Über den Autor:

Der Jurist und Verfassungsrechtler Glenn Greenwald ist einer der einflussreichsten politischen Kommentatoren in den USA und Mitbegründer des investigativen Online-Magazins *The Intercept.* 2010 erhielt er den Online Journalism Association Award für seine investigative Berichterstattung über die Verhaftung des Whistleblowers Bradley Manning. Für die Aufdeckung der NSA-Affäre wurde er mit dem Pulitzer-Preis und dem Geschwister-Scholl-Preis ausgezeichnet. Glenn Greenwald lebt in Brasilien.

Glenn Greenwald

Die globale Überwachung

Der Fall Snowden, die amerikanischen Geheimdienste und die Folgen

Aus dem Englischen von
Gabriele Gockel, Robert Weiß,
Thomas Wollermann und Maria Zybak

KNAUR

Die amerikanische Originalausgabe erschien 2014 unter dem Titel
»No Place to Hide« bei Metropolitan Books, New York.

Besuchen Sie uns im Internet:
www.knaur.de

Erweiterte Taschenbuchausgabe September 2015
Knaur Taschenbuch

Die Übersetzer Gabriele Gockel, Robert Weiß, Thomas Wollermann
und Maria Zybak gehören dem Kollektiv Druck-Reif an.
Covergestaltung: ZERO Werbeagentur, München
Coverabbildung: Gettyimages; Picture Alliance / AP Photo /
The Guardian, Glenn Greenwald and Laura Poitras
Satz: Adobe InDesign im Verlag
Druck und Bindung: CPI books GmbH, Leck
ISBN 978-3-426-78691-8

5 4 3 2 1

Dieses Buch ist all denen gewidmet,
die versucht haben, das von der
amerikanischen Regierung geschaffene System
der Massenüberwachung aufzudecken,
insbesondere den mutigen Whistleblowern,
die dabei ihre Freiheit aufs Spiel gesetzt haben.

Hinweis

Bei einigen Dokumenten, die in diesem Buch veröffentlicht werden, sind auf Veranlassung der National Security Agency (NSA) zur Wahrung der nationalen Sicherheit der Vereinigten Staaten von Amerika Passagen unkenntlich gemacht worden.

Inhalt

Vorwort zur Taschenbuchausgabe 9
Einführung 17

1 Kontaktaufnahme 25
2 Zehn Tage in Hongkong 63
3 Alles sammeln! 145
4 Die Gefahren der Massenüberwachung 251
5 Die vierte Gewalt 305

Nachwort 361

Dank 371

Geschwister-Scholl-Preis 2014
Dankesrede von Glenn Greenwald 375

Vorwort zur Taschenbuchausgabe

Seit der Erstveröffentlichung dieses Buches im Mai 2014 überschlagen sich – gerade in Deutschland, aber auch überall sonst auf der Welt – die Ereignisse infolge der Snowden-Enthüllungen. Dabei wird deutlich, wie groß die Sorge um den Schutz der Privatsphäre ist. Leider ist dies auch auf das Umsichgreifen elektronischer Spionage seitens verschiedener Regierungen zurückzuführen, unter anderem auch der deutschen.

Im Herbst 2013 erschienen im *Spiegel* Spionageberichte, die Deutschland unmittelbar betrafen. Der erste Artikel enthüllte die Massenüberwachung der gesamten deutschen Bevölkerung durch die NSA, was milden Tadel seitens der Regierung Merkel nach sich zog. Als jedoch weitere Spionagefälle bekannt wurden – insbesondere als sich herausstellte, dass nicht nur gewöhnliche Bürger, sondern führende Politiker, darunter Kanzlerin Merkel persönlich, abgehört worden waren –, reagierte die Bundesregierung ungehalten. Gemeinsam mit Brasilien stellte sich Deutschland an die Spitze der öffentlichen Empörung über die Spionagetätigkeit der NSA.

Während sich der Bundestag 2014 anschickte, die Überwachung der Deutschen durch die NSA zu untersuchen, kam ein neuer Skandal ans Licht. Ein Agent des Bundesnachrichtendienstes (BND) wurde unter dem Vorwurf verhaftet, er habe den parlamentarischen Untersuchungsausschuss im Auftrag der NSA bespitzelt. Dass die NSA zunächst ganz Deutschland überwacht hatte und anschließend einen Doppelagenten einsetzte, um den entsprechenden Untersuchungsausschuss

auszuspionieren, war im Grunde eine Demütigung des politischen Berlin in einem nie gekannten Ausmaß.

