BRONNEN SCHRIJFOPDRACHT VWO6 2011-2012:
Moderne communicatiemiddelen en privacy

bron 1

De stelling van Henk van Ess: mensen laten gevaarlijk veel sporen achter op het web

Gepubliceerd: 14 juni 2008 10:10 | Gewijzigd: 28 juli 2008 13:42

Mensen laten veel meer gevoelige informatie achter op het web dan ze in de gaten hebben, zegt internet-deskundige Henk van Ess tegen Marc Leijendekker. Daarover wordt veel te laconiek gedaan.

We maken ons vaak zorgen over de privacygevoelige informatie in handen van de overheid of van grote organisaties. Maar als het om internet gaat, halen veel mensen vaak hun schouders op en zeggen: wat kunnen mij die paar hits bij Google nu schelen. Is dat terecht, dat mensen daar zo laconiek over doen?
„Nee. Na ruim tien jaar internet zou je denken dat mensen attenter zijn geworden op zoekmachines en dergelijke, dat de kans dat je wordt gevonden, afneemt. Maar het omgekeerde is aan de hand. Op sociale netwerken als hyves en facebook bijvoorbeeld wordt veel meer informatie achtergelaten dan verstandig is. Er zijn mensen die rustig schrijven: mijn vader werkt bij de KLPD, de politie, of bij de AIVD. En ook volwassenen laten steeds meer informatie achter. Uit ijdelheid, loslippigheid, maar ook, en dat is misschien wel de belangrijkste reden, uit onverschilligheid. Voor privacygevoelige informatie is het internet nu een eldorado. Er is nog nooit zo veel te vinden geweest over zo veel mensen."

Hebben mensen dat dan wel goed in de gaten?
„Je laat zonder dat je het weet digitale sporen achter. In een worddocument dat je op internet zet, als cv bijvoorbeeld, zit vaak zonder dat je het in de gaten hebt allerlei informatie die je bij de installatie van je software hebt opgegeven. Of informatie over je werkgever – dat kan een probleem opleveren als je solliciteert. Veel mensen reageren dan meewarig: zo'n snippertje informatie is niet belangrijk. Maar in handen van iemand die er iets mee wil, een stalker, een schuldeiser, een belanghebbende, is het goud. Al die stukjes informatie bij elkaar vormen een geweldige bron.
„Neem een brief over kernenergie die een vorige minister op het internet heeft gezet. Als je dan op de revisieknop klikt, kun je de veranderingen in de tekst zien. En daaruit kon je, in dit geval, weer opmaken dat de steun die de minister in het voltallige kabinet dacht te hebben, er niet was."

Is dit soort trucs niet voor de fijnproevers? De meeste mensen kunnen dit soort informatie toch niet achterhalen?
„Als je het eenmaal weet is het heel simpel. En ook zonder computerachtergrond kun je al heel veel. Via google vind je op dit moment ongeveer 21 procent van de informatie die beschikbaar is op internet. Als je daarnaast twee andere zoekmachines gebruikt die qua kwaliteit concurrent aan het worden zijn van google (zie kader), heb je er zeven miljard andere bronnen bij. Met drie zoekmachines kun je op dit manier vijftig procent van de beschikbare informatie vinden. Voor de andere

helft komt het inderdaad aan op deskundigheid en kennis die een normale particulier niet heeft.”

Je kunt hierdoor misschien in verlegenheid worden gebracht. Maar is dat nu zo alarmerend, al die stukjes informatie?
„Kijk naar het kadaster. Dat verkoopt voor iets meer dan een euro persoonsgegevens aan wie het maar wil hebben. Als burger mag je de gemeentelijke basisadministratie niet in. Maar een op de twee huishoudens in Nederland heeft een eigen huis en zit dus in het kadaster. Op die manier kun je heel makkelijk komen aan adresgegevens, geboortedatum, huwelijkse staat. Allerlei informatie die je bij het gemeenteloket absoluut nooit kunt krijgen, omdat de overheid daar dat soort gegevens afschermt voor de burger.
„Een ander voorbeeld. De overheid heeft registers voor mensen die alcoholproblemen hebben, psychische problemen, of onder curatele staan. Het curatele-register is openbaar, want het is nuttig voor de handel: de Wehkamps van deze wereld moeten kunnen intikken of een persoon wel kredietwaardig is. Het lijkt wel goed beschermd, maar als je op een andere manier, via het kadaster, een geboortedatum weet te achterhalen, kun je langs deze weg heel veel informatie over iemand vinden.
„Een derde voorbeeld. Een bedrijf had een pdf-bestand gemaakt van een powerpointpresentatie en dat op het web gezet. In een verborgen broncode was notabene het hele bedrijfsplan te vinden. In het gemiddelde word- of pdf-bestand op internet vind ik altijd wel een flardje informatie. Dat is al tien jaar zo. Ik vind dat nog steeds alarmerend.”

Dan is de oplossing simpel: gewoon weghalen van de website.
Nee, want dan stuit je op een ander privacyprobleem. Het best bewaarde geheim op internet is de site archive.org. Dat is het kerkhof van internet, de plaats waar oude websites worden bewaard. Je kunt daar bijvoorbeeld informatie vinden waarvan de rechter heeft gezegd dat die van het web moet worden gehaald. Je hebt er wel wat dieperliggende kennis voor nodig en vooral veel geduld, maar je vindt het. Ik krijg steeds meer als vraag niet hoe je hoog in google moet komen, maar hoe je er weer uit komt. Een ex-burgemeester belde mij op, hij had ontslag moeten nemen na een sms’je aan een wethouder waar de honden geen brood van lustten. Op de een of andere manier is de tekst daarvan op een weblog gekomen, en dat is weer te vinden via archive.org. Moet je dan altijd met je verleden worden geconfronteerd?

Historici zouden zeggen: je moet geen bronnen verloren laten gaan.
„Dat is inderdaad de drijfveer achter die site. Maar je moet wel weten om te gaan met al die informatie op het web. Ik heb op een congres van personeelswerkers weleens gevraagd hoeveel van hen google gebruikten om te bepalen of een kandidaat überhaupt langs mocht komen. Iedereen. En hoeveel van hen mensen afwijzen op grond van wat ze vinden op het web. Een kwart. Dat vind ik onverantwoord. Want in hyves worden nu al pestprofielen gemaakt. Een voorbeeld: bij het verzonnen profiel van iemand stond ‘Het liefst drink ik van donderdag tot dinsdag, en op woensdag ga ik dan wel weer aan het werk’. Dan kun je je voorstellen dat, als een personeelsmanager dat voor waar aanneemt, hij dan zegt: we zoeken een fulltimer, die doen we maar niet.”

