DE AFLUISTERSTAAT

Glenn Greenwald

De afluisterstaat

Edward Snowden, de NSA en de
Amerikaanse spionage- en afluisterdiensten

VERTAALD UIT HET AMERIKAANS
DOOR JORIS VERMEULEN

Lebowski Publishers, Amsterdam 2014

Het citaat uit *1984* van George Orwell op pagina 224 is afkomstig uit de vertaling (1984) van Tinke Davids, Uitgeverij De Arbeiderspers, Amsterdam 2013, p. 6-7 (49ste druk).

Deze uitgave is tot stand gekomen dankzij bemiddeling door Internationaal Literatuur Bureau B.V.

Oorspronkelijke titel: *No Place To Hide: Edward Snowden, The NSA, and the U.S. Surveillance State*
Published by arrangement with Metropolitan Books, an imprint of Henry Holt and Company, LLC, New York.

Omslagontwerp: Vruchtvlees
Typografie: Perfect Service, Schoonhoven

ISBN 978 90 488 1940 9
ISBN 978 90 488 1941 6 (e-book)
NUR 400

www.lebowskipublishers.nl

Lebowski Publishers is een imprint van Dutch Media Books bv

Dit boek is opgedragen aan al degenen die hebben getracht een licht te werpen op de geheime systemen voor massasurveillance van de Amerikaanse overheid, met name aan de moedige klokkenluiders die hiervoor hun vrijheid hebben geriskeerd.

'De regering van de Verenigde Staten heeft een technologie geperfectioneerd die ons de mogelijkheid verschaft mee te kijken met berichten die door de ether gaan [...]. Die mogelijkheid zou op elk moment tegen de Amerikaanse bevolking kunnen worden gekeerd, waardoor geen Amerikaan nog enige privacy zou hebben, zo groot is ons vermogen met alles mee te kijken: telefoongesprekken, telegrammen, willekeurig wat. Niemand zou eraan kunnen ontsnappen.'

– senator Frank Church, voorzitter van de Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 1975

Inhoud

Inleiding

In de herfst van 2005 besloot ik, zonder daar bijster veel van te verwachten, een politiek blog te beginnen. Destijds voorzag ik niet dat het besluit zulke grote gevolgen voor mijn leven zou hebben. Ik begon het blog vooral omdat ik me steeds meer zorgen maakte over de radicale, extremistische machtstheorieën die het Amerikaanse landsbestuur in de nadagen van 11 september 2001 was gaan aanhangen. Door over dat soort onderwerpen te schrijven hoopte ik meer gewicht in de maatschappelijke schaal te kunnen leggen dan ik kon als advocaat op het vlak van constitutioneel en burgerlijk recht, mijn toenmalige werk.

Nog maar zeven weken na mijn eerste blog kwam *The New York Times* met een spectaculair bericht: in 2001, zo schreef de krant, had de regering-Bush in het geheim de National Security Agency (NSA) de opdracht gegeven tot het aftappen van elektronische communicatie tussen Amerikanen zonder daarvoor eerst de bevelschriften te regelen die krachtens het vigerende strafrecht verplicht waren. Toen dit aan het licht kwam, was dat meekijken en afluisteren zonder bevelschrift al vier jaar aan de gang en waren er minstens een paar duizend Amerikanen aan blootgesteld.

Het onderwerp bood een uitgelezen kans om mijn passies, kennis en ervaring te combineren. De overheid probeerde het geheime NSA-programma goed te praten door precies zo'n extreem beeld van de uitvoerende macht te schetsen waardoor ik was gaan schrijven: het idee dat de dreiging van terrorisme de president een nagenoeg onbeperkt mandaat verschafte om alles te doen 'om het land te beschermen', tot het overtreden van de wet aan toe.

Tijdens het debat dat volgde passeerden complexe kwesties de revue die betrekking hadden op de grondwet en de interpretatie daarvan, kwesties waar ik dankzij mijn juridische achtergrond prima mee raad wist.

Tot twee jaar daarna behandelde ik in mijn blog en mijn bestseller uit 2006 elk aspect van het schandaal dat de NSA met zijn bevelschriftvrije afluisterpraktijken had ontketend. Mijn standpunt was helder: door te besluiten illegaal burgers te laten bespioneren had de president misdaden begaan, misdaden waarover hij rekenschap moest afleggen. In Amerika's steeds chauvinistischer en benepener wordende politieke klimaat bleek dit een uiterst controversieel standpunt.

