



Wie beheert mijn dossiers? Centraal versus de-centraal gegevenbeheer



I. Achtergrond

Wie is die man eigenlijk?

- Hoogleraar computerbeveiliging, in Nijmegen & Eindhoven
- Betrokken bij zaken als **biometrisch paspoort** en **elektronisch stemmen** (lid cie. Korthals Altes over herinrichting stemmen)
- O.a. geïnteresseerd in “identiteitsmanagement”
- Betrokken bij maatschappelijke discussies, soms in de media.
- Auteur van online boek *De Menselijke Maat in ICT*, zie www.cs.ru.nl/B.Jacobs/MM



Computerbeveiliging

- Regulering van toegang tot gevoelige digitale gegevens, zoals:
 - militaire of industriële gegevens
 - privacy-gevoelige gegevens (bijv. over gezondheid, communicatie, financieën)
- Focus niet op functionaliteit van ICT, maar op misbruik
(geen leuke maar nare, onbedoelde dingen)
- Vereist juiste mix van technologische, organisatorische & juridische maatregelen

Jacobs – UvA 1 juni 2007 – p.4/40



II. ICT en samenleving

Jacobs – UvA 1 juni 2007 – p.5/40



Rol van informatici

- Informatici zijn:
 - primair architecten van de *digitale* wereld,
 - steeds meer ook van de *sociale* wereld.
(Lawrence Lessig: **Architecture is politics**)
- Brede visie vereist—maar ontbreekt vaak
- Nu cruciale besluiten over ICT-infrastructuur
 - Centrale of decentrale opslag
 - Identiteits-rijk of -arm, etc
- Over 10 jaar: “*where did we go wrong?*”

Jacobs – UvA 1 juni 2007 – p.6/40



Ontwikkelingen

- Tbv. **terrorisme-/criminaliteits-bestrijding**: altijd identiteiten vastleggen & traceren
- Tbv. **service/gemak**: één identiteit in alle situaties (zoals BSN), als kapstok voor centrale opslag & analyse gegevens
- Tbv. **commerciële profilering**: tracering van gedrag voor focus in marketing & gemak

Veiligheid & gemak als grote vijanden van privacy!?

Jacobs – UvA 1 juni 2007 – p.7/40



Tegengeluiden / risico's

- Universele herkenbaarheid maakt kwetsbaar
 - Vrouwen in blijf-van-mijn-lijf huis / Rfid-bom
 - Huisfoto's en adressen BN-ers mochten niet op web [casabobo.nl]
- Één identiteit verergert identiteitsfraude
 - één nummer / centralisatie vergroot aantrekkelijkheid voor fraudeurs
 - geslaagde fraude is wijd vertakt

Privacy essentieel voor persoonlijke veiligheid!

Jacobs – UvA 1 juni 2007 – p.8/40



III. Privacy

Jacobs – UvA 1 juni 2007 – p.10/40



Wat willen we eigenlijk?

Een maatschappij waarin burgers:

- (a). als gelabeld vee (“met chip in de nek”) voortdurend door allerlei controlepoortjes gejaagd worden, en benaderd en beoordeeld worden op basis van persoonlijke profielen uit centraal opgeslagen gedrag;
- (b). autonoom eigen gegevens/authenticatie beheren en betrouwbaarheid van controlepunten en gegevensverwerking (vooraf) zelf kunnen checken.

Jacobs – UvA 1 juni 2007 – p.9/40



Privacy, begripsmatig

- Lange historie, vooral in juridische & ethische literatuur
- Klassiek: *The right to be left alone* (Warren en Brandeis, 1890)
- Gekoppeld aan menselijke waardigheid, autonomie, vrijheid (en meer moois)
- Essentieel voor sociaal verkeer: je moet niet alles willen weten van je buurman
- Laatste jaren: “schuilplaats van het kwaad”
- Moeilijk hard te verdedigen: *soft value*.

