# De overheid als verschaffer en beschermer van digitale identiteiten

*B. Jacobs*

## 1. Inleiding

Dit artikel zal ingaan op twee actuele vragen.

1 Is het een taak van de overheid in Nederland om haar burgers te voorzien van een betrouwbare digitale identiteit, vergelijkbaar met de taak van het verschaffen van paspoorten en identiteitskaarten in de gewone, niet-digitale wereld?
2 Is het een taak van de overheid om burgers te beschermen in de onlinewereld, bijvoorbeeld tegen digitale aanvallen of tegen de verzamelzucht van de grote informatiegiganten van deze tijd?

Deze twee vragen hangen in zekere mate samen. Het antwoord op de eerste vraag zou kunnen zijn: 'Nee, deze taak kan het beste worden overgelaten aan het bedrijfsleven', vanuit de gedachte dat de overheid zich beter niet met de digitale wereld kan bemoeien. Daarmee is in feite ook een antwoord op de tweede vraag gegeven. Ook is het zo dat veel van de activiteiten van de informatiegiganten erop gericht zijn om in detail te weten te komen wie hun gebruikers zijn, om gedetailleerde profielen op te kunnen bouwen. Die profielen worden vervolgens gebruikt voor persoonlijke advertenties en voor prijsdifferentiatie. In dat laatste geval krijgen verschillende mensen verschillende prijzen voor hetzelfde product voorgehouden, gebaseerd op het opgebouwde profiel. Bij eventuele bescherming van burgers zal hun online-identiteit daarom een centrale rol spelen.
Uiteindelijk behelst het antwoord op bovenstaande twee vragen een politieke keuze. Dit artikel zal niet ontkomen aan dit politieke perspectief. Het beoogt echter vooral om deze vragen inhoudelijk te onderbouwen en in een bredere context te plaatsen, om tot een beter gemotiveerd antwoord te komen.

## 2. Registratie en authenticatie bij de overheid

Ruwweg kan men zeggen dat overheden in continentaal Europa pas onder napoleontische invloed begonnen zijn de identiteiten van burgers systematisch te registreren. De militaire dienstplicht vormde daarbij een belangrijke motivatie. De registraties ontwikkelden zich als basis voor een geheel van plichten en rechten voor burgers. In het hedendaagse Nederland staat de Basisregistratie Personen (BRP)[1] aan de basis van de vastlegging. Bij aangifte van geboorte wordt in deze BRP een nieuwe persoon toegevoegd. De BRP vormt de basis voor rechten en

1 Deze BRP is een samenvoeging van wat eerder de Gemeentelijke Basisadministratie Personen (GBA) en het Register Niet-Ingezetenen (RNI) heette.

plichten, zoals stemrechten, eventuele rechten op uitkering, toelage of onderwijs, belastingplichten, rechten op paspoort en/of identiteitskaarten, enzovoort. Via deze BRP voorziet de overheid de burger van een 'bronidentiteit', die de basis vormt voor eventuele andere identiteiten bij een bank, telecombedrijf, enzovoort.
Sinds 2007 is het burgerservicenummer (BSN) een belangrijk onderdeel van deze registratie binnen het Nederlandse overheidsdomein. Via het BSN worden verschillende registraties binnen de overheid (en aanpalende gebieden, zoals de zorg) aan elkaar gekoppeld. Op basis van het BSN weten overheidsinstanties met wie ze van doen hebben. Het BSN vormt dan ook de kern van elektronische authenticatiemiddelen zoals DigiD. Dit werkt als volgt. Stel, ik ga als burger naar de website van mijn gemeente, bijvoorbeeld om een uittreksel van mijn geboorteregister aan te vragen. Op deze gemeentelijke website word ik doorgeleid naar de centrale authenticatiedienst van DigiD. Daar authenticeer ik mijzelf, dat wil zeggen, daar bewijs ik wie ik ben, ofwel via mijn loginnaam en wachtwoord, ofwel via een eenmalig sms-code. Vervolgens stuurt de DigiD-centrale een bericht naar mijn gemeente van de volgende vorm: 'met zekerheidsniveau X hebben wij vastgesteld dat het hier gaat om een burger met BSN Y'. Vervolgens kan de gemeente op basis van dit BSN Y mijn dossier opzoeken en mij de gevraagde dienst verschaffen.
Bij deze centrale authenticatiedienst van DigiD 'weet' men dus waar ik allemaal naartoe ga: hier worden uitgebreide 'logs' bijgehouden van wie op welk moment welke website bezoekt. Men weet daar of, en wanneer, ik online contact heb met bijvoorbeeld het donnorregister, de SVB, de politie, een ziekenhuis, enzovoort. Deze informatie is natuurlijk privacygevoelig. Omdat het gebruik van DigiD beperkt is tot het overheidsdomein wordt de informatie die op deze manier bij DigiD als centrale hub verkregen wordt echter als minder gevoelig beschouwd. Verder worden deze 'metagegevens' bij DigiD primair voor antifraudemonitoring gebruikt, en worden ze niet commercieel verhandeld.