Dit bracht Edward Snowden er een paar jaar later toe mij als eerste te benaderen om het nog grootschaliger wangedrag van de NSA naar buiten te brengen. Volgens hem, zo zei hij, zou ik als geen ander de gevaren van massale surveillance en een extreem gesloten landsbestuur begrijpen, en niet wijken voor de druk vanuit de overheid en haar vele bondgenoten in de media en elders.

De combinatie van de indrukwekkende hoeveelheid ultrageheime documenten die Snowden aan me doorspeelde en het grote drama waarin Snowden zichzelf had gemanoeuvreerd, heeft wereldwijd ongekend veel belangstelling opgewekt voor de dreiging van massale elektronische surveillance en de waarde van privacy in het digitale tijdperk. Maar de onderliggende problemen hadden al jaren liggen gisten, grotendeels onzichtbaar voor derden.

De huidige controverse rond de NSA kent zonder meer veel unieke aspecten. Tegenwoordig is het technisch mogelijk een soort alomtegenwoordige surveillance in praktijk te brengen die tot voor kort was voorbehouden aan de meest fantasievolle sciencefictionschrijvers. Bovendien is het klimaat dat na 11 september 2001 in de VS is ontstaan – waarin het motto 'veiligheid boven alles' wordt gehuldigd – bijzonder bevorderlijk voor machtsmisbruik. En dankzij Snowdens moed en het relatieve gemak

waarmee digitale informatie kan worden gekopieerd, is ons een unieke, rechtstreekse blik vergund op alle facetten van de 'afluisterstaat'.

In de vragen die de NSA-affaire oproept klinken desondanks talloze gebeurtenissen uit het verleden door, waarvan sommige lang geleden hebben plaatsgevonden. Sterker nog: weerstand tegen een overheid die weinig respect toonde voor andermans privacy heeft in grote mate bijgedragen aan de totstandkoming van de Verenigde Staten zelf. In het verleden protesteerden Amerikaanse kolonisten al tegen wetten die Britse overheidsvertegenwoordigers de ruimte gaven om elke woning naar believen te doorzoeken. De kolonisten vonden het prima als de staat met specifieke, heel gerichte bevelschriften personen doorlichtte als die van wandaden werden verdacht. Maar algemeen geldende verordeningen – die het mogelijk maakten de complete burgerij zonder onderscheid des persoons na te trekken – waren per se niet-legitiem.

Met het Vierde Amendement werd deze bevinding vastgelegd in de Amerikaanse grondwet. De tekst is helder en beknopt: 'Het recht van het volk op vrijwaring van zijn persoon, huis, papieren en bezittingen tegen onredelijke huiszoekingen en inbeslagnemingen zal niet worden geschonden, en geen bevelschriften daartoe zullen worden verstrekt, tenzij er gegronde redenen zijn die door eed of belofte worden bekrachtigd en die duidelijk de te doorzoeken plaats beschrijven, evenals de personen of voorwerpen die moeten worden meegenomen.' Het amendement was vóór alles bedoeld om het de regering voorgoed onmogelijk te maken haar Amerikaanse burgers te onderwerpen aan algemene controles zonder gerichte verdenkingen.

Het conflict over het staatstoezicht had in de achttiende eeuw vooral betrekking op huiszoekingen, maar de aard van dat toezicht ging gelijk op met de voortschrijdende technologie. Halverwege de negentiende eeuw deed zich in Groot-Brittannië een enorm schandaal voor; door de opmars van de spoorwegen kon

post goedkoop en snel worden bezorgd, post die de Britse regering heimelijk opende. Later, tijdens de eerste decennia van de twintigste eeuw, tapte het Amerikaanse Bureau of Investigation – de voorloper van de huidige FBI – bedrade communicatie af om tegenstanders van het Amerikaanse overheidsbeleid bij de kladden te kunnen grijpen. Dit gebeurde in combinatie met het openen van post en de inzet van informanten.

Welke technieken er ook worden gebruikt, grootscheepse surveillance heeft in de loop der geschiedenis diverse terugkerende karakteristieken gehad. Aanvankelijk zijn altijd de landelijke dissidenten en randfiguren het grootste mikpunt van de surveillance, waardoor de sympathisanten van de regering en degenen die het allemaal koud laat er abusievelijk van overtuigd raken dat zij de dans ontspringen. En de geschiedenis leert ons dat alleen al de aanwezigheid van een goed ontwikkeld afluistersysteem volstaat om protest in de kiem te smoren, ongeacht de manier waarop het systeem wordt ingezet. Een bevolking die beseft dat ze altijd en overal in de gaten wordt gehouden, wordt al snel bang en meegaand.

