MEMO

Onderwerp	**Verslag Privacy en geo-informatie een onmogelijke combinatie!?**
Aan	**Deelnemers workshop**
Van	**Geonovum**
Datum	**10 februari 2010**
Status	**concept**

Privacy en geo-informatie een onmogelijke combinatie!?
Op 4 februari organiseerden Geonovum en de TU Delft een workshop onder het motto: 'Privacy en geo-informatie een onmogelijke combinatie!?' De laatste maanden is privacy met enige regelmaat in het nieuws geweest. Het elektronisch patientendossier, de opslag van vingerafdrukken in een centrale database en signaleringen op basis van etnische achtergrond in de jeugdzorg, zet verschillende mensen aan het denken over digitalisering versus privacy. Haarscherpe panaromafoto's en de mogelijkheid om via de koppeling van informatie op locatie dicht bij de persoonlijke levensfeer van bewoners te komen, roept de vraag op, op welke wijze privacyaspecten van invloed zijn of kunnen worden op de toegankelijkheid van publieke geo-informatie. Tijdens de workshop in Den Haag gaf een gemêleerd gezelschap van beleidsmedewerkers, deskundigen van uitvoeringsorganisaties, bedrijfsleven en onderzoekers antwoord op deze vraag.

Na een aftrap aan de hand van presentaties van Bastiaan van Loenen van de TU Delft, Jose Hernandez van Rijkwaterstaat, Cees Guikers van BridGis en Colette Cuijpers van het Tilburg Institute for Law, Technology and Society, discussieerden de vijfentwintig deelnemers aan de workshop over vier stellingen. Het verslag van deze discussies vindt u in het dossier kennisdoorstroming op deze site.

Conclusies en aanbevelingen
Rode draad in de discussie is dat er in Nederland geen overheidsorgaaan beschikbaar is die vragen over privacy toetst. Het College Bescherming Persoonsgegevens is erg terughoudend in het geven van adviezen en andere adviseurs blijken terughoudend in hun adviezen over het verwerken van persoonsgegevens. In het algemeen valt het kennisniveau over wat wel en niet mag, te verbeteren. Voldoende kennis van het onderwerp werkt zelfregulering in de hand, zonder dat het innovatie tegen gaat. Ook was men het erover eens dat privacy bij de inwinning van gegevens niet zo zeer speelt. Het gaat eerder om het (her)gebruik van geo-informatie. Om hier gedragsregels over op te kunnen stellen is een scherpere definitie nodig van het begrip privacy.

Privacy in het geodomein
Aandachtspunt voor de geo-sector is het onderwerp locational privacy. Door het gebruik van signalen van mobiele telefoons en andere zenders die een persoon bewust of onbewust bij zich draagt, kan er spontaan persoonsgevoelige data ontstaan. Als voorbeeld is genoemd dat je het misschien niet zo erg vind als het signaal van je telefoon wordt gebruikt voor filemeldingen, maar wel als je mobiele telefoon langdurig verblijft in een psychiatrisch ziekenhuis. Medewerkers van het CBS wezen de aanwezigen erop dat ook geaggregeerde locatie-informatie nog vaak is terug te leiden naar individuen. Dataland levert bijvoorbeeld de gemiddelde WOZ waarde van 5 adressen. Slimme bevragingen aan Dataland kan een WOZ waarde op adresnvieau opleveren. Ook bij geaggregeerde informatievoorziening moet je daarom alert zijn.

