

Privacy en Identity Management



Inhoud

- I. Achtergrond
- II. Fraude & Privacy
- III. Identiteiten
- IV. Autonomie
- V. Surveillance en Datamining
- VI. Kun je met gegevensbescherming geld verdienen?
- VII. Conclusies



I. Achtergrond

Wie is die man eigenlijk?

- Hoogleraar computerbeveiliging, in Nijmegen & Eindhoven (studie: wiskunde + filosofie)
- Betrokken oa. bij **biometrisch paspoort**, **OV-chip**, **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 (EPD), communicatie, financiën
- Vereist juiste mix van technologische, organisatorische & juridische maatregelen
- Toegang tot informatie (ICT-architectuur) in hoge mate politiek (bijv. bij OV of rekeningrijden)
- Focus niet op functionaliteit van ICT, maar mogelijk misbruik

Jacobs – TNT post, 10 dec. 2008 – p.4/36



II. Fraude & Privacy

Jacobs – TNT post, 10 dec. 2008 – p.5/36



Simpele vragen I

- Hoe is de Yahoo mailbox van Sarah Palin gehackt?
 - Via de optie: *password forgotten*
 - Antwoorden op controlevragen stonden in Wikipedia & Google
- Is haar “identiteit” gestolen?
 - Haar “mail” identiteit zeker
 - en natuurlijk haar identificatie/authenticatie gegevens.

Jacobs – TNT post, 10 dec. 2008 – p.6/36



Simpele vragen II

- Waarom vind ik het een ramp wanneer mijn geboortedatum / BSN / creditcardnr. / ... op het web verschijnen?
- Heb ik hier enige controle over?
- Privacy is belangrijk!
 - Los van ideologie, of van “als je niks te verbergen hebt” flauwekul
 - Id-fraude is maatschappelijk ontwrichtend, en niet enkel persoonlijke verantwoordelijkheid
 - Privacy is essentieel voor persoonlijke veiligheid

Jacobs – TNT post, 10 dec. 2008 – p.7/36



Identiteitsfraude

- Snelst groeiende vorm van criminaliteit
- Via internet bankrekeningen leeghalen is minder risicovol dan met afgezaagd geweer bank binnengaan
- Zeer vervelend & ingrijpend voor slachtoffer
 - herstel langdurig, lastig en tijdrovend
 - vaak onenigheid met 3e partijen
- In cybercrime (vooral identiteitsfraude) gaat meer geld om dan in drugshandel

Jacobs – TNT post, 10 dec. 2008 – p.8/36



Spanningsvelden

- Overheid heeft dubbele rol:
 - bescherming privacy burgers (wettelijke plicht)
 - controle naleving wetten (vnl. reactief)
 - nu ook voorkomen van narigheden (proactief)
 - strategie: iedere burger is potentiële crimineel, kindermishandelaar, terrorist, . . .
- Burger is dubbelzinnig:
 - wil geen fraude, misbruik, lastigvallen
 - wil ook gemak en is weinig kritisch
- Marketeer wil gewoon alles van klanten weten

Jacobs – TNT post, 10 dec. 2008 – p.9/36



Grote issues

Informatie is macht / geld!

Huidige machthebbers beslissen over nieuwe ICT-infrastructuur (*architecture is politics*)

Wie beschermt de burger / klant?

Jacobs – TNT post, 10 dec. 2008 – p.10/36



III. Identiteiten

Jacobs – TNT post, 10 dec. 2008 – p.11/36



Identificatie & authenticatie

- **Identificeren** is zeggen wie je bent
 - Vb. naam, loginnaam, rekeningnr, BSN, ...
- **Authenticeren** is bewijzen wie je bent
 - Vb. wachtwoord, PIN, paspoort (ook identificatie)
- Drie basisvormen van authenticatie:
 - iets wat je **hebt**: sleutel
 - iets wat je **weet**: PIN, wachtwoord
 - iets wat je **bent**: vingerafdruk, irisscan
- Natuurlijke volgorde:
identificatie, authenticatie, autorisatie

Jacobs – TNT post, 10 dec. 2008 – p.12/36



Attribuut-gebaseerde autorisatie

- Autorisatie kan ook zonder identiteiten, maar met attributen / eigenschappen:
 - na bewijs “ouder dan 18” mag je XXX
 - als je genoeg geld hebt mag je ...
 - als je een geldig kaartje hebt mag je ...
- Anonieme diensten zijn heel natuurlijk
 - Soms “revocable” privacy: bij misdraging wordt alsnog identiteit bepaald (kentekens in verkeer)
- IT-systemen werken (nog) zelden met attributen

Jacobs – TNT post, 10 dec. 2008 – p.13/36



OV-chip voorbeeld

- Traditioneel papieren treinkaartje is anoniem (bij 'n treinreis hoef je niet te zeggen wie je bent)
- Iedere OV-chipkaart heeft vast (publiek) nummer, meestal gekoppeld aan persoon
- Resultaat is een Stasi-achtige database met alle persoonlijke reisgegevens.
 - is dit voor invoering duidelijk gemaakt?
 - wie heeft hier voordeel bij en beslist hierover?
- Anonieme kaart is een lachertje
 - bij opladen met bankpas raakt naam bekend
 - te koop via het web!