DigiD is in zekere zin een succesverhaal en een belangrijk onderdeel van de Nederlandse *eGovernment*-praktijk. Veel burgers gebruiken DigiD met enige regelmaat voor hun contact met de overheid. Verschillende Europese landen hebben authenticatiediensten opgezet voor hun burgers, bijvoorbeeld met chipkaarten, maar weinige daarvan hebben een mate van gebruik gerealiseerd zoals in Nederland. Het succes van DigiD is tegelijkertijd de zwakte ervan. DigiD is een laagdrempelig systeem, waarbij loginnaam en wachtwoord in veel situaties voldoende zijn. Later is een sterkere vorm van authenticatie in de vorm van eenmalige codes per sms toegevoegd. Maar 'sterk' is DigiD-authenticatie niet te noemen, bijvoorbeeld omdat er bij uitgifte geen face-to-face-controle plaatsvindt. Wanneer ik een week op de plantjes van een buurtgenoot pas, kan ik makkelijk in diens naam een nieuwe DigiD aanvragen. Ik heb daar slechts enkele persoonsgegevens voor nodig – die daar in huis vast wel te vinden zijn – en ik moet de post kunnen onderscheppen.
Oorspronkelijk was het de bedoeling aan DigiD een derde authenticatieniveau toe te voegen, via een persoonlijke chipkaart. Ondanks enkele pogingen is het daartoe nog niet gekomen. De urgentie voor de overheid is echter alleen maar toegenomen, niet alleen vanwege de voorgenomen ambities op het gebied van

*eGovernment*, maar ook vanwege de grote afhankelijkheid die inmiddels ontstaan is van een systeem met relatief zwakke authenticatie.

## 3. Nieuwe elektronische identiteit

Op dit moment is er een nieuwe poging gaande in Nederland om een sterk authenticatiemiddel in te voeren, onder de naam eID, voor: elektronische identiteit. Vanuit de samenleving wordt gevraagd: overheid, zorg niet alleen voor jezelf, maar introduceer a.u.b. een middel dat ook door private partijen gebruikt kan worden om klanten online te authenticeren. Burgers zijn ook gebaat bij eenvoud en overzichtelijkheid, waarbij ze niet voor elk bedrijf waarmee ze van doen hebben een eigen authenticatiemethode moeten gebruiken.
Deze vraag om breed gebruik is volkomen terecht, maar vormt een mijnenveld, omdat (1) de *security*- en privacyeisen volledig verschillend zijn zodra private partijen meedoen, en (2) allerlei andere belangen mee gaan spelen, zoals: wie mag waar geld voor vragen, wie kan wiens techniek en middelen gebruiken, en – misschien wel het belangrijkste belang – wie krijgt toegang tot welke datastromen? De overheid slaagt er vooralsnog niet goed in zich in dit mijnenveld staande te houden. Hieronder zullen deze twee aspecten kort besproken worden.