Halverwege de jaren zeventig werd door een senaatscommissie onder voorzitterschap van senator Frank Church een onderzoek gedaan naar de spionageactiviteiten van de FBI in de Amerikaanse samenleving. De onthutsende uitkomst was dat de overheidsdienst dag in dag uit mensen puur vanwege hun politieke overtuigingen bespioneerde en een half miljoen Amerikaanse burgers tot mogelijke 'subversieven' had bestempeld. (De verdachten liepen uiteen van Martin Luther King tot John Lennon, van de Women's Liberation Movement tot de anticommunistische John Birch Society.) Maar diepgaand misbruik van al die afluistermogelijkheden is geenszins een louter Amerikaans fenomeen. Integendeel: overal laten machthebbers zonder scrupules zich verleiden tot grootscheepse spionage. En in alle gevallen zien we dezelfde drijfveer: het verlangen opstandigheid te onderdrukken en meegaandheid af te dwingen.

Zo kunnen regeringen van verder bijzonder uiteenlopende politieke snit elkaar de hand schudden waar het spionage betreft. Aan het begin van de twintigste eeuw creëerde zowel de Britse als de Franse wereldmacht speciale afdelingen die antikoloniale bewegingen in het oog moesten houden. Na de Tweede Wereldoorlog werd het Oost-Duitse ministerie voor Staatsveiligheid – 'Stasi' in de volksmond – synoniem met een overheid die zich mengde in privélevens. Een recenter voorbeeld zijn de regimes van Syrië, Egypte en Libië, die allemaal het internetgedrag van hun dissidenten trachtten te volgen toen opstandige burgers zich tijdens de Arabische Lente kritisch uitlieten over hun dictators.

Onderzoek van Bloomberg News en *The Wall Street Journal* heeft uitgewezen dat die dictaturen letterlijk bij westerse leveranciers van afluistertechniek gingen shoppen toen de demonstranten iets te bedreigend werden. Het regime van de Syrische president Assad liet medewerkers van de Italiaanse surveillancefirma AREA overvliegen, die te horen kregen dat de Syriërs 'dringend wat mensen in de gaten moesten gaan houden'. De geheime politie van Mubarak in Egypte kocht materiaal om de versleuteling van Skype te kraken zodat ze gesprekken van activisten konden volgen. En in Libië, zo meldde dezelfde krant, stuitten journalisten en rebellen die in 2011 een afluistercentrum van de regering betraden op 'een muur van zwarte apparaten met de afmetingen van een koelkast', geleverd door de afluisterexperts van het Franse ICT-bedrijf Amesys. De apparatuur 'volgde het internetverkeer' van de grootste Libische internetprovider, 'opende e-mails, kraakte wachtwoorden, luistervinkte tijdens online chats en bracht connecties tussen diverse verdachten in kaart'.

Wie de communicatie van burgers kan afluisteren beschikt over enorm veel macht. En die wordt vrijwel zeker misbruikt als er geen streng toezicht plaatsvindt en er niemand verantwoording over hoeft af te leggen. Een regering als de Amerikaanse die in het grootste geheim een gigantische afluistermachinerie bedient en níet ten prooi valt aan alle verleidingen daarvan, staat

haaks op wat de geschiedenis ons heeft geleerd en op alle beschikbare kennis over de menselijke aard.

Nog vóór de onthullingen van Snowden werd al duidelijk dat het uiterst naïef zou zijn om de Verenigde Staten als een soort uitzondering op het gebied van surveillance te beschouwen. In 2006 vond een hoorzitting van het Congres plaats die de titel 'Internet in China: een middel voor vrijheid of voor onderdrukking?' meekreeg. Sprekers verdrongen elkaar om de Amerikaanse bedrijven te veroordelen die de technologie hadden geleverd waarmee de Chinese overheid dissidenten op internet de mond kon snoeren. Het Republikeinse Congreslid Christopher Smith (New Jersey), voorzitter van de bijeenkomst, vergeleek de samenwerking tussen Yahoo! en de Chinese geheime politie met het uitleveren van Anne Frank aan de nazi's. Het was typisch zo'n donderpreek die Amerikaanse notabelen laten horen als ze over een regime spreken dat een andere koers vaart dan de Verenigde Staten.