Jacobs – UvA 1 juni 2007 – p.11/40

Privacy, juridisch

- Verankerd in grondwet (art. 10): *“Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer”*
- Ondersteund door Wet & College Bescherming Persoonsgegevens (WBP & CBP)
 - Doelbinding voor opslag vereist
 - Beveiligingstaak bij verantwoordelijke
 - Individueel recht op inzage & correctie
 - Bijhouden honderden databanken is dagtaak: niet echt uitvoerbaar [zie later]

Jacobs – UvA 1 juni 2007 – p.12/40

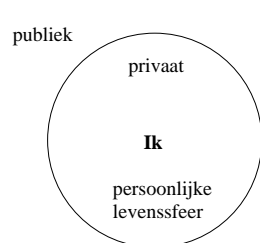
Privacy & rollen/levenssferen I

- Mensen hebben verschillende rollen:
 - collega, moeder, dochter, kerkganger, vrijwilliger, patiënt, etc
 - Bij ieder van die rollen hoort een eigen (kleinschalige) sfeer, met daarbij horende informatie en (betekenis)context
 - Essentieel voor privacy is:
 - individuele controle om informatie die bij een rol hoort ook tot die rol te beperken*
- Dwz. “Informationele zelfbeschikking”

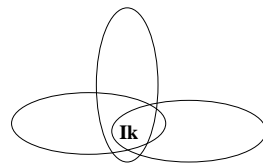
Jacobs – UvA 1 juni 2007 – p.13/40

Privacy & rollen II

- Traditioneel: tweedeling publiek/privaat
- Hier meer gedifferentieerd: compartimentalisatie van (meerdere) rollen en informatie.



Traditionele tegenstelling



Differentiatie naar rollen

Jacobs – UvA 1 juni 2007 – p.14/40

Privacy & rollen III

- Vanuit deze compartimentalisatie-gedachte lijkt het belang van privacy onomstreden
- Maar mensen verschillen mbt. de gebieden en de maten waarin ze compartimentaliseren
- Bij verschillende rollen horen verschillende “deel-identiteiten”
- Mensen tot één identiteit reduceren (zoals via BSN) is onnatuurlijk.

Jacobs – UvA 1 juni 2007 – p.15/40



Privacy & rollen, technisch

- Goede automatisering volgt gevestigde gebruiken (en vereist formalisatie daarvan)
- Rol kan corresponderen met cryptografisch sleutelpaar (publiek, privé)
- Elementair gebruik van sleutelpaar (bij rol):
 - Ondertekening voor commitment vanuit rol (als werknemer, of als secretaris van tennisclub)
 - Versleuteling voor compartimentalisatie van informatie binnen rol

Het eerste met privé sleutel, het tweede met publieke



IV. Keuzes



Hoezo keuzes

- Onze samenleving wordt in toenemende mate “gedigitaliseerd”
- Informatie is macht: wie de informatie-stromen beheer(s)t is de baas
- ICT-architectuur heeft socio-politieke impact
- Vier voorbeelden:
 - Rekeningrijden
 - Elektronisch Patiënten Dossier (EPD)
 - Wie authenticceert zich eerst?
 - Stemwijzer.



Rekeningrijden I

- Eerste ontwerp in 2001 van Pieper iov. Netelenbos (maar nooit gerealiseerd):
- Auto heeft GPS (voor locatiebepaling) en GSM (voor doorgeven verschuldigde heffing)
- Omwille van privacy/zorgvuldigheid:
 - Verdeel NL in rode, groene en gele wegen, ieder met eigen tarief
 - Geef alleen door: hoeveel km op welke kleur.
 - “PET” oplossing: net voldoende data voor doel



Rekeningrijden II

- Hernieuwde actualiteit rekeningrijden
- Te verwachten nieuwe architectuur:
 - centrale opslag alle vervoersbewegingen
 - “mede omwille van terrorismebestrijding”
- Typische keuze: **centraal** of **decentraal** opslag & beheer van gegevens
- Centralisatie niet nodig; geeft risico's voor individuen (omvallen databank); versterkt gevoel van controle; is eenvoudig te omzeilen door kwaadwillenden. **Waarom dan toch?**

Jacobs – UvA 1 juni 2007 – p.20/40



Elektronisch Patiënten Dossier (EPD) I

- EPD nuttig voor onderlinge communicatie & consistentie tussen zorgverleners
- Drie mogelijke architecturen:
 - (a). Centrale databank: risicovolle bottleneck
 - (b). Centrale pointerstructuur & gegevens bij zorgverleners: voorzien in NL als “LSP”
 - (c). Gegevens gecentraliseerd bij individuen: beschikbaarheidsprobleem
- Individuele toegangscontrole over eigen dossier ook voorzien in LSP.

