Privacy: code in context

Jaap-Henk Hoepman, Bart Jacobs[1]

Privacy: het belang van context en de invloed van code

'Je hebt toch niets te verbergen?' Deze retorische vraag wordt vaak gebruikt om een pleidooi voor de bescherming van de privacy te ontkrachten. Maar in feite volstaat een eenvoudig 'Ja zeker wel, en jij trouwens ook!' als antwoord.

~

Privacy is een lastig te definiëren begrip (Solove 2010). Dat blijkt ook wel uit de andere bijdragen in dit jaarboek, waarin verschillende auteurs privacy ieder vanuit hun eigen perspectief behandelen. Wij zullen in dit hoofdstuk privacy vanuit een technologisch perspectief benaderen. Nieuwe toepassingen van ICT zetten privacy onder druk. We zullen echter laten zien hoe een verantwoord gebruik van technologie ook kan leiden tot een verbetering van onze privacy, juist doordat deze technologie het mogelijk maakt contexten te scheiden en privacybescherming te zien als meer dan alleen het beschermen van de confidentialiteit.

Het belang van context

Terug naar de retorische vraag 'je hebt toch niets te verbergen?' Waarom volstaat zo'n simpel antwoord "jawel, en jij ook"? Of eigenlijk: waarom is de oorspronkelijke vraag fout?
De vraag impliceert dat privacy de schuilplaats van het kwaad[2]is, dat alleen slechte bedoelingen hoeven worden afgeschermd, en dat alle andere informatie over jouzelf per definitie onschadelijk is en dus niet verborgen hoeft te worden. Niets is minder waar. Alleen schaamteloze exhibitionisten hebben niets te verbergen. Normale stervelingen houden verschillende levenssferen graag gescheiden. Dat je je partner toevertrouwt dat je een slechte dag op het werk had hoeft niet meteen op de intranetpagina's van het kantoor te staan. Mensen opereren in verschillende sociale contexten, waarbinnen ze verschillende rollen hebben en zich dus ook verschillend opstellen (Nissenbaum 2009). Die mate waarin die contexten gescheiden zijn moet door ieder individu zelf bepaald kunnen worden. Sterker nog, openheid over persoonlijke details van het eigen leven zijn in gezelschap vaak ongemakkelijk en zelfs onbeschaafd. Niet alles van een ander weten vergemakkelijkt het sociale contact.

De vraag gaat er ook ten onrechte vanuit dat privacy alleen een persoonlijk belang is, dat ondergeschikt is aan een groter maatschappelijk belang. De bescherming van de persoonlijke levenssfeer is niet alleen een individueel belang, maar ook een algemeen maatschappelijk belang. Als individuen niet de mogelijkheid hebben om in beslotenheid relaties en verbanden aan te gaan, een mening te vormen en die te herzien, te discussiëren en kritiek te uiten, informatie over zichzelf selectief te delen met anderen, zich te ontwikkelen of te veranderen, dan kan een democratische maatschappij als de onze zich niet verder ontwikkelen. Agre en Rothenberg (2001) definiëren privacy daarom ook als 'freedom from constraints on the construction of one's own identity'. Ten slotte is het van belang te benadrukken dat privacy niet hetzelfde is als confidentialiteit (vertrouwelijkheid).

Persoonlijke informatie mag in bepaalde gevallen best door anderen verzameld worden, als dat maar met een bepaald welomschreven doel gebeurd, en als deze informatie niet zomaar zonder toestemming voor doeleinden gebruikt wordt, of zelfs aan anderen wordt doorgegeven.

Code: de invloed van technologie

Technologische ontwikkelingen hebben altijd een invloed gehad op de privacy in de samenleving. Aan het eind van de 19e eeuw bijvoorbeeld baarde de opkomst van de fotografie en de verspreiding van kranten en (roddel)bladen grote zorgen (Warren en Brandeis 1890). In die tijd bleef de invloed van deze ontwikkelingen op de privacy misschien nog beperkt tot een kleinere groep '*celebrities*'. Er is echter een tweetal ontwikkelingen uit de 20e eeuw aan te wijzen dat een niet te onderschatten invloed heeft gehad op de privacy van eigenlijk alle burgers.

De eerste grote verandering ontstond door de opkomst van de computer, vanaf de jaren '60 van de vorige eeuw. Hierdoor kon informatie voor het eerst op grote schaal digitaal opgeslagen en verwerkt worden. Dat had twee grote voordelen. Ten eerste kon informatie nu makkelijk gedupliceerd worden. Hierdoor raakten dossiers minder vaak zoek. Ten tweede kon informatie veel sneller doorzocht worden, en was er ook een grotere garantie dat áls er informatie over een persoon bestond, die ook inderdaad gevonden zou worden.

