@zwnne

LEIDEN REVISITED
25 SEPTEMBER 2015

Een cybersecurity incident en enkele gedachten over profilering en privacyregels

prof. mr. Gerrit-Jan Zwenne

Universiteit Leiden

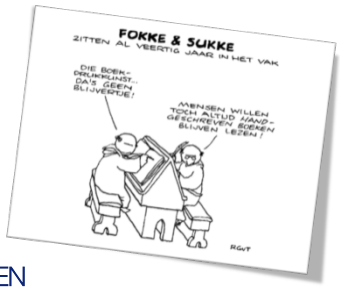
eLaw Leiden

Programma

A. actualiteiten

B. een cybersecurity incident

C. profileren en privacyregels



A. ACTUALITEITEN

- Ham over bewaarplicht
- Bot over Facebook
- Privacy meldplicht & boetes
- AVGB

Een nieuwe Europese privacywet

B. EEN CYBERSECURITY INCIDENT

Holland Energie N.V.

- productie en levering
- beursgenoteerd (AEX)
- marktaandeel ca. 20-25 %

Gerrit-Jan
IT Manager

Joanne
General Counsel

Het is vrijdag 16:45.
De telefoon gaat...

actie

- schade beperken
  - lek dichten
  - betrokkenen
  - verzekering
- lek melden bij autoriteiten
- aangifte
- verder..?

een e-mailbericht

sent: 25 September 2015 (17:46 CET)
to: Joanne (Legal)
cc: IT ALL
subject: Groot Probleem!

Hi Joanne,

Het lijkt veel groter dan gedacht. Mijn voorganger had toegang tot alle systemen waarmee productie wordt aangestuurd. Er is veel meer aan de hand. Ik sluit niet uit dat we centrales moeten afschakelen. :(

Er zijn echt grote fouten gemaakt!! Deze man had natuurlijk nooit toegang mogen hebben tot die systemen.

We duiken erin. Ik houd je op de hoogte.

Cherio,
G-J.

een journalist

"er gaat een gerucht dat jullie kolencentrale is gehackt"

acties

- voorwetenschap (Wft)
- lek melden bij NCSC (ICT-inbreuk)

stappen om over na te denken

- inventarisatie
  - systeemfuncties en gegevensgroepen
- maatregelen
  - risico's en prioritering
  - wettelijke plichten
  - afspraken met leveranciers
  - educatie, awareness
  - ontwikkel beleid (handboek)

C. PROFILERING & PRIVACYREGELS

welke voorbeelden van profiling kent u…?

betaalgegevens

- Omdat u altijd op tijd uw rekeningen betaalt krijgt u een aantrekkelijke rente op uw doorlopend krediet
- U pint op Schiphol 500 USD en ontvangt een SMS met een aanbieding voor een prima reisverzekering
- U bestelt anderhalve kuub tuinaarde bij het tuincentrum en ontvangt een aanbieding voor bloembollen van een tuinspeciaalzaak
- Een minderjarige scholier koopt een vliegticket (enkele reis) naar Adiyaman in Oost Turkije. De bank informeert de ouders (en inlichtingen-diensten)

ING

Rasterfahndung

RAF-terrorists use cash and pay their electricity bill in person at the utility (to keep their apartments associated with a false name)

'no-fly list'

Binnen de wereld van beveiliging zijn gegevensprofielen niets bijzonders, maar wat er met die profielen gebeurt, onttrekt zich aan onze waarneming. [W]anneer de Staat ongebreidelde gegevens verzamelt ter bescherming van de nationale veiligheid, kan dit leiden tot niet gerechtvaardigde en uiteindelijk niet rechtens toelaatbare 'zwarte lijsten'. […]

[B]ekend is dat de Amerikaanse senator Ted Kennedy op de 'no-fly list' stond en daarom meerdere malen […] de toegang tot het vliegtuig is geweigerd.

Borking 2010

Big Data in de sportwereld

Peter Blangé, ex-international en bondscoach van het Nederlands volleybalteam, vertelt op IT Innovation Day over het gebruik van IT in de (top-)sport. Het digitaal analyseren van het eigen team, de spelers en het team van de tegenstander is niet meer weg te denken in de topsport. Talenten worden al op vroege leeftijd gevolgd om zo hun prestaties te meten, te vergelijken en te sturen..

Obama

…those interactions produced data that streamed back into Obama's servers to refine the models pointing volunteers toward the next door worth a knock. The efficiency and scale of that process put the Democrats well ahead when it came to profiling voters…

PvdA

Aan de deur krijgen Rotterdammers een roos en worden vragen gesteld. Wie interesse heeft in de PvdA kan op de hoogte worden gehouden. "Je kunt zo een database opbouwen," zegt bestuurskundige en PvdA-lid Kirsten Verdel, die in de Verenigde Staten ervaring met de methode heeft opgedaan in het campagneteam van Obama.

ethnic profiling

- *stopping or detaining the driver of a vehicle based on the determination that a person of that race, ethnicity, or national origin is unlikely to own or possess that specific make or model of vehicle*
- *stopping or detaining an individual based on the determination that a person of that race, ethnicity, or national origin does not belong in a specific part of town or a specific place*

'online profiling or behavorial advertizing'