Jacobs – UvA 1 juni 2007 – p.21/40



Klantenkaart & EPD issues

- AH en anderen:
 - Geef klant kaart voor identificatie
 - Registreer aankoopgedrag **centraal**
- Alternatief **decentraal** scenario:
 - Laat klant eigen aankoopgedrag opslaan (op GSM of PDA, in de toekomst)
 - Geef gerichte korting bij inzage
 - Geef klant selectieve *delete* optie (bij aambeienzalf, of Playboy + doos tissues)
- Voordelen voor AH & klant. Ook bij DTV?

Jacobs – UvA 1 juni 2007 – p.22/40



Wie authenticceert zich eerst? I

- Stel een agent vraagt u om identificatie
- U heeft alle recht om dan te zeggen:
 - Het is net carnaval geweest ...
 - ... ik wil eerst uw identificatie zien ...
 - ... daarna pas toon ik de mijne.
- Dit is goed geregeld in de wet.

Jacobs – UvA 1 juni 2007 – p.23/40



Wie authenticceert zich eerst? II

- Via uw bankpas en pincode krijgt een geldautomaat toegang tot uw rekening
- Maar hoe weet u of de automaat *echt* is?
- Soms worden nepautomaten (tijdelijk) geplaatst, om rekeningen te plunderen
- Gebruikt u een geldautomaat op het terrein van een autosloper?
(met excuus aan de branche)
- Automaten moeten zich kunnen authenticeren, voordat u dat doet (via pas+pin)

Jacobs – UvA 1 juni 2007 – p.24/40



Wie authenticceert zich eerst? III

- In nieuw paspoort zit chip met biometrie: nu gezichtsfoto & later ook vingerafdrukken
- Ik moet mijn vingerafdrukken bij allerlei grensovergangen laten controleren . . .
- . . . zonder dat ik weet:
 - of de lezer echt / betrouwbaar is
 - wat er vervolgens met mijn opgenomen vingerafdrukken gebeurt
- Mijn vingerafdruk wordt daardoor feitelijk waardeloos.

Jacobs – UvA 1 juni 2007 – p.25/40



Wie authenticceert zich eerst? IV

- Burgers worden aan steeds strengere controles onderworpen,
- en moeten zich steeds vaker authenticeren.
- Voorafgaand moet de burger echter kunnen controleren dat de authenticatiemiddelen goed terechtkomen, en niet misbruikt worden
- Anders is identiteitsfraude onbeheersbaar.
- Leg controle/macht bij burgers.

Jacobs – UvA 1 juni 2007 – p.26/40



Stemwijzer I

- www.stemwijzer.nl veel gebruikt: bijna 4 miljoen keer voor Nov'06.
- Beheerd door Instituut voor Publiek en Politiek (IPP)
- Invullen vragenlijst en berekening stemadvies via locale software (ingebed in webpagina)
- Vervolgens worden statistieken getoond: vereisen doorgifte gegevens aan server!
- Politieke voorkeur geldt als “gevoelig” persoonsgegevens.

Jacobs – UvA 1 juni 2007 – p.27/40



Stemwijzer II

Ingezonden (eigen) stuk Volkskrant 03/07:

- Opslag politieke voorkeuren + IP-adres; (IP-adres is identificerend, volgens CBP)
- Website stemwijzer zonder **Privacy Policy**
- Stemwijzer is feitelijk **Spyware**
- Opsporings- en inlichtingendiensten kunnen deze data in principe vorderen.



