THE WALL STREET JOURNAL.

Het Grote Privacy Debat

Het Is Moderne Handel: Gebruikers van het Web Krijgen net Zoveel als Zij Geven.

iStock Photo

By Jim Harper
Updated Aug. 7, 2010 12:01 a.m. ET

Als je op internet surft, gefeliciteerd! Je maakt deel uit van de informatie-economie. Gegevens verzameld uit uw communicatie en transacties smeren de tandwielen van de moderne handel. Niet iedereen viert dit natuurlijk. Veel mensen zijn bezorgd en ontzet - zelfs geschokt - wanneer ze leren dat 'hun' gegevens brandstof zijn voor het World Wide Web.

Wie verzamelt de informatie? Wat doen ze ermee? Hoe kan dit mij kwaad doen? Hoe stop ik het?

Dit zijn allemaal goede vragen. Maar in plaats van zich te laten gaan in de natuurlijke reactie om 'stop' te zeggen, moeten mensen slim worden en leren hoe ze hun persoonlijke informatie kunnen beheren. Er zijn tal van opties en hulpmiddelen die mensen kunnen gebruiken om privacy te beschermen - en hebbe eigenlijk een verplichting om deze hulpmiddelen te gebruiken. Gegevens over u zijn niet "van u" als u niets doet om ze onder controle te houden. Ondertussen kan een beter begrip over de informatie-economie de vele voordelen van deze economie duidelijk maken.

Het Grote Privacy Debat

Amerikanen worden online gevolgd op nieuwe en geavanceerde manieren. Een debat over de risico's en voordelen, na het “Journal’s What They Know”:

- **Nicholas Carr: The Dangers of Web Tracking**
- **Firms Resist Privacy Regulation**

Het is normaal om bezorgd te zijn over online privacy. Internet is een interactief medium, geen statisch medium zoals televisie. Elk bezoek aan een website stuurt informatie van de gebruiker naar de server voordat de browser informatie binnenhaalt. En de informatie die bezoekers van websites uitzenden kan een openbaring zijn.

De meeste websites volgen gebruikers, met name door het gebruik van cookies, kleine tekstbestanden die op de computers van internetgebruikers worden geplaatst. Sites gebruiken cookies om de inhoud van de site aan te passen aan de verzamelde informatie om zo beter bij de wens van de bezoeker aan te sluiten. En advertentienetwerken gebruiken cookies om informatie over gebruikers te verzamelen.

Een netwerk dat advertenties op veel sites bevat, herkent dat een browser (ofwel de de persoon die deze gebruikt) naar verschillende websites gaat, waardoor het advertentienetwerk een idee krijgt van de interesses van die persoon. Op een site met SUV's geweest? Mogelijk ziet u een SUV-advertentie terwijl u doorgaat met surfen.

De meeste websites en advertentienetwerken ‘verkopen’ geen informatie over hun gebruikers. Bij gericht online adverteren is het bedrijfsmodel, het verkopen van ruimte aan adverteerders – laat gebruikers informatie zien op basis van hun demografie en interesses. Als een advertentienetwerk persoonlijke informatie en contactgegevens zou verkopen, zou dit zijn inkomsten door reclame verminderen en daardoor zijn eigen winstgevendheid ondermijnen.

Sommige mensen houden, om verschillende redenen, niet van dit volgen (*tracking*), Voor sommigen voelt het als een belediging om te worden behandeld als louter een object van commercie. Sommigen vrezen dat gegevens over hun interesses zullen worden gebruikt om hen ten onrechte te discrimineren of om hen uit te sluiten van informatie en kansen die zij zouden moeten kunnen krijgen. Buitensporige aanpassing van de webervaring kan de maatschappij verdelen, geloven sommigen. Als je bijvoorbeeld arm bent of een minderheidsgroep, kan het nieuws, entertainment en commentaar dat je op internet krijgt te zien, verschillen van dat voor anderen, waardoor je niet kunt deelnemen aan de 'nationale' conversatie en cultuur zoals traditionele media die aanbieden. En verbonden met echte identiteiten, kunnen websurfgegevens in de handen van de overheid vallen en verkeerd worden gebruikt. Dit zijn allemaal legitieme zorgen die mensen met verschillende wereldbeelden in verschillende gradaties van belang achten..