- *advertising based on observation of behavior of individuals over time*
- *seeks to study characteristics of this behaviour through actions*
- *to develop a specific profile and provide these individuals with advertisements tailored to their interests*

i.e. site visits, interactions, keywords, online content production, etc.

credit score ('kredietscore')

- a numerical expression based on a level analysis of a person's credit files, to represent the creditworthiness of the person.
- primarily based on a credit report information typically sourced from credit bureaus.
- to evaluate the potential risk posed by lending money to consumers and to mitigate losses due to bad debt

zoekresultaten

Verder kan de door de zoekmachines verrichte ordening en samenvoeging van de op het internet gepubliceerde informatie, teneinde de gebruikers van deze machines gemakkelijker toegang tot deze informatie te verschaffen, ertoe leiden dat, wanneer deze gebruikers op de naam van een natuurlijke persoon zoeken, zij via de resultatenlijst een gestructureerd overzicht krijgen van de over deze persoon op het internet vindbare informatie, waardoor zij een min of meer gedetailleerd profiel van de betrokkene kunnen opstellen.

HvJEU 13 mei 2014, C-131/12 (Google Spain)

uithuisplaatsing

In die tijd, de post-Savannah-periode, ontstond de sterke neiging om maar bij de minste twijfel te handelen. Beter een kind te veel uithuisgeplaatst, dan nogmaals een Savannah, hoorde ik een jeugdzorg-directeur zeggen.

De aanleiding voor de uithuisplaatsingen was niet een calamiteit, zelfs geen incident, maar een risicoprofiel: de moeder was getraumatiseerd door een oorlogsverleden in een ander land, en de vader gebruikte trouw medicijnen voor een ggz-diagnose, waardoor de ziekte onder controle was.

Justine Pardoen
De risico-regelreflex
31 januari 2015
www.ouders.nl

'Bulgaarse zakkenrollers'

„Bulgaarse zakkenrollers herken je nog wel", zegt een van de agenten. „Aan de hak van hun schoen, afgesleten van het lopen." Maar die Chilenen, poeh, dat is het elitegilde van de zakkenrollerij. En nee, zegt hij er meteen achteraan, dat is geen discrimineren. „Dat heet gewoon profiling"

NRC HANDELSBLAD

'digitale predestinatie'

In 2014 had het CBP speciale aandacht voor profilering. […] Via tracking cookies kunnen organisaties grote hoeveelheden persoonsgegevens verzamelen. Door deze analyseren en te combineren kunnen ze profielen toekennen aan doelgroepen en deze anders behandelen of gerichter benaderen.

'Dat kan prettig zijn,' aldus het CBP: 'Als mensen daarover tenminste worden geïnformeerd en zelf een keuze hebben kunnen maken. Maar het kan voor hen ook ongunstige gevolgen hebben.'

wat is «profiling»…?

- *verzamelen, analyseren en combineren van (persoons) gegevens met als doel iemand in te delen in een bepaalde categorie*
- *met profilering kan een organisatie ook het gedrag van mensen voorspellen of een beslissing over hen nemen.*
- *profilering wil dus zeggen dat iemand aan de hand van een (risico)profiel wordt beoordeeld.*
- *profilering brengt privacyrisico's met zich mee. Bijvoorbeeld dat iemand anders wordt behandeld*

cbpweb.nl

profiling *(~ prō'fil'ing)*

any form of automated processing of personal data intended

- *to evaluate certain personal aspects relating to a natural person or*
- *to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour*

European Parliament 22 October 2013

any form of automated processing of personal data consisting of using those data

- *to evaluate personal aspects relating to a natural person,*
- *in particular to analyse and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movement*

Council General Approach

voorstellen

Commission
- right not to be subject to measures based solely on automated processing intended to profile…

European Parliament
- right to object to profiling,
- to be informed about that right in a highly visible manner

Council
- right not to be subject to decision based solely on automated processing, incl. profiling

EDPS
- right not to be subject to measures based solely or predominantly on profiling
- informed about that right in a manner clearly distinguishable from other matters

which produces legal effects or significantly affects him or her…

suggested rules…

- less focus on the results of profiling, more on the process of profiling
- only to be allowed with explicit consent (and nothing else)
- access and modification rights, incl. right to delete profile information and to refuse any measure based on profiling
- higher degree of responsibility and accountability with respect to profiling
- EDPB to issue guidelines on interpretation and application of the rules

Advice paper on essential elements of a definition and a provision on profiling within the EU GDPR - 13 May 2013

The Council's proposal is especially inadequate, because, like [the current rules], it reduces the phenomenon of profiling to decisions based on automated processing and having legal effects for individuals.

This only covers a specific result of data processing in connection with the evaluation of personality features, but not the fundamental question of what purposes and within what boundaries personality profiles may be created and used at all.

Conference of the Data Protection Commissioners of the Federal Government and the Federal States (Länder)
14 August 2015

Someone must have been telling lies about Josef K., he knew he had done nothing wrong but, one morning, he was arrested.

Mr. Marks, by mandate of the District of Columbia Precrime Division, I'm placing you under arrest for the future murder of Sarah Marks and Donald Dubin that was to take place today, April 22 at 0800 hours and four minutes.

@zwnne

g.j.zwenne@law.leidenuniv.nl

DANK VOOR UW AANDACHT!