Vervolg
Naar aanleiding van de workshop zal er een gelegenheidsnetwerk worden ingericht waarbinnen praktijkvoorbeelden worden verzameld die aangeven waar privacy in het geodomein een rol speelt of een barriere vormt. Deze praktijkcases kunnen dan als voedsel dienen voor de bredere discussie die woedt over

T 033 460 41 00
F 033 465 64 57
E info@geonovum.nl
W www.geonovum.nl

bezoekadres
Barchman Wuytierslaan 10
3818 LH Amersfoort

postadres
Postbus 508
3800 AM Amersfoort

digitalisering en privacy. Het is de bedoeling om bij die bredere discussie aan te sluiten. Hierover zullen Geonovum en het programma RENOIR van ICTU elkaar opzoeken.
In de afsluiting geeft Rob van de Velde, directeur van Geonovum, aan, dat hij de bevindingen van dit netwerk graag wil betrekken bij verkenningen naar de impact van geo-technologie op de overheid van de toekomst; een verkenning die door het programma Vernieuwing Rijksdienst wordt uitgevoerd.

-.-.-.-.-.-.-.-

Impressie presentaties groepsdiscussies

Stelling 1.
Of privacy wetgeving van toepassing is op GI moet per situatie worden beoordeeld.
Is dit uitvoerbaar? En zo ja, hoe?
Bijzondere persoonsgegevens kunnen bijvoorbeeld spontaan ontstaan indien een mobiele telefoon via het wireless access point van een moskee contact maakt (bijv. VoIP). Na honderd meter lopen kan de mobiel via een ander access point worden gelokaliseerd, dit keer geen gebouw gekoppeld aan bijzondere persoonsgegevens. Hoe kan hiermee worden omgegaan?

Wat is het probleem:
Op dit moment is het vrijwel niet mogelijk vooraf een vraag te toetsen bij het College bescherming persoonsgegevens. Zij zijn wel de enige autoriteit op dit gebied. Je kan naar adviseurs in de markt, maar die adviseren vaak risicomijdend wat nadelig is voor innovatie.

Wat zijn mogelijke oplossingen:
Je zou kunnen kijken naar certificering van adviseurs om ervoor te zorgen dat het kennisniveau over privacy verbetert. Overheidsinstellingen hebben ook nu de mogelijkheid een functionaris bescherming persoonsgegevens aan te stellen. Als je die hebt, hoe je niet meer alles te melden bij het CBP, maar kan je het gebruik intern registreren.

Wie moeten er wat doen
Aanbeveling is dat BZK en Justitie een nota opstellen over hoe om te gaan met privacy. Gedacht kan worden aan een handleiding op basis van praktijkvoorbeelden (zie ook onder stelling 4). Ook moet er iets als een informatiecentrum voor burgers komen. En burgers zelf moeten gaan signaleren als er iets gebeurt wat hen niet zint: “meld misbruik persoonsgegevens anoniem!”

Stelling 2.
Het generiek verzamelen van GI staat haaks op de doelspecificatie voorwaarde van Wbp. Hoe ga je er mee om?

Wat is het probleem:
We proberen vaak het inwinnen te reguleren terwijl daar het probleem niet ligt. Het probleem ontstaat niet zozeer bij het verzamelen, maar bij het (her-)gebruik. Dit leidt tot vertragingen en onduidelijkheid en het leidt tot risicomijdend gedrag.

Mogelijke oplossingen
- Gebruik van disclaimers
- Voorlichting
- Eigen verantwoordelijkheid
- Toetsing bij het CBP
- WOB toetsing
- Ex-post misbruik van persoonsgegevens melden.
  Deze optie werd kritisch ontvangen door de deelnemers. Ex-post betekent dat de persoonsgegevens al zijn verzameld en zijn gebruikt. Verdere controle op het gebruik wordt zeer moeilijk zoals recente voorbeelden van misbruik op flickr aantonen.
- Is er een probleem dan moet je het ergens kunnen melden.

Stelling 3.
Technische mogelijkheden bepalen de relatie tussen privacy en geo-informatie. Hoe meer er technisch kan hoe moeilijker het is om het privacybelang afdoende te respecteren.

- *Wat is het probleem:*
  wetgeving loopt altijd achter bij realiteit
- Handhaving is nauwelijks te realiseren
- Regimes verschillen per land. Ook speelt het globaliseringsissue (denk aan Google) waarbij helemaal niet meer duidelijk is onder welk regime de verwerking van de persoonsgegevens valt.