Aber viele Deutsche äußerten den stets schwelenden, heimlichen Verdacht, dass die »Empörung« Berlins weitgehend vorgetäuscht war. Fast scheint es, als könne keine Demütigung oder Respektlosigkeit tief genug gehen, um die eherne Unterwürfigkeit der Bundesregierung gegenüber den Vereinigten Staaten zu erschüttern. Zudem war dieser Verdacht durch die Ansicht begründet, dass der BND über die Bespitzelung nicht nur im Bilde gewesen war, sondern sich aktiv daran beteiligt hatte.

Diese Ansicht hat sich in überwältigender Weise bestätigt. Im Jahr 2015 vom *Spiegel* vorgelegte Beweise demonstrieren, dass die NSA, von ihrem Stützpunkt in Deutschland aus, offenbar »über Jahre hinweg mit Wissen des Bundesnachrichtendienstes Ziele in Westeuropa und Deutschland ausgespäht« hat (*Spiegel* 23.04.2015). Andere Dokumente enthüllten zuvor unbekannte Kooperationsabkommen zwischen den beiden Diensten.

All diese Enthüllungen weckten naturgemäß große Sorge um den Schutz der Privatsphäre in Deutschland. Aber in noch stärkerem Maße warfen sie – wie der NSA-Skandal selbst – grundsätzliche Fragen zur Demokratie auf. Wie kann man von einem Land behaupten, es habe eine funktionierende Demokratie, wenn die folgenreichsten Handlungen seiner Regierung vor den Bürgern geheim gehalten werden oder, schlimmer noch, führende Beamte und Politiker systematisch und bewusst die Öffentlichkeit darüber täuschen?

Seit ich das allererste Mal einen Blick in das Snowden-Archiv warf, war es nicht die offenkundig hemmungslose Invasion der Privatsphäre, die mir am meisten Sorge bereitete. Es war die schonungslose Zersetzung der Demokratie, die sich hier zeigte. Dass etwas von so gewaltigen Dimensionen – die Umwandlung des Internets in ein Reich der Massenüber-

wachung, die Schaffung des größten je dagewesenen Systems der Überwachung ohne Anfangsverdacht – vollkommen im Dunkeln vollzogen werden konnte, ließ die Demokratie illusorisch erscheinen. Dieselbe Reaktion stellte sich bei mir ein, als ich beobachtete, wie in Deutschland die Wahrheit ans Licht kam: Es schien klar, dass die Bundesregierung ihre Bürger bewusst getäuscht hatte, als sie ihnen die Tatsache verschwieg, dass sie von dem System der Überwachung, das sie angeblich so empörend fand, Kenntnis gehabt und sich daran beteiligt hatte.

Außerhalb Deutschlands gewannen die Reaktionen auf die Snowden-Enthüllungen noch zwei Jahre nach Publikmachung der ersten Dokumente an Intensität. Und größtenteils wurden schwer zu überwindende Hindernisse für das amerikanische Regime der Massenüberwachung errichtet.

Am 2. Juni 2015 – exakt zwei Jahre nach der Ankunft von Laura Poitras und mir in Hongkong, wo wir Edward Snowden trafen – unterschrieb Präsident Obama den USA Freedom Act. Unter anderem bereitete das neue Gesetz dem allerersten Überwachungsprogramm ein Ende, über das ich im *Guardian* berichtet hatte: der Sammlung und Speicherung der Telefonverbindungsdaten aller Amerikaner.

Zweifellos aber leistet das Gesetz beklagenswert unzureichende Dienste zum Schutz der Privatsphäre. Erstens gilt es nur für Amerikaner und lässt damit 95 Prozent der Bewohner des Planeten, die nach amerikanischer Diktion als »Nichtamerikaner« bezeichnet werden, völlig ungeschützt. Und die große Mehrheit der von der NSA durchgeführten Überwachungsprogramme, von denen Amerikaner betroffen sind, blieb unangetastet. Dieses neue »Reform«-Gesetz gemäßigt zu nennen, oder auch nur »symbolisch«, ist eine Untertreibung.