De tweede grote verandering ontstond door de opkomst van netwerken, en dan met name het Internet, vanaf de jaren 90. Hierdoor kon informatie eenvoudig over de hele wereld gedeeld en geraadpleegd worden. Dit maakte het makkelijk om gegevens uit verschillende databases aan elkaar te koppelen. Bovendien was deze data in principe voor iedereen, technisch gezien, toegankelijk. Dit had tevens tot gevolg dat als een stuk gevoelige informatie openbaar werd, denk aan een sappige roddel of een onthullende foto van een bekende of minder bekende persoon, het binnen de kortste keren op allerlei servers op het Internet terug te vinden was. Dit zogenaamde '*netwerk effect*' maakt het ook een stuk lastiger om systemen (en de daarop opgeslagen informatie) goed te beschermen.

Beide ontwikkelingen zoals hierboven geschetst hebben er voor gezorgd dat informatie alomtegenwoordig is, praktisch onvergankelijk is (Buruma 2011), en eenvoudig te doorzoeken en te combineren is. Dit heeft natuurlijk gevolgen voor onze informationele privacy. Dat is grof gezegd het recht om te bepalen welke informatie over onszelf door anderen verzameld wordt en hoe deze informatie vervolgens gebruikt wordt. In dit hoofdstuk zullen we ons daarom ook richten op het beschermen en uitoefenen van controle op de informatie over jezelf. Dit aspect van privacy wordt ook wel dataprotectie genoemd.

Leeswijzer: code in context

Technologie kan echter ook ingezet worden om onze privacy te beschermen. In dit hoofdstuk wordt daarop nader ingegaan. We zullen een aantal basisprincipes bespreken voor het ontwerpen van privacyvriendelijke informatie verwerkende systemen. Daarna beschrijven we een aantal

kenmerkende *privacy enhancing technologieën* (PET's), en gaan daarna in op een aantal beperkingen daarvan. Nieuwe ontwikkelingen rondom veiligheid aan de ene kant en privacy en identiteitsbeheer aan de andere kunnen hierop deels een antwoord bieden. We laten in dit hoofdstuk bewust fundamenteel andere benaderingen van privacybescherming, zoals benaderingen die gebaseerd zijn op het vergroten van de transparantie, buiten beschouwing. Die komen in andere hoofdstukken in dit boek afdoende aan bod. Dit artikel legt de nadruk op techniek en niet op voor en nadelen van het gebruik van PET's; zie daarvoor andere, uitgebreide, studies.[3]

Wat maakt een systeem privacyvriendelijk?

Voordat we in kunnen gaan op de mogelijke technieken die gebruikt kunnen worden om privacy te beschermen, moeten we eerst wat nader preciseren wat privacy in technische zin betekent. Hierbij beperken we ons tot informationele privacy, dus tot de controle op het gebruik van persoonlijke gegevens door anderen (verzamelen, verwerken, verspreiden et cetera). Persoonlijke gegevens zijn gegevens die herleidbaar zijn tot een natuurlijk persoon. Bij privacybescherming kan men ruwweg een onderscheid maken tussen:

A priori bescherming, die sterk gericht is het voorkomen van een link tussen persoon en gegeven. Immers, zonder persoonlijke gegevens is er ook geen sprake van een inbreuk op de informationele privacy.

A posteriori bescherming, die gericht is op hoe eenmaal verzamelde persoonsgegevens daadwerkelijk gebruikt worden.

De nadruk in deze tekst ligt op technieken voor *a* priori bescherming. Daarom zal de link tussen persoon en gegeven nader bestudeerd worden, zoals is gedaan door (Hansen en Pfitzmann). Zij onderscheiden de volgende eigenschappen.

Anonimiteit: Een entiteit is anoniem als deze niet te onderscheiden is van andere entiteiten in een bepaalde verzameling. Als deze verzameling *k* elementen bevat spreekt men wel van *k*-anonimiteit. K-anonimiteit formaliseert het intuïtieve idee dat je je kunt verbergen in een groep van k personen. In een groep van 2 is dat lastig, maar in een groep van 100 of 1000 val je minder op.