Het probleem is dus niet alleen wat je zelf achterlaat aan informatie, maar ook wat anderen over jou vertellen, al dan niet waar.
„Ja. Het begint al met de grote doos die flickr.com heet en waar iedereen zijn foto's in stopt. Daar kunnen ook mensen op staan die helemaal niet met hun foto op het web willen."

In het privacydebat gaat het meestal om de bescherming van de burger tegen een alwetende overheid. Maar je hebt nu eigenlijk ook bescherming nodig tegen andere burgers. Hebben juridische garanties en wettelijke maatregelen zin?
„Je kunt op dit moment weinig doen tegen iemand die een vals profiel aanmaakt of jou een tag geeft in een facebook, je naam zet bij die foto. Je zou dan als individueel persoon een vaak Amerikaans bedrijf moeten dwingen om iets weg te halen. Voor de doorsneeburger is dat een enorme stap. Veel sociale netwerken laten dat niet eens toe, en met puur juridische middelen valt dat allemaal niet te handhaven. Maar je kunt wel klagen. Google heeft wel in Nederland extra mensen aangenomen om zoekresultaten te verwijderen als je het er niet mee eens bent dat je wordt gevonden. Dan zie je bijvoorbeeld dat een recensie van een Macintosh-apparaat is weggehaald. Dat is per land anders geregeld. Als je in de Duitse googlesite stormfront.org intikt, een extreem-rechtse site, vind je nul resultaten. Maar de rest van de wereld kan dat weer wel zien. Zo zie je maar dat google een schijnwerkelijkheid laat zien.
„En verder: als er iets op het web staat wat niet klopt, neem dan contact op met de auteur van de website. En als die het niet wil verwijderen, stuur dan een mailtje naar de provider."

We hebben het nu vooral gehad over die kleine stukjes informatie die terecht kunnen komen bij kwaadwillende burgers. Een overheid die de controle wil vergroten, kan daar toch ook enorm veel mee doen?
„Ik moet niet denken aan de dag dat de overheid alle digitale opsporingstechnieken zou beheersen en toepassen. Het is nu eerder nog andersom, dat de overheid digitale sporen achterlaat waarvan mijn grijze haren nog grijzer worden. Bijvoorbeeld een lijst met al het marinepersoneel op Aruba, met naam en adres. Of, op Linkedin.com, de hyves voor de aktetas, vind je mensen die trots beweren dat zij een clearance hebben gehad om te werken voor de AIVD."

Maar 'om misdaad en terreur te bestrijden' moeten providers nu gegevens bewaren over telefoonverkeer en surfgedrag.
„Als dat gebeurt om boeven te vangen heb ik daar op zich minder moeite mee, mits de aansturing door het gerechtelijk apparaat en het opsporingsapparaat goed gebeurt. Maar het gebeurt vaak nog erg nonchalant. Je houdt je hart vast.
En wat ook van belang is, is dat de kennis over digitale trucs iedere dag groeit. Ook bij de boeven. De overheid stelt tegenover die kennis eigenlijk nog te veel mensen op mbo-niveau. We hebben daar slimmere mensen voor nodig, op universitair niveau geschoold."

Juridisch is er dus weinig privacybescherming op internet. Wat moet je nu als gemiddelde surfer doen?
„Je moet je bewust worden van de sporen die je achter kunt laten. Verstuur nooit meer worddocumenten naar wie dan ook, maar zet het bestand om in een ander formaat. Denk niet dat je helemaal anoniem bent met een hotmail- of gmail-account,

want met nieuwe technieken kun je ook zien uit welke plaats die mail komt en nog wat andere zaken. Je moet je in de virtuele wereld gedragen zoals in het echte leven. Laat je thuis de deur ook openstaan? Gooi je je foto's en herinneringen zomaar op de stoep, zodat iedereen ze kan zien? Op het web lijkt dat allemaal wel te kunnen. Mijn belangrijkste regel is: doe op het web niet wat je in het echt ook niet zou doen."

http://vorige.nrc.nl/nieuwsthema/privacy/article1933226.ece

---

bron 2
NRC Handelsblad, zaterdag 26 november 2011
Opinie & Debat, door Danny Mekic'

Facebook kent geen uitgang

Facebook is een nutsvoorziening in wording, meent Danny Mekic'. Als het geen bemoeienis van de overheid wil, moet het zijn gebruikers centraal stellen in plaats van zijn adverteerders.

Herkent u de volgende scène? Waar was u gisteravond? Met wie was u daar? Komt deze foto, welke gisteravond op die locatie gemaakt is, u bekend voor en kunt u de mensen op de foto identificeren? Heeft u een partner? Wie is dat? Wat is uw échte en volledige naam? Op welke datum bent u geboren en in welke plaats gebeurde dat? Wie zijn uw ouders, broers en zussen, neefjes en nichtjes? Wat is uw huidige woon- en verblijfplaats?

Dit is geen politieverhoor. Dagelijks beantwoorden wereldwijd meer dan 800 miljoen mensen deze en andere persoonlijke vragen in ruil voor een hoop reacties, likes en andere vormen van sociale bevestiging op het online sociale netwerk Facebook. Vrijwillig. De internationale profielensite bedient inmiddels een achtste van de wereldbevolking en nestelt zich steeds dieper en heimelijk in de levens van honderden miljoenen mensen, zonder altijd rekening te houden met de privacy van haar gebruikers. Als het Amerikaanse bedrijf daarmee doorgaat, overstijgt het commerciële belang op den duur het publieke belang van de samenleving. Hoe moet de politiek reageren?

Het verdienmodel van Facebook (vier miljard dollar dit jaar) is - net als bij de meeste andere gratis websites - het exploiteren van online advertentieruimte. Voor de advertenties die op Facebookpagina's worden weergegeven, ontvangt Facebook een vergoeding per keer dat zo'n advertentie wordt aangeklikt óf iedere 1.000 keer dat een advertentie wordt weergegeven. De tarieven om op de site te mogen adverteren zijn ondanks de economische malaise de afgelopen 12 maanden met 74 procent gestegen.