Was allerdings nicht heißt, dass es völlig bedeutungslos wäre. So mangelhaft dieses Gesetz sein mag, es ist das erste

Mal seit den Anschlägen vom 11. September – vor 14 Jahren –, dass die Machtbefugnisse, die sich die US-Regierung im Namen der Terrorismusbekämpfung aneignete, *beschnitten* und nicht *erweitert* wurden. Hinsichtlich der Neuausrichtung des amerikanischen Wertesystems und seiner Abwägung zwischen Sicherheit und Freiheit ist dies eine wichtige Kurskorrektur. Entscheidender ist allerdings, dass das Gesetz mit breiter Unterstützung beider Parteien verabschiedet wurde: Führende Mitglieder der Demokraten und der Republikaner bekräftigten zum ersten Mal seit beinahe zwei Jahrzehnten die Wichtigkeit der Freiheitsrechte und der Privatsphäre.

Wie ich in diesem Buch jedoch dargestellt habe, kann die US-Regierung sicher nicht selbst ihrer Macht ernstzunehmende Grenzen setzen. Mächtige Institutionen suchen nicht nach Mitteln und Wegen, ihre eigene Macht zu beschneiden. Gelegentlich sind sie gezwungen, den Anschein zu erwecken, aber das Ergebnis ist in der Regel eher Schein als Sein und mehr darauf zugeschnitten, die erzürnte Öffentlichkeit zu beschwichtigen, als tatsächlich Macht abzugeben.

Die wahren Fronten in diesen Schlachten verlaufen fern von Washington. Und dort sind die Zeichen ermutigend.

Vor den Snowden-Enthüllungen arbeiteten die führenden Technologieunternehmen des Silicon Valley eifrig und enthusiastisch mit der NSA zusammen; sie reichten enorme Datenmengen ihrer Nutzer weiter, taten bei dieser Kollaboration oft ihr Bestes und lieferten noch mehr, als das Gesetz es befahl. Schließlich waren damit keine Risiken verbunden (denn es vollzog sich im Geheimen), während andererseits reicher Lohn winkte, und zwar in Form von Regierungsaufträgen und generell engen Beziehungen zu Geheimdienstfunktionären, die jährlich über zweistellige Milliardenbeträge verfügen.

Seit wir Licht auf dieses Beziehungsgeflecht werfen konnten, haben sich die Rahmenbedingungen drastisch geändert.

Und zwar nicht etwa deshalb, weil sich diese Unternehmen plötzlich um die Privatsphäre ihrer Nutzer sorgen würden – in den Jahren vor den Enthüllungen hatten sie klar bewiesen, dass sie derlei Bedenken nicht kennen. Vielmehr hat sich die Situation aus kommerziellem Eigeninteresse verändert: Firmen wie Facebook, Google, Yahoo und Microsoft waren wie gelähmt vor Angst, die gegenwärtige und auch die nächste Generation von Internetusern weltweit zu verlieren, wenn sie als Kollaborateure der NSA wahrgenommen würden. Sie waren beherrscht von der tiefen Sorge, dass in Ländern wie Deutschland, Südkorea und Brasilien die sozialen Medien Teenager vor amerikanischen Internetanbietern warnen könnten, weil sie ihre Daten an die NSA weitergeben würden. Womöglich würden sie den jungen Leuten empfehlen, stattdessen zu Online-Diensten zu greifen, die sich dem Schutz statt der Zerstörung ihrer Privatsphäre verschreiben. Studien zeigen weltweit eine massive Zunahme der Verschlüsselungspraxis durch die Nutzer. Dies verdeutlicht, wie ernst die Menschen heute den Schutz der Privatsphäre nehmen und dass sie bereit sind, entsprechende Maßnahmen zu ergreifen.

Aus der Angst heraus, das neu erwachte kritische Bewusstsein der Öffentlichkeit könne ihre Geschäftsgrundlage bedrohen, schickten sich die Chefs im Silicon Valley an, sich in aller Öffentlichkeit als Schützer der Privatsphäre zu präsentieren. Sie wussten, dass sie unter Beobachtung standen und nicht mehr mit hohlen symbolischen Gesten davonkommen würden, wie sie bei Politikern in Washington so beliebt sind. Um ihre künftigen Geschäftsinteressen in der Post-Snowden-Ära zu wahren, mussten sie echte Schutzmaßnahmen entwickeln und umsetzen. Und genau das haben sie in den letzten zwei Jahren getan.

