

## **Stellingen behorende bij het proefschrift Privacyrecht is Code, Over het gebruik van Privacy Enhancing Technologies van John Borking**

1. Omgevingsanalyse toont aan dat door de toenemende informatisering privacy problemen zullen toenemen ( Hoofdstuk 1)
2. De wetsartikelen die direct betrekking hebben op de verwerking van persoonsgegevens zijn de juridische specificaties voor het ontwerp van informatiesystemen (Hoofdstuk 2)
3. Door de inzet van informatiesystemen, die van gegevensontdekkende-, gegevensvolgende- en gegevenskoppelende technologieën gebruikmaken, erodeert de privacy van de burger in onze risico-toezichtmaatschappij ernstig. (Hoofdstuk 3)
4. De bepaling in artikel 17 van 95/46/EG en het daarvan afgeleide artikel 13 Wbp “(...) gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen”, impliceert dat een privacyrisico analyse voorafgaande aan het gebruik van informatiesystemen wettelijk vereist is. (Hoofdstuk 4)
5. De pentagonale risicoanalyse, die in het EU PISA project is toegepast en de privacy bedreigingsontologie gebaseerd op de methode van Little & Rogova bieden de beste mogelijkheden om zo volledig mogelijk privacyrisico’s en bedreigingen in kaart te brengen. (Hoofdstuk 4)
6. Standaard dient een transparante privacyrisico analyse te worden uitgevoerd voordat een surveillance systeem in gebruik wordt genomen. (Hoofdstuk 3 en 4)
7. In het concept van Privacy Enhancing Technologies (PET), zorgen de identiteitsbeschermer (Identity Protector) met de scheiding van gegevens en identiteitsdomeinen en pseudo-identiteitendomeinen voor adequate bescherming van persoonsgegevens in verwerkingsprocessen online en offline. (Hoofdstuk 5)
8. Een objectieve, methodologische privacyrisico analyse en het gebruik van PET moet wettelijk worden voorgeschreven (hoofdstuk 4,5,8)
9. Vooral in het proces van het gegevens verzamelen is de potentiële effectiviteit van PET het grootst omdat hier de privacy bescherming van de persoonsgegevens aan de bron plaatsvindt. (Hoofdstuk 6)
10. Informatiesystemen moeten zo worden ingericht dat wanneer een onbevoegde een identificerend gegeven in een informatiesysteem vindt, de overige persoonlijke informatie niet automatisch gekoppeld kan worden aan dat identificerende gegeven en omgekeerd. Als er een gegeven door een onbevoegde wordt gevonden mag dat niet leiden tot identificatie van degene waar dat gevonden gegeven bij hoort. (Hoofdstuk 6)
11. Aan de hand van de Diffusion of Innovation (DOI) theorie van Rogers kunnen de positieve en negatieve factoren voor organisaties worden vastgesteld, die van invloed zijn op de adoptie van PET voor de bescherming van persoonsgegevens. (hoofdstuk 7)

12. Goede business modellen met betrekking tot PET-investeringen ontbreken. Wel is er een aantal *Return On Investment* (ROI) formules beschikbaar, die de economische rechtvaardiging voor PET investeringen kunnen onderbouwen. (hoofdstuk 7)

13. Het verdient aanbeveling om de verantwoordelijke manager aansprakelijk te stellen voor privacyinbreuken zoals dat in de Sarbanes-Oxley Act gebeurt voor de financiële verslaglegging. (Hoofdstuk 8)

14. Ter bescherming van de privacy in de *ambient intelligence* (AMI) omgeving dient het individu standaard zijn persoonlijke ruimte elektronisch te kunnen afschermen (vergelijkbaar met een kooi van Faraday) om inkomende elektronische signalen van hem omringende RFIDs en sensors te kunnen beoordelen.

15. Als iedere volwassene tenminste een van zijn dromen per dag zou analyseren, dan zou de zin van zijn leven hem aanmerkelijk duidelijker worden.