Hoe beter een weergegeven advertentie aansluit op de behoefte van de consument, hoe groter de kans is dat de commerciële targets van de adverteerder worden behaald. Dankzij het vrijwillige, met een spervuur aan persoonlijke vragen ingeklede politieverhoor waar Facebookgebruikers dagelijks aan worden blootgesteld, lukt het Facebook iedere dag beter om een allesomvattend beeld te krijgen van meer dan 1 op de 10 wereldburgers en te bepalen welke advertenties in opdracht van de klant, de adverteerder, worden vertoond. Facebook is beter dan welk bedrijf dan ook in staat om relevante advertenties weer te geven bij gebruikers.

Dat product is de Facebookklant, de adverteerder, meer dan veel waard. Kortom, u bent het product.

Door steeds meer en steeds actuelere informatie te verzamelen over zijn gebruikers, krijgt de advertentiegigant een steeds nauwkeuriger beeld van die gebruikers. In 2006 was het nog de Facebookgebruiker die zélf zijn eigen profiel aan moest vullen. Anno 2011 vergaart Facebook het merendeel van de informatie uit de interactie met de gemiddeld 130 Facebookvrienden, en uit de analyse van de online gedragingen van de Facebookgebruiker die op, maar ook buiten Facebook.com stap voor stap wordt gevolgd. Met zo veel informatie over de gebruiker en zijn interesses is het kinderlijk eenvoudig om de juiste advertentie te tonen aan de gebruiker die het meest op de advertentieboodschap zit te wachten. Want als Bachliefhebbers in de meeste gevallen ook gek zijn op het lezen van boeken en GroenLinks-stemmende Parijsliefhebbers het liefst met de Thalys reizen naar de Lichtstad, is niet meer dan een simpele rekensom nodig om de Bol.com-advertentie te tonen aan de Bachliefhebber en de linkse kiezer te verblijden met een kortingsactie, twee minuten nadat deze met het sociale medium heeft gedeeld op zoek te zijn naar een bestemming voor een city trip.

Het gaat de databanksjacheraar al jarenlang voor de wind. Maar de situatie waarbij het grootste deel van de wereldbevolking met toegang tot internet, ook daadwerkelijk actief gebruikmaakt van Facebook is in zicht, en daarmee ook het einde van de groeimogelijkheden van het huidige verdienmodel. Tenzij het de databankexploitant lukt om gebruikers nóg meer informatie te laten delen. Hoe langer een Facebookgebruiker gemiddeld rondstruint, hoe meer informatie over de gebruiker wordt verzameld. Maar ook hoe meer advertenties kunnen worden weergegeven. Meer dan ooit zullen de adverterende Facebookklanten bereid zijn te betalen voor het aan de juiste persoon tonen van hun commerciële boodschap.

Om het product van Facebook, ú dus, een geluksmomentje te bezorgen en de loyaliteit van de miljoenen gebruikers aan het platform kracht bij te zetten, werd twee weken geleden een nieuw ontwerp geïntroduceerd voor de profielpagina's op Facebook, Timeline genaamd. Opvallend is de grote tijdslijn, waar de belangrijkste gebeurtenissen uit het leven van de gebruiker op worden weergegeven. In plaats van iedere stad die de gebruiker heeft bezocht afzonderlijk weer te geven, kiest Facebook er nu bijvoorbeeld voor om een mooie wereldkaart te genereren waarop te zien is waar uw vriend, familielid of collega allemaal is geweest. Wanneer, met wie, en wat hij of zij daar deed.

Met Facebook Timeline is de CERN niet meer nodig om terug de tijd in te gaan: wet wie ging u om in 2011? Wat zijn de plaatsen die u bezocht hebt, en welke foto's maakte u in Berlijn? Hoe vaak bent u met uw ex-partner naar de bioscoop gegaan en wanneer, waar en met wie heeft u Le fabuleux destin d'Amélie Poulain voor het laatst gezien? De nieuwe functionaliteiten maken het gebruik van de website leuker, en zullen de miljoenen gebruikers uitdagen om nóg meer informatie te delen. Het wordt immers automatisch gecategoriseerd en mooi weergegeven in uw online dagboek, waar vrienden, familie en al uw andere Facebookvrienden op kunnen reageren. Iedereen doet immers mee.

Het is moeilijk om Facebook te verlaten. Niet alleen zult u nooit meer in staat zijn uw online dagboek met bijbehorende likes en waardevolle reacties van vrienden en familie in te zien, ook behoudt de website zichzelf het recht toe om foto's, berichten en andere in de loop der jaren verzamelde informatie over uw persoon te blijven gebruiken. De facto kent Facebook geen uitgang. Daar komt bij dat het belang van de sociale netwerksite dagelijks toeneemt, ook omdat bedrijven als ABN Amro,

KLM en Vodafone hun online dienstverlening steeds vaker op de sociale netwerksite plaats laten vinden, en verjaardagsfeestjes en andere evenementen steeds vaker (alleen) op Facebook worden aangekondigd. Daar niet op aangesloten zijn, betekent praktisch gezien een sociaal isolement. Facebook zal alles in het werk stellen om alle internetters aangesloten te krijgen, en bij een zo groot mogelijk deel van hun sociale contacten aan te sluiten, al op zeer jonge leeftijd. U kunt immers nooit meer volledig uitstappen. In de toekomst bestellen we onze boodschappen via Facebook, vertelt de site met welk gerecht u de nieuwe vriendin van uw zoon blij kunt maken, welke stad de volgende vakantiebestemming moet worden en wat u daar zoal kunt doen. Natuurlijk op de zorgvuldig met commerciële motieven uitgezochte voorkeuren van uw beste vrienden en vriendinnen. Over niet al te lange tijd zal de samenleving het punt bereiken waarop het niet langer mogelijk is om als burger te participeren zonder het doorlopend en intensief gebruik van mobiele communicatietechnologieën, het internet en aangemeld te zijn als gebruiker bij Facebook. We praten hier over nutsvoorzieningen in wording.