Ende 2014 verkündete der Chat-Dienst WhatsApp – der inzwischen Facebook gehört und von Hunderten Millionen Menschen weltweit genutzt wird –, er werde, wie *Gizmodo*

kolportierte, »seinen 600 Millionen Usern die Ende-zu-Ende-Verschlüsselung bringen« und es sei die umfassendste Anwendung dieser Verschlüsselungsart, die es je gegeben habe. Wie das Technikportal und Mediennetzwerk *The Verge* erklärte, »bedeutet ›Ende-zu-Ende‹, dass im Gegensatz zu Nachrichten, die von Gmail oder Facebook Chat verschlüsselt werden, WhatsApp nicht in der Lage ist, die Nachricht selbst zu entschlüsseln, selbst wenn das Unternehmen durch Strafverfolgungsbehörden dazu gezwungen würde«.

Noch beeindruckender sind einige Neuerungen von Apple im Bereich der Privatsphäre. Das Magazin *Wired* schilderte sie folgendermaßen:

> **Das neue Betriebssystem von Apple, iOS 8, enthält zwei Veränderungen bei der Verschlüsselung von Daten auf dem Gerät, die die Sicherheit dieser Daten enorm erhöhen. Erstens verschlüsselt es im Gegensatz zu früheren Versionen von iOS jetzt praktisch alle Daten auf dem Gerät und schützt sie mit einem Passwort – etwa Kurznachrichten, Fotos, Kontakte und Notizen. Zweitens und am wichtigsten, schließt es faktisch die Möglichkeit aus, dass jemand ohne Passwort Zugang zu den verschlüsselten Daten bekommt. Frühere Betriebssysteme erlaubten Apple, jedes Gerät mit einem Code zu entsperren, der nur dem Unternehmen bekannt war. Bei iOS 8 hingegen hat Apple im Grunde den Schlüssel weggeworfen und deshalb keinen Zugang zu den Daten. Hacker, Cyberkriminelle und Diebe ebenfalls nicht. Und auch nicht Regierungen, ob ausländische oder die eigene.**

Im Juni 2014 kündigte Google eine ähnliche Ende-zu-Ende-Verschlüsselungstechnik für seinen E-Mail-Service Gmail an. Tim Cook, CEO von Apple und bekennender Schwuler, hat eine Reihe eloquenter und ziemlich extremer Statements zum Schutz der Privatsphäre abgegeben und, motiviert durch eigene Erfahrungen, versprochen, Apple werde standhaft die Privatsphäre vor staatlicher Überwachung schützen.

Eine Wunderwaffe ist, wie ich wiederholt geschrieben habe, nichts von alledem: Die NSA wird alles daransetzen, die neuen Verschlüsselungstechniken auszuhebeln. Darüber hinaus sind die Internetunternehmen kaum vertrauenswürdig, denn sie stehen bekanntermaßen der US-Regierung nahe und haben sich oft genug angebiedert. Doch je mehr Menschen einen zuverlässigen Schutz ihrer Privatsphäre fordern, desto stärker der Anreiz für diese Unternehmen, ihre Nutzer standhaft zu schützen und technologische Wälle um deren Kommunikation und Aktivitäten im Internet zu errichten.

Unter mehreren wichtigen Aspekten verläuft hier die Frontlinie im Kampf um die Privatsphäre im digitalen Zeitalter. Die NSA und ihre britischen Kollegen von der GCHQ fahren eine bemerkenswerte Attacke gegen ihre langjährigen Technik-Partner im Privatsektor, um sie zu bewegen, ihre Verschlüsselungsbemühungen wieder aufzugeben. Die Regierungen beider Dienste sind dazu übergegangen, diese Unternehmen öffentlich der Unterstützung von Terroristen und anderen Gewaltverbrechern zu bezichtigen, weil sie deren Kommunikation dem Zugriff der Strafverfolgung entziehen. Im November 2014 machte das britische Parlament in einem Bericht Facebook für das schreckliche Messerattentat auf einen britischen Soldaten im Jahr zuvor verantwortlich. Facebook, so wurde behauptet, habe sich geweigert, die aufrührerischen Internetbeiträge des Angreifers den Behörden zu übergeben.