‘Slinks’ gebruik van cookies is een van de zwakkere klachten. Cookies zijn sinds het begin een integraal onderdeel van het surfen op het web en hun privacygevolgen zijn al meer dan een decennium onderwerp van openbare discussie. Cookies vormen een heimelijke bedreiging voor de privacy, zoals roken een heimelijke bedreiging voor de gezondheid is. Als je het niet weet, heb je niet opgelet.

Maar voordat gebruikers naar uw browserinstellingen gaan en cookies annuleren, moeten webgebruikers zich een andere vraag stellen over het delen van informatie in de online wereld. Wat krijg ik ervoor terug?

De reden waarom een bedrijf als Google miljoenen en miljoenen dollars aan gratis services kan uitgeven, zoals de zoekmachine, Gmail, Google Maps, Google Groups en meer, is vanwege de verkoop van online advertenties gekoppeld aan persoonlijke gegevens.

En het is niet alleen Google. Facebook, Yahoo, MSN en duizenden blogs, nieuwssites en ‘comment boards’ gebruiken advertenties om te financieren wat ze doen. En gepersonaliseerde advertenties zijn waardevoller dan advertenties die op iedereen zijn gericht. Marketeers betalen meer om u te bereiken als de kans dat u hun producten koopt of hun services worden gebruikt groter is. (Misschien maakt online volgen iedereen speciaal!)

Als internetgebruikers minder informatie aan het web leveren, zal het web minder informatie aan hen verstrekken. Gratis inhoud zal niet verdwijnen als consumenten weigeren personalisatie toe te staan, maar er zal minder van zijn. Bloggers en exploitanten van kleine websites zullen iets minder reden hebben om de dingen te produceren die van ons internet juist zo’n eindeloos fascinerende plek maken. Als beheerder van een kleine overheid-transparantie website, WashingtonWatch.com, voeg ik nieuwe functies toe voor mijn bezoekers wanneer er genoeg geld is om het te doen. Meer geld aan advertenties betekent meer hulpmiddelen die Amerikaanse burgers op het internet kunnen gebruiken.

Tien jaar geleden, tijdens een eerdere golf van zorgen over cookies, vroeg de Federal Trade Commission het Congres om controle over het internet omwille van de bescherming van privacy. Als de FTC de bevoegdheid had gekregen om regels op te leggen die ‘kennisgeving, keuze, toegang en beveiliging' eisen van websites - allemaal goede praktijken, in verschillende mate - is het twijfelachtig dat Google in het afgelopen decennium hetzelfde succes zou hebben behaald. Het is vandaag misschien een behoorlijke, met privacy worstelende zoekmachine. Maar als het niet in staat was geweest de huidige inkomsten te genereren, was de kwaliteit van de zoekresultaten mogelijk lager en had het misschien de middelen niet gehad om al zijn fascinerende en nuttige producten te produceren en te ondersteunen. De opkomst van Google en alle toegang die het biedt, was niet vanaf het begin vastgelegd. De ontwikkelingen hingen af van een bepaalde reeks omstandigheden waarin het bedrijf toegang had tot consumenteninformatie en de vrijheid om deze informatie te gebruiken op een manier die sommigen privacy-dubieus vinden.

Sommige wetgevers, verdedigers van privacy en technologen willen zeer graag de consument beschermen, maar veel "consumentenbescherming" nodigt consumenten zelfs uit om van persoonlijke verantwoordelijkheid af te zien. De *caveat emptor rule* (het principe dat de koper zelf verantwoordelijk is om te controleren dat de kwaliteit en bruikbaarheid goed is voor de aankoop van een product) vereist dat mensen scherp blijven, leren over de producten die ze gebruiken en bedrijven het naadje van de kous vragen. De alertheid van mensen stijgt of daalt met de mate van gestelde verwachtingen. Consumentenverenigingen die uitgaan van incompetentie bij het publiek, kunnen door striktere regels er juist voor zorgen dat die incompetentie toeneemt, waardoor consumenten nog slechter af zijn.