Het is bijvoorbeeld bijna onmogelijk geworden om te leven zonder telefoon. Oké, u kunt gewoon geen telefoon aanschaffen, maar zult vervolgens constant bevraagd worden voor een telefoonnummer en raar worden aangekeken als u zegt: die heb ik niet. Op dezelfde manier zal het leven in de toekomst bijna onmogelijk worden zonder Facebookprofiel, zoals we eerder zagen met posterijen, het openbaar vervoer, de energievoorziening en drinkwaterleidingen. Wat met die voorzieningen gebeurde? Ze staan allen onder streng toezicht van overheden.

Net als deze nutsvoorzieningen is Facebook ook steeds meer van algemeen nut. Misschien nog wel meer dan in het verleden bij telefonie het geval was.

Dit betekent dat als Facebook niet zit te wachten op politieke bemoeienis - bijvoorbeeld duidelijkere en strengere richtlijnen voor bedrijven als Facebook die als product inbreuk maken op mensen hun privacy - ze ingrijpend iets moet veranderen aan de dienstverlening. De gebruiker en alle over de gebruiker verzamelde gegevens moet op een transparante manier centraal komen te staan, waarbij de absolute controle weer in handen van de gebruiker komt. Waarom geven de Facebooks van deze wereld de informatie eigenlijk niet terug aan de gebruiker? We hebben immers allemaal een internetmodem waar in de toekomst best een beveiligde hardeschijf op aangesloten kan worden. Dan bepalen wij weer wie wanneer wat met onze informatie mag doen. En wanneer we daar mee willen stoppen.

Danny Mekic' is jurist en internetexpert bij New Team.

---

bron 3
The New York Times, 28 mei 2011
Door Jonathan Franzen

Liking Is for Cowards. Go for What Hurts.

A COUPLE of weeks ago, I replaced my three-year-old BlackBerry Pearl with a much more powerful BlackBerry Bold. Needless to say, I was impressed with how far the technology had advanced in three years. Even when I didn't have anybody to call or text or e-mail, I wanted to keep fondling my new Bold and experiencing the marvelous clarity of its screen, the silky action of its track pad, the shocking speed of its responses, the beguiling elegance of its graphics.

I was, in short, infatuated with my new device. I'd been similarly infatuated with my old device, of course; but over the years the bloom had faded from our relationship. I'd developed trust issues with my Pearl, accountability issues, compatibility issues and even, toward the end, some doubts about my Pearl's very sanity, until I'd finally had to admit to myself that I'd outgrown the relationship.

Do I need to point out that — absent some wild, anthropomorphizing projection in which my old BlackBerry felt sad about the waning of my love for it — our relationship was entirely one-sided? Let me point it out anyway.

Let me further point out how ubiquitously the word "sexy" is used to describe late-model gadgets; and how the extremely cool things that we can do now with these gadgets — like impelling them to action with voice commands, or doing that spreading-the-fingers iPhone thing that makes images get bigger — would have looked, to people a hundred years ago, like a magician's incantations, a magician's hand gestures; and how, when we want to describe an erotic relationship that's working perfectly, we speak, indeed, of magic.

Let me toss out the idea that, as our markets discover and respond to what consumers most want, our technology has become extremely adept at creating products that correspond to our fantasy ideal of an erotic relationship, in which the beloved object asks for nothing and gives everything, instantly, and makes us feel all powerful, and doesn't throw terrible scenes when it's replaced by an even sexier object and is consigned to a drawer.

To speak more generally, the ultimate goal of technology, the telos of techne, is to replace a natural world that's indifferent to our wishes — a world of hurricanes and hardships and breakable hearts, a world of resistance — with a world so responsive to our wishes as to be, effectively, a mere extension of the self.

Let me suggest, finally, that the world of techno-consumerism is therefore troubled by real love, and that it has no choice but to trouble love in turn.

Its first line of defense is to commodify its enemy. You can all supply your own favorite, most nauseating examples of the commodification of love. Mine include the

wedding industry, TV ads that feature cute young children or the giving of automobiles as Christmas presents, and the particularly grotesque equation of diamond jewelry with everlasting devotion. The message, in each case, is that if you love somebody you should buy stuff.

A related phenomenon is the transformation, courtesy of Facebook, of the verb “to like” from a state of mind to an action that you perform with your computer mouse, from a feeling to an assertion of consumer choice. And liking, in general, is commercial culture’s substitute for loving. The striking thing about all consumer products — and none more so than electronic devices and applications — is that they’re designed to be immensely likable. This is, in fact, the definition of a consumer product, in contrast to the product that is simply itself and whose makers aren’t fixated on your liking it. (I’m thinking here of jet engines, laboratory equipment, serious art and literature.)

But if you consider this in human terms, and you imagine a person defined by a desperation to be liked, what do you see? You see a person without integrity, without a center. In more pathological cases, you see a narcissist — a person who can’t tolerate the tarnishing of his or her self-image that not being liked represents, and who therefore either withdraws from human contact or goes to extreme, integrity-sacrificing lengths to be likable.

If you dedicate your existence to being likable, however, and if you adopt whatever cool persona is necessary to make it happen, it suggests that you’ve despaired of being loved for who you really are. And if you succeed in manipulating other people into liking you, it will be hard not to feel, at some level, contempt for those people, because they’ve fallen for your shtick. You may find yourself becoming depressed, or alcoholic, or, if you’re Donald Trump, running for president (and then quitting).

Consumer technology products would never do anything this unattractive, because they aren’t people. They are, however, great allies and enablers of narcissism. Alongside their built-in eagerness to be liked is a built-in eagerness to reflect well on us. Our lives look a lot more interesting when they’re filtered through the sexy Facebook interface. We star in our own movies, we photograph ourselves incessantly, we click the mouse and a machine confirms our sense of mastery.

And, since our technology is really just an extension of ourselves, we don’t have to have contempt for its manipulability in the way we might with actual people. It’s all one big endless loop. We like the mirror and the mirror likes us. To friend a person is merely to include the person in our private hall of flattering mirrors.

I may be overstating the case, a little bit. Very probably, you’re sick to death of hearing social media disrespected by cranky 51-year-olds. My aim here is mainly to set up a contrast between the narcissistic tendencies of technology and the problem of actual love. My friend Alice Sebold likes to talk about “getting down in the pit and loving somebody.” She has in mind the dirt that love inevitably splatters on the mirror of our self-regard.