Onlinkbaarheid garandeert dat twee entiteiten of gebeurtenissen (bijvoorbeeld het versturen van een e-mailbericht, of het bezoeken van een bepaalde website) niet met elkaar in verband kunnen worden gebracht.

Onobserveerbaarheid betekent dat het onmogelijk is te bepalen of een bepaalde gebeurtenis al dan niet heeft plaatsgevonden.

Merk op dat door deze *a* priori focus op het voorkomen van een link tussen gegeven en persoon er beduidend minder aandacht is voor *a posteriori* beschermingsmaatregelen tegen het verspreiden en gebruiken van persoonlijke gegevens, of tools om gebruikers inzage en controle over hun gegevens te geven. Daarover verderop meer.

Wel is er een meer algemeen aanvaard principe van *privacy by design* (Cavoukian 2009). Hierbij wordt niet alleen gekeken naar technische beschermingsmaatregelen, maar ook naar

organisatorische en procesmatige maatregelen. Bovendien wordt de bescherming van persoonsgegevens hier integraal, over de hele keten, beschouwd. Hierbij is het noodzakelijk om vooraf een zogenaamde *privacy impact assessment* (PIA) uit te voeren om te bepalen welke privacyrisico's kunnen ontstaan door het gebruik van het te ontwikkelen systeem. Zo wordt bij het ontwerpen volgens *privacy by design* direct invulling gegeven aan de wettelijke bepalingen zoals die in Nederland in de Wet bescherming persoonsgegevens (Wbp) staan. Voorbeelden zijn het expliciet maken van het doel van de informatieverwerking, het bepalen of de verwerking proportioneel is, er voor zorgen dat de verzamelde gegevens afdoende beveiligd zijn, en nagaan of aan de mogelijkheid tot inzage en correctie is voldaan.

Een aantal ontwerpprincipes (*privacy design patterns*) kunnen helpen bij het ontwerp van een privacyvriendelijk systeem (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2004). Het is daarbij wel van belang dat deze principes vanaf het begin van het ontwerp van het systeem worden meegenomen. Net als security is privacy geen eigenschap die je later nog aan een systeem kunt toevoegen. Het meest bekend zijn de volgende principes.

Select before you collect. Dit principe staat ook wel bekend als het dataminimalisatie principe. Volgens dit principe mag je niet eerst alle mogelijke informatie verzamelen om vervolgens te kijken welke informatie je echt nodig hebt. In plaats daarvan moet je meteen beoordelen of je een bepaald data item nodig hebt, en mag je het alleen verzamelen en verder verwerken als dit inderdaad zo is (Jacobs 2005). Dit kunnen we het beste toelichten aan de hand van een voorbeeld. Stel je wilt weten of voertuigen van bekende criminelen de grens passeren. Je kunt hiervoor een zogenaamd ANPR-systeem (*Automatic Number Plate Recognition*) op de grensovergang zetten en het kenteken van alle passerende voertuigen doorsturen en opslaan. Het *select before you collect* principe vereist dat het ANPR-systeem zelf voorzien wordt van de lijst van kentekens waar je naar op zoek bent, en alleen de nummers die op de lijst voorkomen doorgeeft aan achterliggende systemen (en personen).

Context scheiden. Dit principe vereist dat gegevens over een persoon uit de ene context niet gebruikt worden in een andere context, of gecombineerd worden met gegevens over deze persoon uit een andere context. Informatiestromen uit verschillende contexten moeten dus gescheiden gehouden worden. Dit principe onderkent dat een persoon niet één vaste identiteit heeft, maar verschillende identiteiten kan hebben die in verschillende contexten naar voren komen. Mensen hebben verschillende rollen en verantwoordelijkheden in verschillende contexten, en zullen zich daarom in de ene context anders gedragen dan in de andere context. Informatie over een persoon in de ene context is irrelevant of misschien zelfs schadelijk in een andere context. Daarom mogen medische gegevens niet zomaar binnen de context van iemands werk gebruikt worden. Datzelfde geldt voor iemands financiële omstandigheden (inkomen, schulden, uitgavenpatroon).

Anonimiseren. Dit principe gaat nog een stap verder en vereist dat alle gegevens die er voor zorgen dat de informatie tot een persoon herleidbaar is wordt verwijderd. In feite zorgt het ervoor dat de informatie niet langer persoonlijke informatie is.

We zullen nu bespreken hoe enkele basistechnieken gebruikt kunnen worden om bovenstaande eigenschappen en design te implementeren.