Dies wirft ein Schlaglicht auf die eigentliche Schlacht, nämlich die zwischen Regierungen auf der einen und dem individuellen Recht auf Privatsphäre auf der anderen Seite, wobei die Internetunternehmen – über die wir miteinander kommunizieren – zwischen die Fronten geraten. Bislang verpflichten sich die Unternehmen weiterhin, den Schutz der Privatsphäre zu verbessern, weil die Öffentlichkeit es von ihnen verlangt. Doch um dafür zu sorgen, dass es Regierun-

gen nicht gelingt, diese Firmen zur Umkehr zu bewegen, muss jeder Einzelne unmissverständlich deutlich machen, dass er keine Dienstleistungen von Unternehmen in Anspruch nimmt, die seine Privatsphäre unterminieren, statt sie zu schützen, und dass der Panikmache, wie sie die US-Regierung und ihre Verbündeten seit 15 Jahren betreiben – indem sie lauthals *Terrorismus* schreien, bis sich die Menschen unterwerfen –, kein Erfolg mehr beschieden ist.

Ein echter politischer Wandel findet nicht über Nacht statt; fast immer vollzieht er sich in Schritten. Außerdem ist er ohne Bewusstseinsveränderung nicht denkbar. Das ist es vor allem, was die Snowden-Enthüllungen bewirkt haben: eine weltweite Debatte über ein breites Themenspektrum, die das Denken der Menschen auf der ganzen Welt beeinflusst hat. Und sie haben gezeigt, dass eine umwälzende Veränderung nach solch einem Ereignis unumgänglich ist. Die einzige Frage ist, wie lange es dauern und was genau dabei herauskommen wird.

Auch zwei Jahre nach dem ersten dazu erschienenen Bericht befinden wir uns noch in den Anfangsstadien eines Wandels, der aus diesen Enthüllungen folgen wird. Dennoch wird zunehmend klar, dass es echte Fortschritte und wirklich positive Veränderungen für all jene gibt, denen die Privatsphäre heilig ist – die an die individuelle Autonomie glauben und den Wert der Demokratie hochhalten.

Rio de Janeiro, 30. Juni 2015
Glenn Greenwald

Einführung

Im Herbst 2005 beschloss ich, einen politischen Blog zu eröffnen, allerdings ohne mir allzu viel davon zu versprechen. Damals hatte ich nicht die geringste Ahnung, wie sehr diese Entscheidung mein Leben verändern würde. Mein Hauptmotiv für den Blog war, dass mich das radikale und extremistische Machtdenken der amerikanischen Regierung nach dem 11. September zunehmend beunruhigte und ich hoffte, mit dem Schreiben über diese Themen mehr erreichen zu können als in meiner bisherigen Laufbahn als Verfassungs- und Zivilrechtler.

Nur sieben Wochen nach dem Start meines Blogs ließ die *New York Times* eine Bombe platzen: Die Bush-Regierung, so berichtete die Zeitung, habe 2001 die National Security Agency (NSA) insgeheim beauftragt, die elektronische Kommunikation von Amerikanern ohne die von den einschlägigen Gesetzen verlangte richterliche Genehmigung zu überwachen. Als dies bekannt wurde, war die unbefugte Ausspähung bereits vier Jahre an der Tagesordnung, und etliche tausend Amerikaner waren unmittelbar betroffen.

Das Thema fügte sich geradezu perfekt in meine Interessens- und Spezialgebiete. Die Regierung rechtfertigte das geheime NSA-Programm, indem sie genau jene extreme Haltung zur Exekutivgewalt vertrat, die mich zum Schreiben motiviert hatte: die Auffassung, die Bedrohung durch den Terrorismus gebe dem Präsidenten praktisch unbegrenzte Befugnisse, wenn es darum ging, die »nationale Sicherheit zu wahren« – das Recht zum Gesetzesbruch eingeschlossen. In

der Debatte darüber wurden komplexe Fragen des Staatsrechts und der Auslegung der Gesetze erörtert, zu denen ich aufgrund meines beruflichen Hintergrunds einen kompetenten Beitrag liefern zu können hoffte.

Die folgenden zwei Jahre schrieb ich – in meinem Blog und in einem 2006 veröffentlichten Buch, das ein Bestseller wurde – über sämtliche Aspekte des NSA-Abhörskandals. Meine Position war klar und eindeutig: Die Anordnung illegaler Lauschangriffe durch den Präsidenten war ein Verbrechen, für das er zur Verantwortung gezogen werden sollte. Im zunehmend chauvinistischen und repressiven Klima der Vereinigten Staaten erwies sich meine Position jedoch als höchst kontrovers.