The simple fact of the matter is that trying to be perfectly likable is incompatible with loving relationships. Sooner or later, for example, you’re going to find yourself in a hideous, screaming fight, and you’ll hear coming out of your mouth things that you

yourself don't like at all, things that shatter your self-image as a fair, kind, cool, attractive, in-control, funny, likable person. Something realer than likability has come out in you, and suddenly you're having an actual life.

Suddenly there's a real choice to be made, not a fake consumer choice between a BlackBerry and an iPhone, but a question: Do I love this person? And, for the other person, does this person love me?

There is no such thing as a person whose real self you like every particle of. This is why a world of liking is ultimately a lie. But there is such a thing as a person whose real self you love every particle of. And this is why love is such an existential threat to the techno-consumerist order: it exposes the lie.

This is not to say that love is only about fighting. Love is about bottomless empathy, born out of the heart's revelation that another person is every bit as real as you are. And this is why love, as I understand it, is always specific. Trying to love all of humanity may be a worthy endeavor, but, in a funny way, it keeps the focus on the self, on the self's own moral or spiritual well-being. Whereas, to love a specific person, and to identify with his or her struggles and joys as if they were your own, you have to surrender some of your self.

The big risk here, of course, is rejection. We can all handle being disliked now and then, because there's such an infinitely big pool of potential likers. But to expose your whole self, not just the likable surface, and to have it rejected, can be catastrophically painful. The prospect of pain generally, the pain of loss, of breakup, of death, is what makes it so tempting to avoid love and stay safely in the world of liking.

And yet pain hurts but it doesn't kill. When you consider the alternative — an anesthetized dream of self-sufficiency, abetted by technology — pain emerges as the natural product and natural indicator of being alive in a resistant world. To go through a life painlessly is to have not lived. Even just to say to yourself, "Oh, I'll get to that love and pain stuff later, maybe in my 30s" is to consign yourself to 10 years of merely taking up space on the planet and burning up its resources. Of being (and I mean this in the most damning sense of the word) a consumer.

When I was in college, and for many years after, I liked the natural world. Didn't love it, but definitely liked it. It can be very pretty, nature. And since I was looking for things to find wrong with the world, I naturally gravitated to environmentalism, because there were certainly plenty of things wrong with the environment. And the more I looked at what was wrong — an exploding world population, exploding levels of resource consumption, rising global temperatures, the trashing of the oceans, the logging of our last old-growth forests — the angrier I became.

Finally, in the mid-1990s, I made a conscious decision to stop worrying about the environment. There was nothing meaningful that I personally could do to save the planet, and I wanted to get on with devoting myself to the things I loved. I still tried to keep my carbon footprint small, but that was as far as I could go without falling back into rage and despair.

BUT then a funny thing happened to me. It's a long story, but basically I fell in love with birds. I did this not without significant resistance, because it's very uncool to be a

birdwatcher, because anything that betrays real passion is by definition uncool. But little by little, in spite of myself, I developed this passion, and although one-half of a passion is obsession, the other half is love.

And so, yes, I kept a meticulous list of the birds I'd seen, and, yes, I went to inordinate lengths to see new species. But, no less important, whenever I looked at a bird, any bird, even a pigeon or a robin, I could feel my heart overflow with love. And love, as I've been trying to say today, is where our troubles begin.

Because now, not merely liking nature but loving a specific and vital part of it, I had no choice but to start worrying about the environment again. The news on that front was no better than when I'd decided to quit worrying about it — was considerably worse, in fact — but now those threatened forests and wetlands and oceans weren't just pretty scenes for me to enjoy. They were the home of animals I loved.

And here's where a curious paradox emerged. My anger and pain and despair about the planet were only increased by my concern for wild birds, and yet, as I began to get involved in bird conservation and learned more about the many threats that birds face, it became easier, not harder, to live with my anger and despair and pain.

How does this happen? I think, for one thing, that my love of birds became a portal to an important, less self-centered part of myself that I'd never even known existed. Instead of continuing to drift forward through my life as a global citizen, liking and disliking and withholding my commitment for some later date, I was forced to confront a self that I had to either straight-up accept or flat-out reject.

Which is what love will do to a person. Because the fundamental fact about all of us is that we're alive for a while but will die before long. This fact is the real root cause of all our anger and pain and despair. And you can either run from this fact or, by way of love, you can embrace it.

When you stay in your room and rage or sneer or shrug your shoulders, as I did for many years, the world and its problems are impossibly daunting. But when you go out and put yourself in real relation to real people, or even just real animals, there's a very real danger that you might love some of them.

And who knows what might happen to you then?

Jonathan Franzen is the author, most recently, of "Freedom." This essay is adapted from a commencement speech he delivered on May 21 at Kenyon College

---

bron 4
NRC Handelsblad, zaterdag 8 oktober 2011
Opinie & Debat, door Guido van Diepen en Ad Lagendijk

Maak alle ict-beveiliging openbaar

Eer de hacker die een lek in computerbeveiliging vindt, stellen Guido van Diepen en Ad Lagendijk.

Het fiasco met DigiNotar, waarbij voor de zoveelste keer burgers het slachtoffer zijn van internetcriminelen, is geen incident. De ict-blunders bij de overheid volgen elkaar op. De projecten zijn grootschalig, duur en roepen veel ergernis op. Het C2000-communicatiesysteem voor politie, brandweer en ambulancepersoneel, dat in noodsituaties regelmatig tekortschiet, zoals bij de ongeregeldheden op het strand van Hoek van Holland, is een flop. De digitalisering van de WAO-administratie, het afgeblazen elektronisch patiëntendossier, DigiD-fraude, ict-mislukkingen bij de gemeente Amsterdam en gelekte overheidsnota's zijn andere voorbeelden uit de afgelopen jaren.

De oplossing die in alle media en door politici wordt voorgedragen, is om meer ict-experts bij de overheid aan te stellen. Deze oproep doet echter vreemd aan in een tijd waarin de overheid zich terugtrekt en de burgers geacht worden problemen zelf op te lossen. In plaats van blikken dure experts open te trekken, komen wij met een andere - uiteindelijk veel goedkopere - aanpak, geheel in stijl van de slogan 'De overheid, dat zijn wij'. Wij pleiten voor een cultuuromslag: maak ict onderdeel van de cultuur. De maatschappij is gebaat bij meer ict-kennis bij de doorsneeburger.
De recente hack bij DigiNotar heeft geleid tot heftige kritiek op de overheid, hoewel het overgrote deel van de Nederlanders geen idee heeft wat een websitecertificaat (X.509v3) is. De burger die de overheid al haar ict-blunders kwalijk neemt, is als de pot die de ketel verwijt dat hij zwart ziet.