Privacy Enhancing Technologies

Er is de afgelopen decennia veel onderzoek verricht naar zogenaamde *Privacy Enhancing Technologies* (PET's). Dit onderzoek heeft bouwstenen opgeleverd die veelal gebaseerd zijn op cryptografie (met name het versleutelen en weer ontsleutelen van gevoelige informatie).

Pseudoniemen. Een eenvoudige techniek is het gebruik van *pseudoniemen*. In plaats van bijvoorbeeld in elk bestand het Burger Service Nummer (BSN) van iemand op te slaan, kan ook gebruikt gemaakt worden van een uniek sector specifiek nummer dat van het BSN is afgeleid. Dit sector specifieke nummer is dan een pseudoniem. Belangrijk is dat het onderliggende BSN niet af te leiden is uit het pseudoniem, en dat van twee pseudoniemen niet te bepalen is of ze tot dezelfde persoon behoren. Dit betekent dat er restricties zijn op de manier waarop een pseudoniem van het BSN wordt afgeleid. In de cryptografie worden hiervoor zogenaamde *hashfuncties* gebruikt. Dit zijn functies *h* die gemakkelijk uitgerekend kunnen worden (gegeven *x* is *h(x)* eenvoudig uit te rekenen), maar die moeilijk te inverteren zijn (gegeven *h(x)* kun je niet zomaar *x* achterhalen).

Zulke pseudoniemen kunnen gebruikt worden om contexten van elkaar te scheiden, en om te voorkomen dat databases uit verschillende contexten met elkaar gekoppeld kunnen worden. Een dergelijke koppeling kan onmogelijk gemaakt worden door voor elk van de databases voor dezelfde persoon verschillende pseudoniemen te gebruiken die niet tot elkaar herleidbaar zijn. Als een persoon in de ene context bekend is onder een pseudoniem dat niet gekoppeld kan worden aan het pseudoniem van dezelfde persoon in een andere context, dan zijn beide contexten effectief gescheiden van elkaar.

Anonieme credentials. Vaak is het noodzakelijk om aan te kunnen tonen dat je een bepaalde eigenschap hebt (dat je ouder bent dan 18 jaar bijvoorbeeld, of dat je een abonnement hebt op een digitale krant). Zo'n eigenschap heet ook wel een *credential*. Soms is het gewenst om dit op een privacyvriendelijke manier te doen, zodat het gebruik van een credential anoniem. In deze context betekent dat dat de krant niet kan zien wie gebruik maakt van zijn abonnement, of dat de slijterij niet kan zien wie een fles sterke drank koopt.

Anonieme credentials zijn bedacht door David Chaim (Chaum, 1985). Een credential is niets anders dan een certificaat, waarin staat dat de houder een bepaalde eigenschap heeft, die is ondertekend door de uitgever. Om een credential aan te vragen moet je jezelf identificeren aan de uitgevende

instantie. Deze moet immers controleren of jij inderdaad de gevraagde eigenschap bezit (bijvoorbeeld dat je ouder bent dan 18). Aan de andere kant moet jouw identiteit later niet te koppelen zijn bij het gebruik van de credential. Het is dus van belang om de *uitgifte* van een credential en het *gebruik* van een credential van elkaar te scheiden. Technisch gesproken realiseert Chaum dit door gebruik te maken van zogenaamde *blind signatures*. Cruciaal bij een blind signature is dat de ondertekenaar niet ziet wat hij ondertekent: hij tekent het certificaat zogezegd met gesloten ogen. Dat kan in de niet-digitale wereld bijvoorbeeld als iemand je een brief voorhoudt met daarop een carbonpapiertje en vraagt onderaan te tekenen. Normaal gesproken doe je zoiets niet, maar in digitale wereld kan het wel handig zijn, zeker als je verschillende handtekeningen gebruikt voor verschillende doeleinden. Bij anonieme credentials zorgen blind signatures ervoor dat het unieke nummer in het certificaat niet bekend is bij de uitgever. De sleutel die de uitgever gebruikt voor ondertekening bepaalt de 'waarde' van het certificaat: dwz. of het certificaat aangeeft dat de houder ouder is dan 18, dan wel een geldig abonnement heeft. Het certificaat zelf is verder inhoudsloos. Zelfs meer formele zaken als geldigheidsduur en betrouwbaarheidsniveau kunnen gekoppeld worden aan de gebruikte sleutel voor ondertekening.