Jacobs – TNT post, 10 dec. 2008 – p.14/36



Twee aanpakken identiteitsfraude

- Identiteiten **meer** en beter vastleggen.
 - voor de hand liggende reactie
 - vergelijkbaar met: meer politie!
 - omvat meer gegevens voor meer fraude
- Identiteiten **minder** vastleggen
 - wanneer identiteiten niet bekend zijn kunnen ze ook niet gestolen & misbruikt worden
 - terug naar attribuut-gebaseerde autorisatie?
 - of meer pseudoniemen?

Jacobs – TNT post, 10 dec. 2008 – p.15/36

IV. Autonomie

Jacobs – TNT post, 10 dec. 2008 – p.16/36

Twee stellingen

- I. Individuele autonomie is fragiel/kwetsbaar
- II. Onze maatschappij is van oudsher voor een belangrijk deel ingericht ter bescherming van deze autonomie.

Jacobs – TNT post, 10 dec. 2008 – p.17/36

Autonomie voorbeeld I: stemmen

- Stemmen vindt plaats in aparte stemlokalen, waar
 - geen politieke uitingen toegestaan zijn
 - mensen alleen het stemhokje in moeten
 - geen bewijs van eigen stem gegeven wordt
- Men wordt “beschermd” om autonoom te stemmen! Kennelijk is die bescherming nodig
- Terzijde: Stemmen via internet bedreigt deze autonomiebescherming (“*family fraud*”)

Jacobs – TNT post, 10 dec. 2008 – p.18/36

Autonomie voorbeeld II: advertenties

- Motie Vietsch (31/10/06) vraagt verbod op tv kredietreclames voor persoonlijke leningen
- Niet iedereen is bestand tegen agressieve marketing
- Direct marketing nog in de kinderschoenen
 - postcodegebied, bijv bij folders (Cendris)
 - websites geven persoonlijke suggesties (Amazon)
 - behavioural targeting / prijsdiscriminatie
 - is aanvullende bescherming nodig?

Jacobs – TNT post, 10 dec. 2008 – p.19/36



Autonomie voorbeeld III: verhoren

- Niet iedereen vertelt de waarheid onder grote druk
- Bekende dwalingen (Schiedam, Putten, ...)
- Roep om bescherming van verdachten, bijv. via videoopname / advocaat bij verhoor.

Jacobs – TNT post, 10 dec. 2008 – p.20/36



Surveillance

- Bijna al ons gedrag laat digitale sporen na:
 - Mailen, surfen, bellen (ook locatie), TV, betalen
 - Reizen: vliegen, OV, auto (evt. via km-heffing)
 - Medische gegevens & biometrie
- Dominante paradigma: centrale opslag
 - Risico's: hacken, verlies, misbruik, slordigheid
 - Incidenten zijn structureel (in GB; ook in NL)
 - Gebruik: commercie, dienstverlening, veiligheid

Jacobs – TNT post, 10 dec. 2008 – p.22/36



V. Surveillance & datamining

Jacobs – TNT post, 10 dec. 2008 – p.21/36



Voorbeelden I

- **Orn** weet van vrouwen wanneer ze ongesteld zijn (mbv. bonuskaarten)
- **Vodafone** weet van mannen of ze in hoerenbuurten komen (mbv. locatiegegevens)
- **Stemwijzer** weet van miljoenen de politieke voorkeur (mbv. IP-adressen)
(Anonimisering alleen na CBP-opdracht daartoe)

Jacobs – TNT post, 10 dec. 2008 – p.23/36



Wat is datamining?

- Geautomatiseerde, statistische analyse van grootschalige gegevensbestanden
- Gericht op:
 - testen van hypothesen
 - ontdekken van verbanden
- **Nota bene:** datamining levert statistische patronen, geen oorzakelijke verbanden

Jacobs – TNT post, 10 dec. 2008 – p.24/36



Voorbeeld II

- Ben je een mogelijke terrorist als je:
 - onlangs in Pakistan was
 - niet lokaal, maar wel veel internationaal belt
 - in het vliegtuig 'n hallal maaltijd bestelt en aan de gang wil zitten . . .
- Ben je een mogelijke weetteler als je:
 - alleenstaande bent, met een vette auto
 - en een hoog stroomverbruik
- Of een liefhebber van zonnenbanken?

