over indirect-identificerende gegevens: "Zij kunnen zijn ontdaan van de naam, doch onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon. Daarnaast zijn er gegevens die zodanig uniek zijn dat zij ook identificerend zijn, zoals het sociaal-fiscaal nummer of unieke biometrische gegevens zoals stem, vingerafdruk of DNA-profiel."¹⁴ Volgens de MvT zelf zijn NAW-gegevens dus geen noodzakelijk vereiste voor een gegeven om te gelden als een persoonsgegeven. En dus zouden bovengenoemde voorbeelden wèl identificeerbaar zijn en onder de Wbp vallen?

Naar de heersende leer vallen de genoemde voorbeelden waarschijnlijk niet onder de bescherming van de Wbp omdat de identiteit van de betrokkenen niet zonder onevenredige inspanning kan worden vastgesteld.¹⁵ Naar ons idee wordt de Wbp hierdoor verkeerd gehanteerd. Anonimiteit hoort niet lijnrecht tegenover herleidbaarheid te worden gesteld. Als er tien mensen in één ruimte staan en één van de tien mensen heeft rood haar, dan kan je een rode haar op de grond herleiden tot die persoon, zonder zijn of

¹² Kamerstukken II 1997-1998, 25 892, nr. 3, p. 47.

¹³ L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Wet bescherming persoonsgegevens, Ministerie van Justitie, Den Haag, april 2002.

¹⁴ Kamerstukken II 1997-1998, 25 892, nr. 3, p. 48.

¹⁵ Kamerstukken II 1997-1998, 25 892, nr. 3, p. 47.

haar naam te weten. Alan F. Westin schaarde anonimiteit onder één van de vormen van privacy en vond dat deze zich voordeed wanneer een individu zich in een openbare ruimte begeeft of in het openbaar handelingen verricht, maar hij tegelijkertijd vrijwaring van identificatie en controle zoekt en deze vrijwaring ook daadwerkelijk vindt. Een interessant standpunt in deze tijd waar verplichte identificatie steeds meer de kop opsteekt, de OV-chipkaart is hier een goed voorbeeld van. Opvallend is trouwens, dat deze onduidelijkheid over de interpretatie van de Wbp (en de problemen waartoe dit onzes inziens in de praktijk leidt) in het geheel niet aan de orde is geweest in de recente evaluatie van de Wbp.¹⁶

Het gaat er maar om, wat je in dit kader onder ‘identiteit’ verstaat. Wanneer weet je ‘wie’ iemand is? Voor de supermarkt in het voorbeeld van Henk is het niet relevant om Henks NAW-gegevens te hebben: ze gaan niet bij hem op bezoek en sturen hem ook geen geadresseerde reclame.

Naar ons idee is het van belang dat je de relevante gegevens gerelateerd aan die persoon kunt opslaan, dat je iemand als uniek individu binnen een groep kunt aanwijzen. Want dan kan een beeld gevormd worden over die persoon, een profiel aan hem gekoppeld worden, en kan hij op basis van zijn eigen gegevens of op basis van het profiel op een bepaalde manier behandeld worden. En dan ontstaat er (potentieel) een privacyprobleem, als de betrokkene geen weet van of invloed op de gegevens heeft die over hem zijn opgeslagen.

Dat privacyprobleem komt aan de oppervlakte zodra iemand ook adresseerbaar is: als je op de een of andere manier met hem kunt communiceren. Dat kan door het filmscherm in de supermarkt, door pop-ups en banners op het internet, door sms-jes naar een mobiele telefoon, etc. NAW-gegevens zijn voor adresseerbaarheid in het digitale tijdperk overbodig geworden.

Die adresseerbaarheid kan meteen aanwezig zijn bij het aanleggen van de gegevensverzamelingen (zoals bij het aanmaken van een account bij een site waar je een emailadres voor moet opgeven), maar kan ook later, als het ware met terugwerkende kracht, gecreëerd worden, bijvoorbeeld door koppeling van gegevens. Terstege gebruikte hiervoor, in het vorige nummer van dit tijdschrift, de term ‘voorwaardelijke persoonsgegevens’: men weet niet of en zo ja wanneer dergelijke gegevens in een identiteitsrelevante context worden geplaatst.¹⁷ Daarom zou adresseerbaarheid geen vereiste moeten zijn van identificeerbaarheid. Het creëren van individuele profielen op zich zou al moeten worden gezien als het verzamelen van persoonsgegevens. Het is immers nooit zeker of iemand ooit wordt aangesproken op zijn of haar profiel. Met het oog op de snelheid waarmee technologie zich ontwikkelt, is in ieder geval zeker dat deze onzekerheid er in de toekomst niet minder op zal worden.