Onlinkbare credentials. Een sterkere garantie wordt gegeven door *onlinkbare* credentials. Onlinkbaar betekent in deze context dat de krant niet kan zien wanneer en hoe vaak iemand gebruik maakt van zijn abonnement, of dat de slijterij niet kan zien hoe vaak iemand een fles sterke drank koopt. Een onlinkbare credential kan gemaakt worden door gebruik te maken van zogenaamde *zero knowledge* technieken (Quisquater et.al. 1990). Een zero knowledge protocol stelt iemand in staat om te bewijzen dat hij een bepaald credential bezit, zonder dat hij informatie over dit credential aan anderen prijsgeeft. In het bijzonder onthult hij hiermee niet dat hij bezit van hetzelfde credential al eens eerder heeft aangetoond. Ook kan de andere partij (die ik ooit mijn credential op deze wijze heb "getoond") niet een andere partij er van overtuigen dat ik het credential bezit.

Secure multiparty computation. Een andere benadering is die van de *secure multiparty computations* (MPC) (Yao 1982). Stel een aantal partijen wil gezamenlijk het resultaat van een functie uitrekenen over de afzonderlijke inputs, zonder deze inputs aan de andere partijen te openbaren. Twee miljonairs willen bijvoorbeeld van elkaar weten wie het rijkst is, zonder aan elkaar te verklappen hoe rijk ze precies zijn. Dit zou je kunnen doen door gebruik te maken van een Trusted Third Party (TTP), waar ieder zijn input naar toe stuurt, en die vervolgens het resultaat over de waarden berekent en aan iedereen terug geeft. Nadeel is alleen dat de TTP volledig vertrouwd moet worden… In een secure multiparty computation (MPC) wordt de functionaliteit van de TTP (namelijk het uitrekenen van de functie) over alle deelnemers verspreid, op een dusdanige manier dat geen van de deelnemers meer leert over de inputs van de andere deelnemers dan in de zogenaamde *ideale* situatie (waarin de TTP al het werk doet). Je zou het bepalen van de uitslag van verkiezingen ook als een vorm van MPC kunnen zien, waarbij iedereen zijn geheime stem aanlevert en het eindresultaat op betrouwbare wijze bepaald wordt zonder de persoonlijke inputs te onthullen. Onderzoek heeft aangetoond dat voor allerlei functies een MPC-protocol te vinden is (veelal automatisch), met als nadeel dat deze

protocollen vooralsnog vrij veel rekenkracht, tijd en communicatie vergen, en daardoor bijvoorbeeld moeilijker op een chipkaart geïmplementeerd kunnen worden.

Mixing. Door gebruik te maken van cryptografie is de inhoud van boodschappen te verbergen voor derden. Maar vaak zijn de afzender of de ontvanger eenvoudig te achterhalen uit het bericht zelf (denk aan de onversleutelde headers in versleutelde e-mailberichten) of door te kijken naar pakketten waarmee het bericht via Internet wordt verstuurd. Een credential kan nog zo anoniem zijn, als je een website bezoekt vanaf je eigen pc dan is je identiteit eenvoudig te achterhalen via het IP-adres van die pc. Het observeren van netwerkverkeer om de afzenders of ontvangers van berichten te achterhalen heet *traffic analysis*. Dit is een krachtig opsporingsmiddel, dat door opsporingsinstanties ook wordt ingezet bij (mobiele) telefonie om snel criminele netwerken te achterhalen. Om traffic analysis tegen te gaan moet de directe relatie tussen afzender en ontvanger van een bericht dat zich door het netwerk verplaatst verbroken worden. Hiervoor wordt gebruik gemaakt van zogenaamde *mixing* technieken (Chaum 1981). Hierbij worden berichten niet direct van zender naar ontvanger gestuurd, maar via een aantal speciale routers (mixers) gestuurd, die een aantal van zulke berichten een korte tijd vasthouden en daarna in willekeurige volgorde (en met andere sleutels versleuteld) doorsturen. Zo is het verband tussen inkomende en uitgaande berichten verstoord, en is het veel moeilijker geworden om een bericht over het Internet op zijn pad van afzender naar ontvanger te volgen. Een bekend en praktisch bruikbaar mix-netwerk is het Tor-netwerk[4], dat berichten op internet bewust omleidt om de herkomst te maskeren.