Elke dag groeit het aantal handelingen dat via de digitale snelweg gaat: het invullen van de meterstand, betalen van een boete, het bestellen van een nieuwe wasmachine of gewoon bellen. Alles gebeurt steeds meer via het internet. De kennis van de werking ervan is echter nihil. Wat moet je met eentjes en nulletjes als je weet hoe je een foto kunt uploaden naar Facebook? Nog nooit heeft een technologie zich zo diep in onze samenleving genesteld, zonder dat we - op enkele nerds na - weten hoe zij werkt. Dit blinde vertrouwen in de techniek is gevaarlijk. Internetveiligheid ligt niet alleen in goede software, het ligt net zo goed in menselijk gedrag.

Een rijbewijs voor de digitale snelweg verplichten gaat misschien te ver, maar het zou mooi zijn als zo'n rijbewijs net zo vanzelfsprekend wordt als een zwemdiploma. Aangezien basisschoolleerlingen zich al op het internet begeven, is het zaak om het belang van ict-kennis terug te zien in het onderwijs. Wachtwoordles of surfles zouden daarom geen overbodige luxe zijn. Ook is het verstandig om ict-experts wat vaker in het zonnetje te zetten.

Het ontbreken van wettelijke aansprakelijkheid in de ict-sector is niet te vergeten ook een oorzaak van veel problemen. Bij de meeste industriële sectoren is de leverancier verantwoordelijk voor de kwaliteit en veiligheid van zijn product. Auto's met mankementen worden teruggeroepen. Het risico van schade te moeten vergoeden aan gedupeerde klanten dwingt de fabrikanten de veiligheidsaspecten van hun producten hoog op de agenda te zetten.

Maar de makers van software lopen geen enkel risico. De wetgever heeft toegelaten dat de aansprakelijkheid geheel bij de gebruiker is komen te liggen. Nieuwe wetgeving kan deze onbalans herstellen. Wij verwachten dat de toename van kennis bij de burger op termijn zal leiden tot de nodige hervormingen.

Amateurs - met inbegrip van alle Nederlandse banken en het bedrijf Trans Link Systems dat verantwoordelijk is voor de ov-chipkaart - denken dat het geheim houden van de beveiligingsmethode boeven buiten de deur houdt. In werkelijkheid vermindert deze 'security through obscurity' de veiligheid, omdat zwakheden pas naar buiten komen als het systeem is gekraakt en veel onheil al is geschied.

In een beter systeem, genaamd 'security through openness', worden niet de methodes geheim gehouden, maar slechts de sleutels. Aanvallen op het systeem worden gestimuleerd, omdat zwakheden in het ontwerp hierdoor naar boven komen en gerepareerd kunnen worden. De hacker die het lek vindt in het open systeem, wordt beloond. Wij denken dat beter geïnformeerde burgers deze open strategie zullen eisen van hun banken en andere leveranciers van digitale diensten.

De voorgestelde verbeteringen nemen de onveiligheid in het digitale verkeer niet geheel weg. Het blijft ook hier een voortdurende wapenwedloop tussen de enkele kwaden en de vele goeden. Maar op dit moment wordt het de criminelen wel heel makkelijk gemaakt.

Hoe eenvoudig het kan zijn om met enige kennis digitale rampen te voorkomen, zullen we demonstreren aan de hand van DigiNotar. Een websitecertificaat bestaat uit een paar korte regels tekst met het internetadres van de organisatie - bijvoorbeeld http://'bankieren.rabobank.nl' - en het postadres. De certificaatautoriteit ondertekent de korte tekst met een geheime sleutel, wat een certificaat oplevert voor de website-eigenaar - in dit geval Rabobank. Als u naar de betreffende site surft, leest uw browser het websitecertificaat en als deze browser de certificaatautoriteit vertrouwt, ziet u dat terug in het linkerdeel van de adresbalk dat groen kleurt of een slotje weergeeft. U logt dan met een veilig gevoel in, omdat u weet dat http://'bankieren.rabobank.nl' van een organisatie is die in Utrecht zit, 'Rabobank Nederland' heet en niet toebehoort aan een stelletje struikrovers in Nigeria.

Er zijn honderden commerciële partijen, allen met zelfverklaarde betrouwbaarheid, die dergelijke certificaten uitgeven. Wie zou u het meest vertrouwen? (a) het Amerikaanse VeriSign, de wereldmarktleider, die bij verlies van zijn geheime sleutel vele miljarden euro's kwijt is of (b) het piepkleine DigiNotar. Bij beide organisaties worden de certificaten binnen 24 uur geleverd en kosten ze een paar honderd euro per stuk.

De mondige digitale burger zou versteld zijn geweest om te vernemen dat de overheid, voor haar paar honderd benodigde certificaten, de voorkeur gaf aan DigiNotar. De schade die burgers hebben geleden door DigiNotar zal niet worden vergoed, want multinationaleigenaar Vasco heeft onmiddellijk zijn handen afgetrokken van zijn dochteronderneming en faillissement aangevraagd. Van het aanvaarden van wettelijke aansprakelijkheid voor het geblunder is blijkbaar geen sprake. Vasco is trouwens het bedrijf dat verantwoordelijk is voor de veiligheid van het internetbankieren bij de Rabobank.

Guido van Diepen is cultureel antropoloog, gespecialiseerd in nieuwe media. Ad Lagendijk is universiteitshoogleraar UvA, groepsleider FOM-Instituut AMOLF en hoogleraar natuurkunde aan de Universiteit Twente.

---

bron 5
4 november 2011, De Groene Amsterdammer
Door Axel Arnbak van Bits of Freedom (verdedigt digitale burgerrechten)

De bewaarplicht als boegbeeld van onze bevrijding

Het internet en de telefoon brengen ongekende vrijheid, maar scheppen tegelijkertijd onvoorstelbare mogelijkheden voor verregaande controle. Sinds 1 september 2009

beveelt onze overheid telecomaanbieders om al het bel-, sms-, e-mailverkeer en log-in-pogingen van iedere burger op te slaan, ongeacht verdenking. Deze 'bewaarplicht' of 'dataretentie' vormt het boegbeeld van die ambivalentie: internetten en bellen mag, maar de overheid kijkt permanent mee.