Ten aanzien van het eerste punt: laten we als gedachte-experiment de huidige DigiD uitbreiden naar het bedrijfsleven. Dit lijkt een voor de hand liggende aanpak. Een direct probleem is dat het BSN niet buiten de overheid gebruikt mag worden. Laten we daar in ons experiment geen probleem van maken, en dit BSN door een ander uniek bepalend nummer vervangen, zeg het klantenservicenummer (KSN). De nieuwe DigiD kan dan functioneren zoals hierboven beschreven: klant X gaat naar de website van bedrijf Y en wordt voor authenticatie doorgestuurd naar de nieuwe DigiD; van daaruit ontvangt bedrijf Y een bericht 'dit is de persoon met KSN KX'. Bedrijf Y kan nu in de eigen database informatie over de klant met KSN KX opzoeken, en daarop het verdere contact baseren. Probleem opgelost! Of toch niet?
Echter, als ik met hetzelfde unieke nummer online boodschappen doe bij de slijter, dit gebruik voor de apotheek, de videoverhuurder, mijn sociale netwerk en mijn verzekering, dan kunnen al deze transacties onderling gekoppeld gaan worden. Een advertentiebureau kan bijvoorbeeld voor verschillende bedrijven de transacties met het nummer KX gaan bijhouden en daarmee een uitgebreid profiel samenstellen en verkopen. Burgers raken hierdoor in detail traceerbaar. Vanuit privacyperspectief is dit volstrekt onaanvaardbaar. Google en Facebook, om maar een paar bedrijven te noemen, zouden met zo'n universeel KSN de middelen in de schoot geworpen krijgen om de Nederlandse burgers nog intensiever en breder te volgen.
Dit probleem geldt niet alleen voor een eventuele uitbreiding van DigiD. Elk nieuw authenticatiemiddel, zoals een chipkaart of een mobiele telefoon, dat door zowel overheid als bedrijfsleven gebruikt wordt, zal geen uniek bepalende informatie kunnen bevatten die door alle partijen uitgelezen kan worden. Dit is een

elementaire constatering, die belangrijke technische en organisatorische consequenties heeft.

## 4. Het belang van context

Maar wat kan dan wel bij een authenticatiemiddel dat breed gebruikt moet gaan worden? We kunnen niet anders concluderen dan dat authenticatie contextafhankelijk zal moeten werken. Concreet wil dat zeggen dat elke organisatie iets anders te zien krijgt van de houder van het authenticatiemiddel, waardoor mijn transacties bij mijn slijter niet gekoppeld kunnen worden aan mijn transacties bij mijn verzekeraar. Een manier om dit te doen is via pseudoniemen. Zulke pseudoniemen zijn in feite per organisatie verschillende klantnummers. Dit is de oplossing die in de Duitse nationale chipkaart *Neue Personal Ausweis* (NPA) gebruikt wordt: de kaart hanteert per bedrijf een uniek bepalend nummer waarmee de klant een volgende keer alleen bij hetzelfde bedrijf herkend kan worden. Omdat deze pseudoniemen per bedrijf verschillen, is het maken van een onderlinge koppeling onmogelijk.[2]

Maar er zijn meer contextafhankelijke oplossingen behalve pseudoniemen. Als alternatief kan men gebruik maken van attributen in plaats van identiteiten. Attributen zijn eigenschappen van personen, zoals 'boven de 18', 'man', 'woonplaats is …', 'nationaliteit is …', 'BSN is …', 'bloedgroep is …', 'bankrekeningnummer is …', enzovoort. Authenticatie kan met attributen op proportionele wijze plaatsvinden, waarbij alleen die attributen die voor de transactie relevant zijn, getoond worden. Bij een aankoop bij de slijter is alleen het attribuut 'boven de 18' vereist. Als ik verder niks van mijzelf hoef te laten zien, kan de transactie ook nergens aan gekoppeld worden en kan mijn identiteit ook niet gestolen worden. Bij korting in de bus is het attribuut 'boven de 65' relevant. En bij een onlineboekverkoper zijn bijvoorbeeld alleen het bankrekeningnummer (voor betaling), het huisadres (voor fysieke bezorging, als het geen e-boek betreft) of het 'boven de 18'-attribuut (bij bepaalde inhoud) relevant. Via zulke selectieve onthulling van attributen kunnen verschillende *personas* worden ondersteund. Dit is heel natuurlijk. U bent weliswaar een en dezelfde persoon in verschillende situaties, maar u laat andere dingen van uzelf zien bij de huisarts dan bij de hobbyclub. Sterker nog, een essentieel aspect van privacy is dat informatie in context moet blijven:[3] wanneer de medische zaken die u met de huisarts bespreekt bij de hobbyclub opduiken, bent u (terecht) geschokt. Elk elektronisch systeem dat wijd gebruik nastreeft, zal nauw moeten aansluiten bij zulke gevestigde praktijken en verwachtingen. Juist

2 De technische realisatie van deze pseudoniemen heeft nogal wat voeten in aarde. In essentie wordt het pseudoniem berekend uit een combinatie van een kaartnummer en bedrijfsnummer. De kaart moet deze berekening zelf uit kunnen voeren. Het resulterende pseudoniem is in Duitsland kaartafhankelijk. Als gevolg heeft een klant, na vervanging van de kaart, verlies of diefstal, allemaal nieuwe pseudoniemen, die in principe niet gekoppeld kunnen worden aan de oude pseudoniemen. Dit is natuurlijk niet erg handig.