Mogelijke oplossingen
Definiëren welke gegevens nu echt moeten worden beschermd. Niet alle persoonsgegevens zijn even gevoelig. Techniek inzetten om privacy beter te beschermen. Denk aan een digitale kluis of sluis waar je zelf kan aangeven als burger waarvoor je gegevens gebruikt mogen worden. Geeft ook inzicht in welke gegevens van jou worden vastgelegd door wie en waarvoor. Aandachtpunt: overheid mag in principe alles gebruiken (binnen de regels die daarvoor al bestaan). Bedrijfsleven zou op geaggregeerd niveau ook van deze gegevens gebruik moeten kunnen maken.

Wie moet wat doen?
Justitie en BZK moeten de definitie van gegevens die beschermd moeten worden nader definieren. Het lijkt zinvol om onderscheid te maken in wat persoonlijke levenssfeer is en wat niet.

Stelling 4.
Privacy is een belemmering om onze taken succesvol uit te voeren. Wat is het proleem en wat moet er worden veranderd.

Deze vraag is opgepakt aan de hand van 4 cases, om duidelijk te illustreren waar het om gaat.

Hulpverleners zouden graag via het (mobiele-)telefoontoestel van een slachtoffer en/of een getuige het slachtoffer localiseren. Zij zouden dan naar hem toe kunnen gaan en hem helpen, als de beller zijn telefoongesprek niet kan afmaken. Dit kan nu echter niet, waarschijnlijk om privacyredenen. De politie kan dan dan nl. ook de beller localiseren (een gecombineerde meldkamer) en wil die gegevens wellicht gebruiken voor opsporing, terwijl de beller mogelijk zijn gegevens niet wil doorgeven aan de politie (aldus GGD Amsterdam) Advies: maak het mogelijk om via het (mobiele-)telefoontoestel een slachtoffer te localiseren. Dit mag, omdat er sprake kan zijn van vitaal belang (art 8.d van de WBP), dat boven het belang van de privacy gaat. Zodra blijkt dat van vitaal belang geen sprake is, wis je de gegevens opdat een getuige die anoniem wil blijven, toch durft te melden. Dit leg je vast in een protocol dat je voor advies voorlegt aan het College bescherming persoonsgegevens (CBP).

WOZ. Je kan inzage krijgen op 3 vergelijkbare panden. Ben je niet tevreden dan kan je na toetsing van je verzoek inzage krijgen in nog eens 9 vergelijkbare panden. Gemeenten willen WOZ transparanter maken om het vertrouwen in de uitvoering te verbeteren. Modernisering van het taxatieverslag en de mogelijkheid bieden om de belanghebbende zelf 9 WOZ-waarden van derden te laten selecteren, zou daaraan kunnen bijdragen. Het belang hiervan zou aangetoond kunnen worden. Zodat een afweging gemaakt kan tussen meer transparantie ten behoeve van verbetering van het vertrouwen en het privacybelang van betrokkenen individuen. De vermindering van administratieve lasten als er geen tussenkomst van de gemeente meer nodig is kan daarbij ook worden betrokken. Wellicht zijn er technische mogelijkheden om bepaalde waarden af te schermen.

Evacuatie: bij een evacuatie wil je graag gegevens hebben over de omvang van de evacuatie die nodig is. Geaggregeerde informatie is (meestal) niet privacygevoelig. Het argument om in dit geval gegevens niet vrij te geven is mogelijk eerder een vals argument. Om administratieve lasten te voorkomen, wordt privacy als excuus gebruikt.

Cyclomedia: heeft weinig last van privacy doordat zij de doelomschrijving en voorwaarden goed op orde hebben en zich daar ook aan houden. Afnemers van hun product hebben vaker problemen met hergebruik. Als cyclorama's persoonsgegevens bevatten, zoals een kenteken, en de afnemer wil deze via internet ontsluiten, dan moeten de persoonsgegevens onherkenbaar worden gemaakt.