Stilaan openbaart zich de impact van deze massale controlemaatregel op de privacy en vrijheid op het internet. Deens onderzoek laat zien dat iedere burger door de bewaarplicht circa 225 keer per dag wordt gemonitord. Iedere zes minuten wordt vastgelegd met wie iemand belde, hoe lang, waar hij was. Inkomende en uitgaande e-mailtjes, sms'jes en mms-berichten vallen eveneens onder de bewaarplicht. 'Wie zijn de anonieme bronnen van die kritische journalist?', 'was u op kerstavond van 17:01:12 tot 17:34:51 bij uw psycholoog?' Door dataretentie ligt het antwoord op dit soort vragen voor het oprapen in de databanken van telefonie- en internetproviders.

Voor het oprapen, omdat deze privé-informatie eenvoudig opgevraagd kan worden door instanties belast met de bestrijding van terrorisme en criminaliteit ('opsporingsdiensten'). De bepalingen in het Wetboek van Strafvordering zijn zo ruim geformuleerd dat in theorie van vrijwel iedereen gegevens kunnen worden opgevraagd. Je hoeft niet 'verdacht' te zijn, de aanduiding 'betrokkenheid' is al voldoende voor een vordering, die niet getoetst wordt door een rechter-commissaris. Dus als uw collega verdacht wordt van de 'heling van een goed' (koopt een fiets op straat, bijvoorbeeld), kan de officier van justitie al uw bel-, sms- en internetverkeer van de afgelopen twaalf maanden inzien. Het wordt zelfs grappig, als we de wet goed bestuderen. Als uw zoon verdacht wordt van het 'gebruiken van een hond als trekkracht' kan de politie al uw telecomverkeer opvragen. Laat die hond voortaan zelf maar uit, u weet nooit wat kleine Max van plan is!

Hoe vaak de opsporingsdiensten onze gegevens opvragen, houdt het ministerie van Justitie geheim. In alle andere Europese lidstaten is deze informatie overigens publiek. In Brussel horen we ondertussen van verschillende bronnen dat Nederland dit aantal opvragingen onlangs als eerste (!) EU-lidstaat aan de Europese Commissie heeft doorgestuurd. Onze overheid vertelt het blijkbaar liever aan Brussel dan aan ons. Dat voorspelt weinig goeds. Het wordt nog mysterieuzer: ook al hoort u achteraf op de hoogte gesteld te worden van die inzage door de politie (de zogenaamde 'notificatieplicht'), dit wordt in de praktijk nooit uitgevoerd. Het respecteren van onze privacy is voor de politie een 'te hoge administratieve last', volgens interne documenten.

Nederlanders wordt vaak naïviteit verweten als het om privacy gaat. Toch blijkt er sprake te zijn van een significante kentering. Uit een recent onderzoek van ECP-EPN, het Nederlandse platform voor de informatiesamenleving, komt zelfs naar voren dat 89 procent van onze bevolking privacy 'belangrijk' vindt, 68 procent vindt het 'erg' dat bedrijven en instanties persoonsgegevens verwerken. Ook jongeren gaan steeds slimmer om met hun privacy: 85 procent schermt bijvoorbeeld zijn Facebook-profiel af. Het is een logische ontwikkeling: na de verwondering over en gewenning aan het internet maken steeds meer gebruikers zich zorgen over hun privacy op internet.

Nu de bewaarplicht een poosje van kracht is, blijkt het structureel monitoren van een half miljard Europeanen bovendien onnodig en ineffectief. Er is geen enkele onafhankelijke studie die aantoont dat dataretentie zorgt voor een veiligere samenleving. Intussen maakten de hoogste rechters in Duitsland en Roemenië resoluut korte metten met deze massale surveillance. Rechters zijn nu eenmaal minder vatbaar voor de reusachtige lobby van opsporingsdiensten, Amerikaanse

inlichtingendiensten en zelfs de auteursrechtenindustrie - die ook belanghebbende was in de Duitse rechtszaak.

De Europese dataretentierichtlijn wordt momenteel geëvalueerd door de Europese Commissie, het is daarmee een brandend actueel vraagstuk. 'We moeten niet de privacy van alle burgers op het spel zetten', zei eurocommissaris mensenrechten Viviane Reding kort geleden in NRC Handelsblad. Ze heeft gelijk. Hopelijk leggen haar collega's in de commissie, onder wie onze eigen Neelie Kroes (Digitale agenda), hun oren bij haar te luisteren en schaffen zij de verplichte opslag van telecommunicatiegegevens af. Zodat wij ons niet op iedere internetter en beller, maar specifiek op verdachten zullen richten.

Want de vrijheid van vijfhonderd miljoen Europeanen staat op het spel. Het internet en informatie- en communicatietechnologie (ICT) bieden ons ongekende handelingsvrijheid, innovatieve diensten en maatschappelijke betrokkenheid. ICT is van alle burgers geworden, al jarenlang 'gedomesticeerd' en verweven met ons dagelijks leven. Het is niet langer alleen een middel om informatie op te zoeken, we zijn vandaag de dag overgeleverd aan ICT voor ons sociale en zelfs emotionele leven - we kunnen en willen niet meer zonder. Verregaande controlemechanismen, die in de offline wereld helemaal niet mogelijk waren, moeten we niet over ons heen laten komen, tenzij ze noodzakelijk zijn.

De Europese evaluatie schept dus een kans voor onze vrijheid en om de ambivalente werking van het internet op onze vrijheid te beperken. Ten slotte, de meerderheid van de Nederlanders is het met ons eens. Laten we de gevolgen van de bewaarplicht voor onze vrijheid en privacy op internet dus omdraaien: niet als schoolvoorbeeld van verregaande controle, maar als boegbeeld van onze bevrijding.

http://www.groene.nl/commentaar/2010-11-04/de-bewaarplicht-als-boegbeeld-van-onze-bevrijding

---

bron 6
zaterdag 17 december 2011
door Marc Chavannes van NRC Handelsblad

Schippers orkestreert iedereen over de elektronische snelweg

Minister Edith Schippers kwam donderdag in de Tweede Kamer met de schrik vrij. Een plafondlamp plofte spontaan naast haar spreekgestoelte neer. Of het even fortuinlijk afloopt met het cosmetisch tot ‘persoonlijk gezondheidsdossier’ omgedoopte elektronisch patiëntendossier (EPD) is de vraag.