3 Zie bijv. H. Nissenbaum, *Privacy in Context. Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press 2009.

vanwege deze flexibiliteit wordt attribuutgebaseerde authenticatie als een belangrijke ontwikkeling gezien op het vakgebied *identity management*.
De conclusie tot nu toe is dat het voor de overheid relatief eenvoudig is om alleen voor zichzelf een sterk authenticatiemiddel in te voeren, als derde niveau binnen DigiD, maar dat een middel dat ook door private partijen gebruikt kan worden buitengewone zorgvuldigheid vereist om universele traceerbaarheid van burgers te voorkomen. Technieken die daarvoor gebruikt kunnen worden, zijn pseudoniemen en attributen. Er valt veel te zeggen over de verschillen tussen deze twee benaderingen, maar dat valt buiten het bestek van dit artikel.[4]

## 5. De rol van bedrijven

De vraag dient zich aan: moet de overheid dit eigenlijk wel zelf doen, of kan de introductie van zo'n sterk authenticatiemiddel beter aan de markt overgelaten worden? Banken geven bijvoorbeeld ook hun eigen bankpassen uit, waarmee sterkere vormen van authenticatie mogelijk zijn, zoals gebruikt worden bij internetbankieren. Ook zijn er bedrijven die over het hele land verspreide loketten bezitten, waar betrouwbare face-to-face-uitgifte van nieuwe authenticatiemiddelen mogelijk is. Kortom, moet de traditionele rol van de overheid als verschaffer van de bronidentiteit van burgers zich uitstrekken tot het digitale domein?

Een uitstapje naar Angelsaksische landen is verhelderend. In de Verenigde Staten (VS) en in het Verenigd Koninkrijk (VK) bestaan geen (centrale) burgeradministraties zoals in continentaal Europa. Betrouwbare identiteitsvaststelling in de VS is een probleem: er is geen nationale identiteitskaart, slechts weinig burgers hebben een paspoort, en rijbewijzen worden per staat volgens verschillende standaarden uitgegeven (en niet aan alle burgers). Omdat rijbewijzen echter zo wijd verbreid zijn, vormen ze het *de facto*-authenticatiemiddel in de niet-digitale wereld. Ook in de VS is er behoefte aan een betrouwbare digitale identiteit. President Obama heeft daartoe de National Strategy for Trusted Identities in Cyber Space (NSTIC) in het leven geroepen.[5] Het bedrijfsleven speelt daarin een belangrijke rol. Opvallend is dat grote databrokers hun diensten aanbieden. Dit zijn bedrijven, zoals Acxiom, Experian en Datalogix, die jarenlang over grote aantallen mensen systematisch allerlei gegevens verzamelen, hetgeen in de VS op veel grotere schaal toegestaan is dan in Europa. Die bedrijven beweren identiteiten op betrouwbare wijze vast te kunnen stellen. Als er bijvoorbeeld twijfel bestaat, zullen ze je vragen stellen als: welke kleur auto reed u begin jaren negentig? Omdat deze databrokers bijhouden welke auto op welk moment op wiens naam staat (en nog veel meer), hebben ze hier informatie over.
Het moge duidelijk zijn dat in een continentaal-Europese traditie met door overheden beheerde nationale registers en met grondwettelijk verankerde privacy-

4 Tevens is de auteur van dit artikel zelf nauw betrokken bij een van deze twee benaderingen, namelijk attribuutgebaseerde authenticatie, zie <www.irmacard.org>, waardoor hij mogelijk niet degene is met het meest objectieve relaas.