Maar zelfs degenen die aan de hoorzitting deelnamen konden niet om het feit heen dat die amper twee maanden plaatsvond nadat *The New York Times* had onthuld hoe de regering-Bush zonder enig bevelschrift massaal Amerikaanse burgers had afgeluisterd. In het licht van die onthullingen klonken ze nogal hol, de afkeurende woorden aan het adres van andere landen die hun eigen bevolking bespiedden. Afgevaardigde Brad Sherman (Democraat, Californië), die na Christopher Smith sprak, stelde dat de technologische bedrijven die het verzoek kregen het Chinese regime links te laten liggen ook kritisch moesten zijn ten aanzien van hun eigen regering. 'Anders kan het een dezer jaren weleens zo zijn,' waarschuwde hij op profetische wijze, 'dat terwijl de Chinezen zien hoe hun privacy op de meeste slinkse wijzen wordt geschonden, wij hier in de Verenigde Staten moeten vaststellen dat een of andere president vanuit ultrabrede interpretaties van de grondwet onze e-mails leest, en ik heb liever niet dat dit zonder bevelschrift gebeurt.'

De afgelopen decennia hebben de Amerikaanse leiders de wijdverbreide angst voor terroristen aangewakkerd door voortdurend de werkelijke dreiging te overdrijven, en die angst vervolgens aangegrepen om een breed scala aan extreme maatregelen te rechtvaardigen. Dit heeft tot aanvalsoorlogen geleid, tot een regime dat op mondiale schaal martelt en zowel allochtone als autochtone Amerikanen vastzet (en zelfs vermoordt) zonder enige vorm van aanklacht. Maar het alomtegenwoordige, stiekeme systeem waarmee zonder enige verdachtmaking derden worden afgeluisterd, zou weleens de hardnekkigste consequentie van deze politiek kunnen zijn. Dit omdat het huidige schandaal rond de NSA ondanks een groot aantal overeenkomsten met eerdere affaires een volslagen nieuwe dimensie kent: de rol die het internet tegenwoordig in ons dagelijks leven speelt.

Vooral voor de jongste generaties is het internet niet een of ander op zichzelf staand, apart gebied waar sommige delen van ons bestaan zich afspelen. Het is méér dan ons postkantoor en onze telefoon. Het vertegenwoordigt eerder het epicentrum van onze wereld, het is de plek waar nagenoeg alles gebeurt. Dáár worden vriendschappen gesloten, boeken en films uitgezocht, dáár maken politieke activisten hun afspraken, wordt het gros van onze privégegevens aangemaakt en opgeslagen. Het is de plek waar we onze persoonlijkheid en ons zelfbewustzijn ontwikkelen en tot uitdrukking brengen.

Dat netwerk veranderen in een systeem voor grootscheepse surveillance heeft consequenties die volslagen anders zijn dan die van welk eerder afluisterprogramma ook. Alle voorafgaande spionagemethodes waren als vanzelf kleinschaliger en konden gemakkelijker worden omzeild. Als permanente surveillance wortel kan schieten op het internet zouden bijna alle vormen van menselijke interactie, al onze plannen en zelfs onze gedachten worden onderworpen aan ingrijpend staatstoezicht.

Sinds het internet op grote schaal wordt gebruikt, hebben velen het een bijzondere kracht toegedicht: het vermogen hon-

derden miljoenen mensen te bevrijden door de politieke arena te democratiseren, de machthebbers en de machtelozen op één niveau te plaatsen. Internetvrijheid – het netwerk onbevreesd kunnen gebruiken zonder dwang van buitenaf, zonder sociale of overheidscontrole – is essentieel om die belofte te kunnen inlossen. Wie het internet tot een afluisterinstrument maakt, treft het dus recht in zijn hart. Sterker nog: hij verandert het in een middel voor onderdrukking dat kan verworden tot het meest extreme, repressieve wapen voor overheidsbemoeienis in de geschiedenis van de mensheid.

Daarom zijn de onthullingen van Snowden zo onthutsend en uiterst belangrijk. Door zijn moedige besluit de verbluffende afluistertechnieken en de nog schokkender ambities van de NSA bloot te leggen, heeft hij bewezen dat we ons op een historisch kruispunt bevinden. Zal het digitale tijdperk, dankzij de unieke kenmerken van het internet, meer persoonlijke vrijheid en politieke speelruimte inluiden? Of zal het een systeem van alomtegenwoordig toezicht en ingrijpen in de hand werken dat zelfs de stoutste dromen van de grootste tirannen uit het verleden overtreft? Op dit moment kan het nog beide kanten uit gaan. Ons doen en laten bepaalt waar we belanden.