Het EPD is uitgegroeid tot een schoolvoorbeeld van Nederlands openbaar bestuur. Hoe een voor de hand liggend idee door ieders goede bedoelingen plus een dosis ondoorzichtig zakendoen verwordt tot een monster. In dit geval een monster dat al meer dan eens definitief is verslagen. Kennelijk zijn de zakelijke belangen te groot.

Het idee dat medische zorg door veel handen en hoofden optimaal wordt verleend als zij van elkaar weten wie wat heeft gedaan, is niet ingewikkeld. De vaak gebruikte schattingen van het aantal vermijdbare sterfgevallen (‘1900 per jaar’) door het ontbreken van zulke informatie zijn natte vingerwerk. Maar mensen hebben natuurlijk meer kans op goede zorg als al hun gegevens beschikbaar zijn. Eind jaren

’90 zaten we volop in de droom dat grote computersystemen ieder vraagstuk zouden oplossen. De automatiseringsbranche beloofde graag wonderen.

Intussen weten we hoe vaak dat is misgegaan. Steeds nieuwe wensen, alles kon, tegen een aanzienlijke meerprijs. Het politie-communicatiesysteem C2000, de gewone informatie-uitwisseling binnen de politie, steeds meer uitkeringen en toeslagen via UWV en Belastingdienst, de OV-chipkaart, het beveiligingscertificaat van DigiNotar, het Digi-D-systeem waarmee burgers het stadhuis en de belastingdienst ‘veilig’ elektronisch kunnen bezoeken. 100-en miljoenen weg.

Geen wonder dat de Tweede Kamer heeft besloten een parlementair onderzoek in te stellen naar de lange reeks van mislukte en kostbare ict-projecten bij de overheid. Ook het EPD staat op de lijst. Extra curieus dat de Kamer vrijwel tegelijkertijd een motie van de VVD’er Mulder aannam waarin de minister van volksgezondheid wordt gevraagd het EPD te redden.

In april stemde de Eerste Kamer unaniem tegen het EPD-wetsontwerp. De Senaat had zich zeer uitvoerig laten voorlichten door een rij deskundigen en was tot de conclusie gekomen dat het in vele jaren ontwikkelde systeem log, achterhaald en onveilig was. Conclusie: begin met de regionale uitwisseling van medische gegevens. Die is verreweg het meest nodig. Wat op dat gebied bestaat rammelt ook, verbeter dat eerst. Zei ook de VVD.

In een poging het voor 300 miljoen opgebouwde landelijk schakelpunt (LSP) te redden probeerden een aantal koepels van zorgverleners in zomer en herfst hun leden zover te krijgen samen de landelijke boedel over te nemen. Huisartsen voelden er in meerderheid niet voor, apothekers waren niet veel enthousiaster. Het einde leek nabij.

Toen gooide de Inspectie voor de Gezondheidszorg (IGZ) een dreigement in de strijd: goede zorg verloopt via elektronische gegevensuitwisseling. Onderbouwing was het rapport Staat van de Gezondheidszorg 2011 dat naar verluidt door een extern bureau werd geschreven. Ook dat leverde geen enthousiasme op bij de mensen die daadwerkelijk zorg verlenen. Dwang spreekt nooit zo aan bij professionals.

Toen greep de minister in met de motie-Mulder, die gerust de motie-Schippers mag worden genoemd. Het indienende Kamerlid toonde deze week in een Kamerdebatje over de miraculeuze wederopstanding van het oude monster niet dat hij wist waar het over ging. Dat gold ook voor het PvdA-lid Kuiken, die haar fractie liet meestemmen met de motie-Schippers – de PvdA bezorgde VVD en CDA zo een meerderheid voor deze ministeriële orkestratie van een lange neus naar de Eerste Kamer en uw privacy.

Nu wetgeving voor het EPD is gestrand in de Senaat, heeft de minister spontane actie ‘uit het veld’ geregeld. Het meer op inhoud en kwaliteit georiënteerde Nederlands Huisartsen Genootschap (NHG) doet niet mee, maar de koepel van huisartsen wel. Net als de apothekersclub en de Nederlandse Patiënten Consumenten Federatie, de gesubsidieerde patiëntenpoedel die al jaren met overheidsgeld pleit voor het EPD van WC Eend.

Grootste verrassing van deze ‘spontane actie’ is dat de zorgverzekeraars meebetalen. Zij mogen niet in de dossiers kijken. Dat is strafbaar, zegt de minister. Maar wie betaalt, bepaalt op den duur natuurlijk. Het bestaande systeem is onder meer onveilig omdat te veel mensen een pas krijgen (die op zichzelf ook weer makkelijk te kraken is). Hoe reageren verzekeringsartsen als de directie een uitdraai vraagt van mensen met een bepaalde aandoening, of juist een blanco medisch strafblad – aantrekkelijk marketingdoelwit?

Nog steeds dramt VWS, nu bij monde van minister Schippers, een centraal systeem door de strot van artsen en andere zorgverleners. Wie niet is aangesloten, krijgt niet vergoed, zeggen nu ook de verzekeraars. Het net sluit zich. Er mag niet geëxperimenteerd worden met echte persoonlijke gezondheidsdossiers (op een usb-stick). Regionale systemen, bekijk het maar. Ons centrale plan of de medische steppe.

Waarom dat erg is? In Engeland is voor nog veel meer geld zo'n centraal systeem vastgelopen. Privacybeloftes gegarandeerd door de onderbemande privacy-waakhond CBP of de IGZ met één ict-er? Lees hoe de voorzitter van de Raad voor Volksgezondheid en Zorg pleit voor de 'weetplicht van de gemeente om zicht te hebben op de gezondheidstoestand van hun inwoners'. Hoe? Via de centrale toverdoos. De gemeentes zijn al lekker bezig met hun project 'Mens Centraal'. Eén zieke gedachte en uw persoonlijke zorgambtenaar staat op de stoep.

Dit verhaal is geplaatst op zaterdag 17 december 2011 om 08:51 uur op
http://weblogs.nrc.nl/opklaringen/2011/12/17/schippers-orkestreert-iedereen-over-de-elektronische-snelweg/