Als een centrale autoriteit, zoals het Congres of de FTC, voor consumenten zou beslissen hoe ze met cookies zouden moeten omgaan, zou het in vele, zo niet de meeste, gevallen verkeerd generaliseren over persoonlijke belangen, waardoor die consumenten de verkeerde mix van privacy en interactiviteit zouden krijgen. Als bijvoorbeeld de FTC besluit dat consumenten cookies van derden moeten accepteren, zullen de meeste consumenten dit niet doen, waardoor de

rijkdom aan 'gratis' inhoud en services, die de meeste mensen als vanzelfsprekend beschouwen, stilletjes uit het zicht zal verdwijnen. En het zou de consument onbeschermd laten voor bedreigingen buiten zijn rechtsgebied (zoals bij het volgen van gebruikers door sites buiten de Verenigde Staten). Onderwijs is een moeilijke, en enige, manier om de privacybelangen van consumenten in evenwicht te brengen met hun andere belangen.

Maar misschien is dit een passiespel van de overheid versus het bedrijfsleven, met de overheid als privacyverdediger. The Journal meldde vorige week dat ingenieurs, die aan een nieuwe versie van Microsoft's Internet Explorer-browser werkten, dachten dat ze bepaalde standaardwaarden zouden kunnen instellen om privacy beter te beschermen, maar ze werden teruggeroepen toen de zakelijke afdeling bij Microsoft van het plan op de hoogte kwam.

Privacy "sabotage", zo noemde de Electronic Frontier Foundation het. En een nieuwsbericht van Wired meldt: Microsoft "verminkt" online privacybescherming.

Getty Images

Maar als het plan van de ingenieurs waren verwezenlijkt, zou een vergelijkbare, tegengestelde reactie het gevolg zijn geweest: Microsoft ‘saboteert’ webinteractiviteit op het internet en ‘saboteert’ het bedrijfsmodel van de reclame, waardoor de toegang van de consument tot gratis inhoud wordt belemmerd.

De nieuwe versie van de browser van Microsoft hield de cookiefunctionaliteit in stand, net als Google's Chrome-browser en Firefox, een product van de nonprofit Mozilla Foundation. Het verhaal 'handel bedrijgt privacy' verdwijnt derhalve niet.

Dit wil niet zeggen dat bedrijven geen persoonlijke informatie willen -- juist wel, zodat ze hun klanten de maximale service kunnen bieden. Maar ze worstelen om erachter te komen hoe ze alle aspecten van consumentenbelangen kunnen dienen, inclusief de van nature inconsistente eisen van privacy, gratis inhoud, aangepaste internetervaringen, gemak enzovoort, door de consument.

Slechts één ding is zeker: niemand weet hoe zich dit moet gaan ontwikkelen. Cookies en andere trackingtechnologieën veroorzaken legitieme zorgen die dan weer moeten worden afgewogen tegen de voordelen die ze bieden. Standaardinstellingen van de browser zouden kunnen convergeren naar iets dat meer privacybescherming biedt. (De Safari-browser van Apple wijst cookies van derden af, tenzij gebruikers dit anderszins aangeven.) Browser-plug-ins zullen de controle van consumenten over cookies en andere volgtechnologieën vergroten. Consumenten zullen beter gewend raken aan de informatie-economie en zij zullen duidelijker kiezen hoe ze erin willen passen. Het gaat erom dat het debat wordt voortgezet.

—Jim Harper is director of information policy studies at the Cato Institute.

Jim Harper is the Web master of *WashingtonWatch*, a site that tracks federal spending; the editor of *Privacilla*, a Web-based think tank; and the director of information policy studies at the Cato Institute in Washington, DC. He is also a founding member of the Data Privacy and Integrity Advisory Committee for the Department of Homeland Security. Harper studied political science at the University of California at Santa Barbara and in 1994 received a law degree from Hasting College of the University of California. His articles about privacy and security have appeared in *Administrative Law Review*, the *Minnesota Law Review*, the *Hastings Constitutional Law Quarterly*, the *Blaze*, and the *Technology Liberation Front*. He has also published two books: *Identity Crisis: How Identification Is Overused and Misunderstood* (2006) and *Terrorizing Ourselves: Why US Counterterrorism Policy Is Failing and How to Fix It* (2010), coedited with Benjamin H. Friedman and Christopher A. Preble. As an expert in the legal complications surrounding new technologies, Harper has testified at several congressional hearings and lectured widely.