De beperkingen van de huidige stand der techniek

Ondanks dat er de afgelopen decennia veel onderzoek is gedaan naar *privacy enhancing* technologieën, staat onze privacy in toenemende mate onder druk. Dit heeft een aantal oorzaken. Ten eerste is onze samenleving risicomijdend geworden. Er is een toenemende wens naar een welhaast absolute vorm van veiligheid. Pech wordt niet meer getolereerd. Hierbij worden privacy en security als tegenpolen gezien, met als gevolg dat in het huidige maatschappelijke klimaat verscherpte veiligheidsmaatregelen genomen worden die ten koste gaan van onze privacy. Ten tweede is onze samenleving meer en meer een informatiemaatschappij geworden. Informatie, ook persoonlijk informatie, is eenvoudig te bewaren, te kopiëren en te verspreiden. We doen daar zelf ook naar hartenlust aan mee door gebruik te maken van sociale netwerken zoals Facebook, Hyves en Twitter. Dat is ook niet zo vreemd, omdat het gebruik daarvan voor ieder van ons ook grote voordelen oplevert. Maar niet iedereen is zich bewust van de privacyrisico's. Bedrijven als Google en Facebook rekken de grenzen van de privacy bewust op omdat zij verdienen aan het delen van zoveel mogelijk informatie. Zo bepalen zij hoe onze privacy er in de toekomst uit gaat zien.
Ten derde zijn PET's met name gericht tegen het *verzamelen* van persoonlijke informatie, en veel minder op het voorkomen van *misbruik* van dergelijke informatie nadat deze is verzameld. Dit is een gemis omdat veel mensen eenvoudig persoonlijke informatie weggeven door gebruik te maken van sociale netwerken, of van allerlei bonuskaarten. Soms word je er ook toe gedwongen, bijvoorbeeld als je met het openbaar vervoer wilt reizen en gebruik moet maken van de OV-chipkaart die

vervoersgegevens jarenlang bewaart. Daarnaast vindt veel informatievergaring haast onmerkbaar plaats, door camera's en andere sensoren en door de opbouw van grote `log' bestanden (soms verplicht, zoals bij dataretentie). Ten vierde staat bij veel van de ontwikkelde technieken de gebruiker aan de zijlijn. Hij heeft geen invloed op het proces, en kan ook niet nagaan of en hoe zijn persoonlijke gegevens worden beschermd. Ten slotte worden bestaande PET's maar mondjesmaat gebruikt. Dat kan deels verklaard worden door onwetendheid over de mogelijkheden van de techniek, en de specialistische kennis die nodig is om de bestaande technieken op de juiste wijze toe te passen. Maar een belangrijke oorzaak is simpelweg dat er voor bedrijven geen directe voordelen te behalen zijn bij het toepassen van PET's, maar dat ze wel geld kosten om in te voeren en te onderhouden. Anders gezegd: de business case voor privacy ontbreekt. Dat kan alleen doorbroken worden door aan bedrijven een wettelijke verplichting op te leggen om PET's toe te passen.

Nieuwe privacybeschermende technieken

Een aantal van de bovengenoemde beperkingen ten aanzien van de toepassing van privacy enhancing technologieën kan worden weggenomen door radicaal andere benaderingen. Een tweetal hiervan zal hieronder worden besproken.

Revocable privacy

Veiligheid en privacy worden ten onrechte als elkaars tegenpolen gezien. Hierdoor gaan oplossingen voor (maatschappelijke) veiligheid ten onrechte ten koste van de privacy. En wordt bij de ontwikkeling van privacybeschermende technologieën te weinig rekening gehouden met redelijke veiligheidswensen. Het *revocable privacy* concept probeert deze kloof te overbruggen (Hoepman 2008). De crux is om zowel de security als de privacy leidend te laten zijn in de architectuur van een systeem (voor rekeningrijden, voor paspoortcontrole, voor identiteitsbeheer, noem maar op). De achterliggende gedachte is dat "architectuur = politiek". De architectuur van een systeem bepaalt niet alleen hoe een systeem op dit moment functioneert, maar ook hoe het zich in de toekomst kan ontwikkelen. Een architectuur schept mogelijkheden, maar kadert ook in. Het is in zeker zin een abstracte filosofie over hoe de wereld (in ieder geval de wereld waar het systeem in opereert) in elkaar zit. Niet alleen in prescriptieve zin, maar zeker ook in normatieve zin. De architectuur van een systeem is dus een politieke keuze. Deze moet dus op basis van politieke argumenten bepaald worden. De consequenties van de architectuur moeten bij het nemen van de beslissing dan wel bekend en onderkend worden.