5 Zie de officiële website <http://nist.gov/nstic/>.

rechten een dergelijke houtje-touwtje-identiteitsvaststelling ondenkbaar is. Echter, het is moeilijk voorstelbaar hoe in zo'n Europese traditie welk fatsoenlijk opererend bedrijf dan ook tot een breed vertrouwde, juridisch verankerde identiteitsvaststelling kan komen. Aldus lijkt het voor de hand te liggen dat hier een natuurlijke rol voor de overheid ligt, temeer daar de overheid deze rol van verschaffer van een digitale bronidentiteit zelf van juridische waarborgen en garanties kan voorzien, inclusief gebruik van open standaarden en opensourcesoftware.[6] Het zou de uitgangspunten in de huidige discussie in Nederland verhelderen en versimpelen als de overheid zich deze principiële rol nadrukkelijk toe-eigent. Vermoedelijk is dat, in het licht van de eigen Nederlandse/Europese traditie, weinig omstreden.
(Oorspronkelijk werden informatici slechts gezien als architecten van de digitale wereld. Inmiddels is duidelijk dat ze architecten van de sociale wereld geworden zijn. In de manier waarop we maatschappelijk belangrijke software ontwerpen en vormgeven, worden sociale en culturele waarden zichtbaar. Juist op het gebied van *identity management* is het klakkeloos importeren van oplossingen van buiten gevaarlijk, en is een nauwe aansluiting bij de eigen traditie en gebruiken belangrijk.)

## 6. De rol van de overheid

Hiermee is de eerste vraag aan het begin van dit artikel (positief) beantwoord en komen we toe aan de tweede vraag: heeft de overheid ook een rol om de eigen burgers te beschermen in de digitale wereld? Immers, in de niet-digitale wereld wordt het misschien wel als de belangrijkste overheidstaak beschouwd om de burger te beschermen, bijvoorbeeld tegen misdaad of ook tegen bezetting door een andere mogendheid.
In het digitale domein zijn er velerlei dreigingen, variërend van allerlei vormen van cybercrime (zoals plundering van internetrekeningen, fraude, afpersing) tot commerciële uitbuiting van gegevens en misleiding. Aan de basis van veel van deze dreigingen staat misbruik van de digitale identiteit.[7] De rest van het artikel zal zich daarop concentreren, en daarmee aansluiten bij de bovenstaande bespreking.

In de relatief korte historie van het internet is overheidsbemoeienis omstreden en snel verdacht. Veelal wordt het internet gezien als het domein van grote vrijheden, waar overheden zich vooral verre van moeten houden. Dit beeld wordt

6 Omwille van controleerbaarheid, bruikbaarheid, mogelijkheden voor onafhankelijke innovatie, en om afhankelijkheid en *vendor lock-in* (de onmogelijkheid om van leverancier te veranderen) te voorkomen is het van belang dat de manier waarop door software(programmatuur) met gegevens omgegaan wordt, openbaar is. Dit gebruik van open standaarden is officieel beleid van de Nederlandse overheid. Bij opensourcesoftware is ook de broncode van de programmatuur vrij beschikbaar. Dit wordt door de overheid gestimuleerd, maar niet als norm gesteld, zie <www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-data-en-open-standaarden>.

7 Zie de website <http://gov.nl/identiteitsfraude> van het Centraal Meldpunt Identiteitsfraude voor nadere informatie, inclusief aantallen en soorten meldingen.

niet alleen uitgedragen door de internetpioniers, die vol waren van ideeën over hoe internet mensen vrij zou maken, transparantie zou bevorderen en machtsmisbruik zou uitroeien. Dit beeld is zo naïef gebleken, omdat vooral burgers op internet transparant geworden zijn. Het vrijheidsideaal wordt ook uitgedragen door bedrijven die hun activiteiten op internet liefst zonder regulering van overheden willen kunnen ontplooien, waardoor grote asymmetrie in kennis en macht is ontstaan. Het is zinvol in deze context het begrip vrijheid preciezer te maken, in termen van het door de Britse filosoof Isaiah Berlin geïntroduceerde onderscheid tussen positieve en negatieve vrijheid. Positieve vrijheid betreft 'vrijheid om', die je in staat stelt om aangename dingen te doen, terwijl negatieve vrijheid gaat over 'vrijheid van', die je vrijwaart van onaangename zaken. Een eventuele overheidsrol die hier aan de orde is, betreft vooral deze negatieve vrijheid, gericht op het beschermen van burgers.