1

Contact

Op 1 december 2012 ontving ik voor het eerst een bericht van Edward Snowden, maar zijn naam kreeg ik toen niet te horen.

Het contact werd gelegd via een e-mail van iemand die zichzelf Cincinnatus noemde. Die naam verwees naar Lucius Quinctius Cincinnatus, een Romeinse boer die in de vijfde eeuw v.Chr. tot dictator van Rome werd benoemd om de stad te verdedigen. Hij leeft vooral in de herinnering voort vanwege hetgeen hij deed nadat hij de vijanden van Rome had overwonnen: hij gaf direct én vrijwillig zijn politieke macht uit handen en ging weer boeren. Cincinnatus, geprezen als 'toonbeeld van civiele deugd', is symbool komen te staan voor de inzet van politieke macht ten gunste van het algemeen belang en voor het beperken of zelfs opgeven van persoonlijke macht ten bate van de publieke zaak.

De e-mail begon als volgt: 'Ik vind het heel belangrijk dat iedereen veilig kan communiceren'. Ik kreeg het nadrukkelijke verzoek om PGP-versleuteling te gaan gebruiken, zodat 'Cincinnatus' me dingen kon sturen waar ik, zo zei hij, vast en zeker belangstelling voor zou hebben. PGP, ontwikkeld in 1991, is een afkorting van 'Pretty Good Privacy'. Het is in de loop der jaren een geraffineerd hulpmiddel geworden om e-mail en andere vormen van online communicatie te vrijwaren van meekijkers en hackers.

Het programma voorziet in feite elke e-mail van bescherming, een schild in de vorm van een code die uit honderden of zelfs duizenden willekeurig gekozen cijfers en hoofdlettergevoelige letters bestaat. De meest geavanceerde inlichtingendiensten op aarde – een divisie waar de NSA zonder meer deel van uitmaakt – be-

schikken over software die één miljard kraakpogingen per seconde kan doen. Maar de codes van de voornoemde PGP-encryptie zijn zo lang en onvoorspelbaar dat zelfs de meest vernuftige software soms jaren bezig is ze te achterhalen. Degenen die het meest beducht zijn voor meekijkers, zoals personeel van inlichtingendiensten, spionnen, burgerrechtenactivisten en hackers, zoeken hun toevlucht in deze vorm van versleuteling om hun communicatie af te schermen.

In de e-mail die ik kreeg schreef 'Cincinnatus' dat hij overal had gezocht naar mijn 'PGP *public key*' (een unieke code waarmee iemand versleutelde e-mail kan ontvangen en lezen), maar die niet had kunnen vinden. Daaruit concludeerde hij dat ik het programma niet gebruikte. 'Daardoor loopt iedereen die met je communiceert gevaar,' deelde hij me mee. 'Ik beweer niet dat elke vorm van communicatie waarbij je betrokken bent versleuteld moet zijn, maar je zou je correspondenten in elk geval de mogelijkheid moeten bieden.'

'Cincinnatus' refereerde vervolgens aan het seksschandaal dat generaal David Petraeus trof. Diens carrière strandde door een buitenechtelijke verhouding met journaliste Paula Broadwell, die aan het licht kwam toen onderzoekers een Google-mailwisseling tussen de twee ontdekten. Als Petraeus zijn berichten eerst had versleuteld voordat hij ze toevertrouwde aan zijn Gmail-account of aan zijn map met 'concepten', schreef 'Cincinnatus', hadden de onderzoekers ze niet kunnen lezen. 'Encryptie is belangrijk, niet alleen voor spionnen en rokkenjagers.' Het installeren van e-mailversleuteling is, zo zei hij, 'een ernstig noodzakelijke voorzorgsmaatregel voor iedereen die met jou wil communiceren.'

Om me aan te moedigen zijn advies op te volgen voegde hij eraan toe: 'Er zijn daarbuiten mensen waar je graag meer van wilt weten maar die nooit met jou in contact kunnen treden zolang ze niet zeker weten dat hun berichten niet onderweg worden gelezen.'