Architectuur is in die zin vergelijkbaar met wetgeving. Niet voor niets noemde Lawrence Lessig het boek waarin hij deze ideeën uitwerkte "*Code, and other laws of cyberspace*" (Lessig 1999). Code staat hier voor architectuur. Er is echter een cruciaal verschil tussen architectuur aan de ene kant en wetgeving aan de andere kant. Wetgeving is aan verandering onderhevig. In extreme gevallen kunnen wetten zomaar veranderen. Voor architectuur geldt dit niet. Die is min of meer onveranderbaar. De architectuur is de kern van het hele systeem, en kan dus alleen veranderd worden door het systeem volledig te vervangen door een nieuw systeem. Een systeem implementeert

revocable privacy als de architectuur van het systeem garandeert dat gegevens over individuen slechts dan beschikbaar komen als aan een aantal vooraf gedefinieerde voorwaarden is voldaan. Zolang de gebruikers van het systeem zich aan de regels houden, dan is hun privacy gegarandeerd. Als je het revocable privacy principe toepast op bijvoorbeeld rekeningrijden, dan is gegarandeerd dat de overheid niet weet waar je gereden hebt, tenzij jij je rekening niet betaald hebt.

Er zijn twee mogelijke varianten om revocable privacy te realiseren. In de eerste variant wordt toegang tot de gegevens bewaakt door een onafhankelijke derde partij, de zogenaamde Trusted Third Party. Deze controleert of aan de voorwaarden voor opheffen van de privacy is voldaan. Deze controle is in een vooraf opgestelde procedure vastgelegd. Het moge duidelijk zijn dat hierbij wel vertrouwd wordt op de integriteit van deze derde partij. Ook mogen er geen situaties ontstaan waardoor de procedures of de voorwaarden later veranderd worden. Dit is echter moeilijk te garanderen. Wet- en regelgeving zijn immers altijd aan verandering onderhevig. In de tweede, zogenaamde self-enforcing, variant is het systeem zo ingericht dat persoonsgegevens alleen vrij kunnen komen als aan de voorwaarden voor vrijkomen voldaan is. Het is dus een technische beperking (vergelijkbaar met een auto die voorzien is van een snelheidsbegrenzer), en niet een procedurele. Het heeft dus niet de nadelen van de eerste variant. Echter, self-enforcing systemen blijken lastig te maken te zijn. Één voorbeeld is welbekend: het voorkomen dat digitaal geld tweemaal uitgeven wordt (het zogenaamde "double spending"). Welke variant er ook gekozen wordt, de harde eis is dat geen van de partijen eigenhandig persoonlijke gegevens uit het systeem kan halen. Daar is altijd medewerking van een andere partij voor nodig (in het geval van self-enforcement door het feit dat de gebruiker de regels overtreedt). Het ontwikkelen van systemen voor revocable privacy is een actief onderzoeksgebied.

Identiteitsbeheer

Sterk gerelateerd aan het begrip privacy is het technische concept van identiteitsbeheer (*identity management*, IDM). Identity management is ontstaan uit de wens om het voor gebruikers van allerlei verschillende computersystemen en websites makkelijker te maken om zich aan te melden. In plaats van voor iedere website een aparte gebruikersnaam en wachtwoord te hoeven onthouden, hoef je je maar één keer aan te melden bij de zogenaamde *identity provider* die vervolgens er voor zorgt dat je op de juiste wijze wordt aangemeld bij alle websites die je bezoekt. Dit concept van *single sign-on* legt de nadruk bij identity management op toegangscontrole. Maar je kunt een IDM-systeem ook gebruiken om gegevens over gebruikers te beheren. In plaats van overal maar weer je adres of telefoonnummer in te voeren kun je die ook één keer opgeven aan je identity provider. Deze geeft deze dan wel door aan websites die dergelijke gegevens nodig hebben. Uit oogpunt van privacy is het hierbij natuurlijk wel van belang dat de gebruiker hier controle over heeft. Idealiter maakt het systeem hierbij gebruik van anonieme credentials. Door de gebruiker centraal te stellen, kunnen IDM-systemen gebruikt worden om je sociale identiteit (of eigenlijk identiteiten) te beheren: jij bepaalt zo welke gegevens over jou bekend zijn, en aan wie deze gegevens in een bepaalde situatie worden doorgegeven. Hoe dit soort IDM-systemen er uit moet zien en hoe ze in de praktijk kunnen en moeten worden toegepast is

een levendig onderzoeksgebied. Vooral de vraag of en hoe mobiele apparaten zoals smartphones hierbij een rol kunnen spelen om de gebruiker werkelijk centraal te stellen, en ook vanuit een technisch perspectief meer controle op zijn omgeving uit te laten oefenen, vergt nadere studie en ervaring. Te meer door de opkomst van het Internet der Dingen, dat door sommigen als een IDM-probleem in de overtreffende trap wordt gezien (Hof 2007).