§ 5. Conclusie

¹⁶ Zwenne, Gerrit-Jan; Duthler, Anne-Wil; Groothuis, Marga; Kielman, Hugo; Koelewijn, Wouter en Mommers, Laurens, ‘Eerste fase evaluatie Wet bescherming persoonsgegevens, Literatuuronderzoek en knelpuntenanalyse’, WODC, december 2007, online beschikbaar op http://www.wodc.nl/images/1382a_vollledige_tekst_tcm44-61969.pdf.

¹⁷ J. Terstege, Is het privacyrecht klaar voor de toekomst? in: Tijdschrift voor Internetrecht, jaargang 1 nummer 3, p. 65.

Om de informationele privacy van een ieder te beschermen is het van belang dat de Wbp niet al te benepen geïnterpreteerd wordt. Het begrip 'identiteit' omvat anno 2008 ook onze vele digitale identiteiten. Persoonsgegevens mogen, ook als er geen NAW-gegevens bij zitten of die gemakkelijk te achterhalen zijn, niet zonder medeweten en toestemming van de betrokkene worden verzameld en verwerkt. Ook aan de hand van digitale identiteiten is beeldvorming mogelijk, en de kern van het aspect van menselijke waardigheid dat aangeduid wordt met de term informationele privacy is dat een ieder zelf mag bepalen wie wat over hem weet.

Literatuur

- Alberdingk Thijm, C., 'Privacy vs. auteursrecht in een digitale omgeving', ITeR reeks nr. 49, Den Haag: Sdu Uitgevers 2001.
- Clarke, R., 'The digital persona and its application to data surveillance', The Information Society, vol. 10, issue 2, June 1994.
- Dommering E., e.a, Informatierecht: fundamentele rechten voor de informatiesamenleving, Amsterdam 2000.
- Dommering, E., Gevangen in de waarneming, Hoe de burger de communicatiemiddelen overnam en zelf ook de bewaking ging verzorgen, Amsterdam: Otto Cramwinckel Uitgever, 2008.
- Gibson, S., 'The Ethics of Anonymous Surveillance for Profit', in: OptOut, Subliminal Persuasion is Against the Law, 2003, <http://www.grc.com/oo/ethics.htm>.
- Holvast, J., 'Persoonsgegevens of niet: dat is de vraag', in: ITeR reeks nr. 2, Alphen aan den Rijn: Samsom BedrijfsInformatie 1996.
- Holvast, J., 'Wet bescherming persoonsgegevens: privacywet of een wet die gegevens beschermt?', Privacy & Informatie, 2005, 6.
- Hooghiemstra, T.F.M., 'Wet bescherming persoonsgegevens, Tekst en toelichting', Den Haag, 2003.
- Huydecoper, S., 'Wet bescherming persoonsgegevens en ICT', Den Haag, 2006
- Kuitenbrouwer, F., Het recht om met rust te worden gelaten, Amsterdam 1991.
- Prins, J.E.J., en Vries, M. de, ID or not to be? Naar een doordacht stelsel voor digitale identificatie, 's-Gravenhage 2003.
- Schermer, B. en Durinck, M., Privacyrechtelijke aspecten van RFID, ECP.NL, 2005.
- L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Wet bescherming persoonsgegevens, Ministerie van Justitie, Den Haag, april 2002.
- Terstegge, J., Is het privacyrecht klaar voor de toekomst?, Tijdschrift voor Internetrecht, jaargang 1 nummer 3, juli 2008, pp. 64-65.
- Warren S. en Brandeis L.D., 'The Right to Privacy', Harvard Law Review, 1891, 5, online beschikbaar op http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html.
- Westin, A.F. 'Science, Privacy and Freedom: Issues and Proposals for the 1970's. Part II, Balancing the Conflicting demands of Privacy, Disclosure and Surveillance', in: Columbia Law Review, 1966

- Winkelhorst, R.C., Elektronische communicatie en privacy, Zutphen: Paris 2006.
- Wisman, Tijmen, De RFID-golf in de detailhandel, Worden wij verplicht mee te surfen in het internet van dingen? Doctoraalscriptie Nederlands Recht, Universiteit Utrecht, juli 2007, online beschikbaar op <http://www.uu.nl/uupublish/content-cln/RFID-golf.pdf>.
- Zwenne, G.J en Schermer, B., Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen, 's-Gravenhage, 2005.
- Zwenne, Gerrit-Jan; Duthler, Anne-Wil; Groothuis, Marga; Kielman, Hugo; Koelewijn, Wouter en Mommers, Laurens, 'Eerste fase evaluatie Wet bescherming persoonsgegevens, Literatuuronderzoek en knelpuntenanalyse', WODC, december 2007, online beschikbaar op http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969.pdf.