De intensieve bemoeienis van de Amerikaanse overheid met internet is de afgelopen jaren duidelijk geworden uit de onthullingen van Edward Snowden. Aangenomen mag worden dat andere overheden vergelijkbare – maar mogelijk technologisch minder geavanceerde – activiteiten ontplooien. Deze onthullingen tonen aan dat overheden wel degelijk intensief actief zijn en ingrijpen op internet. De activiteiten zijn uiteindelijk wel gericht op bescherming van de eigen burgers, maar zullen op individueel niveau misschien niet altijd als zodanig ervaren worden.

Veel minder intensief zijn de overheidsactiviteiten die gericht zijn op het beschermen van burgers tegen grote commerciële partijen. Het zijn vooral de Europese Commissie en de Amerikaanse Federal Trade Commission (FTC) die met enig gewicht grenzen stellen en boetes en beperkingen opleggen. De Nederlandse overheid steekt vooral energie in het bestrijden van cybercrime, maar kent vooralsnog geen traditie van bescherming van eigen burgers tegen commerciële uitbuiting op internet. In het laatste geval wordt snel geroepen dat Nederland weinig kan uithalen op nationaal niveau tegen de grote informatiegiganten, terwijl in het eerste geval bij de aanpak van cybercrime wel degelijk voortvarend nationale wetgeving geïntroduceerd wordt.

In de gewone, niet-digitale wereld is het gebruikelijk dat de wetgever heldere normen en regels stelt. Zo is het in de meeste beschaafde landen verboden dat mensen hun eigen organen verkopen. Dit is een duidelijk betuttelend verbod. Toch is het onomstreden dat mensen op een dergelijke manier tegen zichzelf beschermd worden, zodat zij in een (financieel) kwetsbare situatie niet uitgebuit kunnen worden. Organen worden hiermee nadrukkelijk buiten de handel geplaatst. Is het vanuit dit perspectief onredelijk om te denken aan vergelijkbare beperkingen aan het verhandelen van de eigen medische gegevens of intiemste gedragsgegevens?

Indien de Nederlandse overheid, zoals hierboven gesuggereerd, zich daadwerkelijk de rol toe-eigent om verschaffer van een met waarborgen omklede digitale bronidentiteit te zijn, dan hoort daarbij ook de rol om die digitale identiteit adequaat te beschermen. In de niet-digitale wereld zijn er immers ook velerlei regels en sancties die het gebruik van paspoorten en identiteitskaarten in goede banen moeten leiden, en identiteitsfraude en misbruik moeten voorkomen. Een vergelijkbare rol is nodig in de digitale wereld. Bij een zorgvuldig doordacht authentica-

tiemiddel hoort contextafhankelijk gebruik, om misbruik van de digitale identiteit (bijvoorbeeld via tracering, profilering en prijsdifferentiatie) tegen te gaan. Het is aan de overheid om hier allereerst als wetgever vorm aan te geven. Vanuit het *code is law*-idee[8] moeten die wettelijke normen vorm krijgen binnen de gebruikte technologie. De technische realisatie van de beoogde identiteitsinfrastructuur is daarmee relevant voor de wetgever. Daarnaast zal zij moeten optreden tegen activiteiten die de beoogde bescherming ondermijnen. De Apples, Googles en Facebooks van deze tijd zijn helemaal niet gebaat bij een privacyvriendelijk authenticatiemiddel. Zij willen dat hun gebruikers altijd contextonafhankelijk inloggen en daarmee traceerbaar (en exploiteerbaar) zijn. Indien er een proportioneel authenticatiemiddel beschikbaar is, zal niet-proportionele authenticatie, bijvoorbeeld via Facebooklogins, aan banden gelegd moeten worden. Dit is vergelijkbaar met de beperkingen die de overheid oplegt aan het misplaatste 'kopietje paspoort', om misbruik te voorkomen.

Uiteindelijk is het aan de wetgever om vanuit een heldere visie en met een assertieve houding ook op internet aan 'de publieke zaak' invulling te geven, om de eigen waarden vorm te geven, de zwakkeren te beschermen, en om een *level-playing field* te bewerkstelligen.

8 L. Lessig, *Code and Other Laws of Cyberspace*, New York: Basic Books 1999.