Conclusies

Privacyvriendelijke systemen zorgen er voor dat informatie uitwisseling tussen de verschillende contexten waarin een individu zich begeeft onder controle blijft van het individu. Een belangrijke rol is hierbij weggelegd voor privacybeschermende technologieën, als onderdeel van een meer holistische, *privacy-by-design*, benadering waarin ook organisatorische en procesmatige aspecten worden meegenomen. Deze nadruk op *a priori* afscherming van gegevens is het uitgangspunt, maar bij toenemende onmerkbare registratie van gedragsgegevens is verdere *a posteriori* regulering van gebruiksmogelijkheden en transparantie onvermijdelijk.

De toepassing van deze technieken in de maatschappelijke praktijk is weerbarstig. Er zijn op dit moment geen grootschalige ICT systemen aan te wijzen die volledig met een privacy-by-design benadering zijn ontworpen. De te nemen hobbel is niet zozeer technisch maar meer bedrijfsmatig van aard. Voor rekeningrijden zijn er wel systemen bedacht met geavanceerde privacy beschermende maatregelen, maar dit systeem is vooralsnog niet in de praktijk gebracht. Op dit moment is voor de aanstaande invoering van slimme meters zeker aandacht voor de privacy, maar voor slimme meters is de privacy bescherming voornamelijk gerealiseerd door de hoeveelheid en de frequentie van de te verzamelen gegevens te beperken. Dat is winst, maar voor de toekomst is het te hopen dat bij grootschalige ICT projecten de privacy-by-design benadering wordt gevolgd, en bovenstaande technieken bredere toepassing vinden.

7. Resources

Achtergrondinformatie bij dit hoofdstuk is te vinden op de Privacy wiki, te vinden op http://wiki.science.ru.nl/privacy. Lezers worden uitgenodigd aan deze wiki bij te dragen.

8. BRONNEN

Agre, P. E., en **M. Rothenberg**, *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts: MIT Press, 2001.

Buruma, Y. Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld. In: D. Broeders, C.M.K.C. Cuijpers en J.E.J. Prins (red.) *De staat van informatie*, WRR-verkenning nr. 25, Amsterdam: Amsterdam University Press, 2011, 165-221.

Cavoukian, A. Privacy by design – the 7 foundational principles. Available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples. Information and Privacy Commissioner of Ontario, 2009.

Chaum, D. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM* 28 (10), October 1985 pp. 1030-1044.

Chaum, D. Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM* 24 (2), Feb. 1981.

Pfitzmann, A., en M. Hansen, *Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology.* http://dud.inf.tu-dresden.de/Anon_Terminology.shtml.

Hoepman, J.-H. Revocable Privacy. *Privacy en Informatie*, 11(3):114-118, juni 2008.

van 't Hof, C. *RFID and identity management in everyday life*, Rathenau Instituut, 2007.

Jacobs, B. Select before you collect. *Ars Aequi* 54 (Dec. 2005), 1006–1009.

Lessig, L. *Code and other laws of cyberspace.* Basic Books, 1999.

Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press, 2009.

Quisquater, J-J, Guillou, L.C,,en T.A. Berson,. How to Explain Zero-Knowledge Protocols to Your Children. *Advances in Cryptology - CRYPTO '89: Proceedings*, p.628-631, 1990

Solove, D. Understanding privacy, Harvard, MA: Harvard University Press, 2010.

Warren S. en Brandeis, L. The right to privacy. The implicit made explicit. *Harvard Law Review*, IV (5), December 15, 1890, 193–220.

Koorn, van Gils, ter Hart, Overbeek, en Tellegen Privacy Enhancing Technologies. Witboek voor beslissers. Uitgave van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, december 2004.

Yao, A.C. Protocols for Secure Computations (Extended Abstract). *Proceedings of Foundations of Computer Science* (FOCS) 1982, IEEE: 160-164.

[1] Dr. Jaap-Henk Hoepman is senior scientist bij TNO en Universitair Hoofddocent aan de Radboud Universiteit Nijmegen. Prof. Bart Jacobs is hoogleraar Digital Security aan de Radboud Universiteit Nijmegen

[2] Toegeschreven aan de Amsterdamse korpschef Welten

[3] E.g. http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf

[4] https://www.torproject.org/