Vervolgens bood hij me aan om te helpen met het installeren

van het programma: 'Als je assistentie nodig hebt, wat dan ook, laat het me alsjeblieft weten, of vraag anders hulp via Twitter. Je hebt veel technisch onderlegde volgers die bereid zullen zijn om je meteen te helpen.' Hij sloot af met: 'Dank je. C.'

Ik was al lange tijd van plan geweest om encryptiesoftware te gebruiken. Ik had al jaren over WikiLeaks geschreven, over klokkenluiders, het hackerscollectief dat zichzelf Anonymous noemt en aanverwante zaken, en ook had ik van tijd tot tijd gecommuniceerd met senior medewerkers van de Amerikaanse veiligheidsdiensten. Veel van hen zijn erg alert op veilige communicatie en het voorkomen van ongewenst meekijken. Maar de software in kwestie is heel complex, zeker voor iemand die niet echt handig is met computers en het beheer daarvan, zoals ik. Daardoor was ik er nooit aan toegekomen.

Ik reageerde niet op C.'s e-mail. Omdat ik bekendsta als iemand die schrijft over thema's die andere journalisten links laten liggen, krijg ik regelmatig berichten van mensen die me een 'fantastisch verhaal' aanbieden dat meestal niets blijkt voor te stellen. En het gros van de tijd werk ik aan meer verhalen dan ik aankan. Met als gevolg dat ik een concrete prikkel nodig heb om mijn klus van dat moment te laten rusten en achter een nieuwe lead aan te gaan. In zijn e-mail mocht C. dan wel een vage toespeling maken op 'mensen daarbuiten waar ik graag meer van zou willen weten', er stond niets in waar ik voldoende door werd getriggerd. Ik las het bericht maar beantwoordde het niet.

Drie dagen later liet C. opnieuw van zich horen. Hij vroeg me of ik wilde bevestigen dat ik de eerste e-mail had ontvangen. Ditmaal antwoordde ik snel. 'Ik heb hem gehad en ga ermee aan de slag. Ik heb geen PGP-code en weet niet hoe ik eraan moet komen, maar ik zal proberen iemand te vinden die me kan helpen.'

Later die dag kwam hij terug met een heldere uitleg, stap voor stap, van het PGP-systeem; in feite een soort Encryptie voor Dummies. Tegen het einde van de instructies, die ik toch nog ingewikkeld en verwarrend vond, grotendeels vanwege mijn eigen

onkunde, merkte hij op dat het hier nog maar 'de meest basale grondbeginselen' betrof. 'Als je niemand kunt vinden om je door de installatie te loodsen, het genereren van codes en het gebruik ervan,' voegde hij eraan toe, 'laat het me alsjeblieft weten. Ik kan je in contact brengen met mensen, bijna overal ter wereld, die crypto begrijpen.'

Deze e-mail eindigde bloemrijker dan de voorgaande twee: 'Cryptografisch de uwe, Cincinnatus'.

Mijn goede bedoelingen ten spijt kwam ik er niet aan toe om met die encryptie aan de slag te gaan. Zeven weken verstreken zonder actie op dit punt, wat me toch wel enigszins dwarszat. Wat als deze figuur echt een belangrijk verhaal voor me had, dat aan mijn neus voorbij zou gaan, alleen omdat ik er niet in slaagde een computerprogramma te installeren? Los daarvan wist ik dat encryptie later van pas zou kunnen komen, ook als zou blijken dat Cincinnatus niets interessants te bieden had.

Op 28 januari 2013 mailde ik hem dat ik iemand ging zoeken die me kon helpen met de encryptie en dat ik het hopelijk de dag erna voor elkaar zou hebben.

De volgende dag antwoordde hij: 'Wat een geweldig nieuws! Als je verder nog hulp nodig hebt of later met vragen komt te zitten, je bent altijd welkom, aarzel niet. Ik ben je echt heel dankbaar dat je wilt bijdragen aan meer privacy op het vlak van de communicatie! Cincinnatus.'

Maar ik deed opnieuw niets. Ik werd volledig in beslag genomen door een overvloed aan andere verhalen en was er nog steeds niet van overtuigd dat C. iets interessants te melden had. Het was niet zo dat ik bewust besloot niet in actie te komen. Het was gewoon zo dat ik zoals altijd een te lange *to do*-lijst had, en het installeren van encryptiesoftware ten faveure van een onbekende werd nooit urgent genoeg om andere aandachtspunten te verdringen.

C. en ik waren in een catch-22 beland. Zolang ik geen encryptie had geïnstalleerd was hij niet bereid me nadere informatie te