Jacobs – TNT post, 10 dec. 2008 – p.26/36



Voorbeeld I

- Winkelier wil weten welke producten samen gekocht worden (om ze bij elkaar te plaatsen)
- Werwijze:
 - maak lijst van alle paren producten
 - zoek voorkomen bij flink aantal klanten
- Mogelijke uitkomst:
 - taco chips & chili saus; bonensoep & toiletpapier (!)
 - hondenvoer & oude kaas (?)
- Levert hooguit aanwijzingen

Jacobs – TNT post, 10 dec. 2008 – p.25/36



Datamining is omstreden

- Associatie met “pre-crime” (*Minority Report*) en Kafka (beschuldiging onbekend)
- Privacy schendingen met grote bestanden
 - gedeeltelijk oplosbaar, via anonimisering
 - alleen identificatie bij “hit”
 - maar wat is een “hit” (en wie bepaalt dat)?
- Veel bestanden zijn vervuild; door koppelingen propageren fouten
- Omdraaiing bewijslast: **Niet:** politie moet bewijzen, **Maar:** burger moet uitleggen.

Jacobs – TNT post, 10 dec. 2008 – p.27/36



Datamining in commerciële wereld

- Fouten zijn minder belangrijk
 - bij stoppen met pil, stuur luierreclame
 - werkt niet bij begin 'overgang'
 - Nou ja, ach, jammer.
- Trend: *behavioural targeting*
- Grote vraag: hoeveel zal klant (& overheid) accepteren?

Jacobs – TNT post, 10 dec. 2008 – p.28/36



Diensten op open netwerken

- Internet is “open”, zonder monopolie, waardoor *overlay* diensten mogelijk zijn.
- Anoniem surfen mogelijk via **Tor**: page request gaat niet rechtstreeks maar in hops via special servers
- Wegwerp email adressen mogelijk bijv. via **spamgourmet.com**: eenmalige adressen voor beperkt aantal emails

Jacobs – TNT post, 10 dec. 2008 – p.30/36




VI. Kun je met gegevensbescherming geld verdienen?

Jacobs – TNT post, 10 dec. 2008 – p.29/36



Op gesloten netwerken ...

- Mbv. “baas” op het netwerk, bijv.
 - wegwerp 06 nrs (ik zou mobiel meer gebruiken)
 - wegwerp bankrekeningnrs (opladen OV-chip)
 - wegwerp “huisadressen”
- Wanneer het systeem gebroken is 
 - OV-chip is open kaart / portemonnee
 - daarmee anonimiseerbaar
 - organiseer een pool van gebruikers
 - download identiteit vanuit pool voor gebruik

Jacobs – TNT post, 10 dec. 2008 – p.31/36



ICT op maat

- Individuele benadering van burgers / klanten mogelijk met moderne ICT
- Wordt vooral gebruikt om dingen door de strot te duwen (*behavioural targeting*)
- Waarom niet om (commercieel) dingen mogelijk te maken die mensen *echt* willen?
- Ook al willen ze (bijna) niks!
- Bouw allereerst vertrouwen op.

Jacobs – TNT post, 10 dec. 2008 – p.32/36



Webportal voorstel

Bied klanten een individueel portal, met:

- sterke authenticatie (niet alleen wachtwoord)
- versleutelde opslag van eigen gegevens (digitale kluis)
- toegang tot (commerciële) diensten
- reclame onder klantcontrole: over auto's alleen wanneer tijdelijk aangevinkt; anders echt niet
- klantcontrole over logging
- anonimisering (wegwerp adressen + betaling)
- durf businesskansen te missen tbv. vertrouwen

Jacobs – TNT post, 10 dec. 2008 – p.33/36



Business model

- Neem privacy fanaat als uitgangspunt, en biedt vervolgens opties
- Schatting:
 - 90% van deelnemers wil wel reclame + diensten
 - 10% fanatici leveren geen opbrengst (en dat moet je ook niet willen)
- **Maar:** met deze 10% binnen boord:
 - heb je een vertrouwensbasis voor de rest
 - groeit je absolute aantal gebruikers
 - en neemt het relatieve aantal privacy fanaten misschien wel af.

Jacobs – TNT post, 10 dec. 2008 – p.34/36



VII. Conclusies

Jacobs – TNT post, 10 dec. 2008 – p.35/36



Belangrijkste punten

- Toekomst ligt in gepersonaliseerde diensten; begrip van identiteiten dus belangrijk
- Bescherming van persoonsgegevens vanwege privacy, persoonlijke veiligheid, identiteitsfraude, vertrouwen, autonomie
- Nieuwe business opportunities, waarin vertrouwen van klanten de basis is, en (commerciële) kansen soms onbenut moeten blijven, om vertrouwen te houden
- *In der Beschränkung zeigt sich der Meister!*