Stemwijzer IV: conclusies

- Kwaadaardige opzet niet waarschijnlijk; onbenulligheid wel.
- Bewustzijn voor gevoeligheid van gegevens is laag, bij beheerders & gebruikers.
- Anonimiseren had gemoeten (wsch. ook voorwaarde voor evt. toestemming CBP)
- We zijn afhankelijk geworden van beschavingsniveau van opspoorders
- Mogelijkheid vordering voortaan noemen in privacy policies



Stemwijzer III: reacties

- IPP / Stemwijzer:
 - Aanvankelijk: wat is het probleem?
 - Na een maand: OK, we anonymiseren & plaatsen privacy policy
- CBP: we starten een onderzoek (Vooralsnog geen uitkomst)
- AIVD: zulke gegevens vorderen wij niet!
- Volkskrant: inbraak georkestreerd, maar mislukt



V. Proactieve overheid



Uitgangspunten

- Cruciaal voor onze rechtstaat is een **machtsbalans** tussen overheid en burgers:
- Overheid heeft beperkingen:
 - gebonden aan regels (niet zo maar arresteren)
 - kan aangeklaagd en veroordeeld worden
- Nederlanders hebben groot vertrouwen in overheid (itt. bijv. Amerikanen)
- Grootschalig gegevens afstaan vereist ook vertrouwen in alle toekomstige regeringen



Veiligheid & proactiviteit I

- Basisprincipe: alleen op basis van een “redelijk vermoeden” wordt je verdachte.
 - Vervolgens kunnen je privacy-rechten geschonden worden, bijv. via tappen
 - Dwz. eerst slecteren, dan verzamelen!
- Steeds vaker: eerst verzamelen, dan selecteren!
 - Duidelijkst bij data-retentie (verkeersgegevens)
 - Iedereen is verdachte!
- Proactief, discutabel veiligheidsbeleid.



Gemak & proactiviteit I

- Overheid weet veel van burger, en meent ook te weten wat goed is voor burger
- Gemak voor burger als hoogste goed!
 - “makkelijker kunnen we het wel maken”
 - Dogma van “eenmalige gegevensverstrekking”
 - Houd de burger vooral passief & dom
- Waarom privacy of autonomie niet als hoogste goed? Wie beslist dat eigenlijk?
- En op grond waarvan?



Gemak & proactiviteit II

- Waarom “eenmalige gegevensverstrekking”?
 - Formulieren met de hand invullen is vervelend
 - Maar daarom centraliseren?
 - Stel nou dat je kunt *beamen*; of pointers uitdelen
- Raad van State: BSN is service voor overheid, niet voor burger
- BSN is *identity management for dummies*
- Compartmentalisatie beter voor privacy en tegen identiteitsfraude.



VI. Conclusies

Jacobs – UvA 1 juni 2007 – p.36/40



Wie beheert mijn dossiers?

Waarom geen overheid die zegt...

- Beste burger, wij kunnen al uw doen en laten registreren en analyseren, maar dat doen wij niet want zo'n samenleving willen we niet.
- Wij kunnen ook al uw formulieren al invullen en besluiten wat goed voor u is, maar ook dat doen wij niet want we willen u blijven zien als vrije, autonome individuen die de eigen gegevens beheren.
- Wij realiseren dat dat u moeite kost, maar wij zijn niet bang dat te vragen: het is onze taak hogere waarden te beschermen

Jacobs – UvA 1 juni 2007 – p.37/40



Wie beheert mijn dossiers?

Suggesties aanpassing WBP

- Verplicht online inzagemoogelijkheid in eigen gegevens (nu al soms bij telefoon of energie)
- Verplicht (additionele) diensten die op profilering gebaseerd zijn **optioneel** te zijn.
 - Bij weigering, mogen ook geen gedragsgegevens verzameld worden
 - Bij toestemming, geef deelnemers online toegang en beheer van hun gedragsgegevens
- Bij authenticatieverplichting, vereis dat (vertegenwoordiger van instantie) zich eerst authenticceert

Jacobs – UvA 1 juni 2007 – p.38/40



Wie beheert mijn dossiers?

Samenvatting

- We staan voor cruciale keuzes mbt. ICT-infrastructuur en samenleving (bijv. mbt. centralisatie)
- Onze fundamentele waarden staan daarbij onder druk, en verdienen bescherming
- Geef burgers echte zeggenschap: beheer over gegevens en authenticatie
- Veiligheid vs. privacy: *select before you collect*
- Gemak vs. privacy: geef burgers middelen & doorbreek gemaksterreur.

Jacobs – UvA 1 juni 2007 – p.39/40



Tenslotte

Meer details & discussie in gratis online boek:

De Menselijke Maat in ICT
www.cs.ru.nl/B.Jacobs/MM

Dank voor de aandacht!