Vor diesem Hintergrund wählte mich Edward Snowden ein paar Jahre später als die erste Kontaktperson aus, der er Vergehen der NSA in noch viel massiveren Dimensionen enthüllte. Er glaubte, ich würde die Gefahren der Massenüberwachung und der extremen staatlichen Geheimhaltung erkennen und mich keinem Druck seitens der Regierung und ihrer zahlreichen Verbündeten in den Medien und anderswo beugen.

Das umfangreiche Archiv streng geheimer Dokumente, das Snowden mir zukommen ließ, und die hochdramatische Situation, in der er sich befand, haben weltweit ein beispielloses Interesse an der Bedrohung durch elektronische Massenüberwachung und an der Bedeutung der Privatsphäre im digitalen Zeitalter ausgelöst. Dem liegen Probleme zugrunde, die bereits seit Jahren weitgehend unbeachtet im Dunkeln schwelen.

Sicherlich sind viele Aspekte der gegenwärtigen Kontroverse um die NSA ein Novum. Die Technik hat eine allumfassende Bespitzelung ermöglicht, wie sie sich zuvor nur die fantasievollsten Science-Fiction-Autoren ausmalen konnten. Darüber hinaus hat vor allem der amerikanische Sicherheitswahn nach dem 11. September eine Atmosphäre geschaffen,

die ganz besonders zu Machtmissbrauch verleitet. Snowdens mutiger Tat und der Leichtigkeit, mit der sich digitale Informationen kopieren lassen, verdanken wir es, dass wir nun aus erster Hand einen einzigartigen Einblick in die gegenwärtige Funktionsweise des Überwachungssystems haben.

Doch in vielerlei Hinsicht erinnern die Fragen, die durch die NSA-Affäre aufgeworfen werden, an Ereignisse der vergangenen Jahrhunderte. Widerstand gegen staatliche Eingriffe in die Privatsphäre war einer der Hauptfaktoren für die Gründung der Vereinigten Staaten, denn die amerikanischen Kolonisten wehrten sich gegen Gesetze, die britischen Beamten willkürliche Hausdurchsuchungen ermöglichten. Es sei zwar, meinten die Siedler, durchaus legitim, dass der Staat gezielt Nachforschungen über bestimmte Personen anstelle, wenn der Verdacht eines strafbewehrten Fehlverhaltens bestehe. Die generelle Ermächtigung dazu – also die gesamte Bevölkerung unterschiedslos zu überwachen – sei hingegen grundsätzlich rechtswidrig.

Mit dem vierten Verfassungszusatz wurde dieser Gedanke im amerikanischen Recht verankert. Seine Formulierungen sind klar, kurz und bündig: »Das Recht des Volkes auf Sicherheit der Person und der Wohnung, der Urkunden und des Eigentums vor willkürlicher Durchsuchung, Festnahme und Beschlagnahme darf nicht verletzt werden, und Haussuchungs- und Haftbefehle dürfen nur bei Vorliegen eines eidlich oder eidesstattlich erhärteten Rechtsgrundes ausgestellt werden und müssen die zu durchsuchende Örtlichkeit und die in Gewahrsam zu nehmenden Personen oder Gegenstände genau bezeichnen.« Die Absicht war vor allem, in den USA das Recht der Regierung, ihre Bürger einer allgemeinen, auf keinem spezifischen Verdacht beruhenden Überwachung zu unterwerfen, für immer abzuschaffen.

Der Streit um die Überwachung konzentrierte sich im 18. Jahrhundert hauptsächlich auf die Hausdurchsuchungen,

doch mit dem technischen Fortschritt weitete sich die Überwachung aus. Als Mitte des 19. Jahrhunderts der Ausbau des Schienennetzes einen kostengünstigen und schnellen Posttransport möglich machte, löste die heimliche Öffnung der Sendungen durch die britische Regierung in Großbritannien einen großen Skandal aus. In den ersten Jahrzehnten des 20. Jahrhunderts nahm das Bureau of Investigation – der Vorläufer des heutigen FBI – mit Hilfe von Abhörgeräten sowie Postüberwachung und Informanten diejenigen ins Visier, die gegen die amerikanische Politik opponierten.

Unabhängig von der jeweils verwendeten Technik hat die Massenüberwachung seit jeher bestimmte konstante Eigenschaften. Zunächst sind es immer die Regimekritiker und die Randgruppen eines Landes, die vor allem überwacht werden, weniger diejenigen, die die Regierung unterstützen oder einfach so unpolitisch sind, dass sie irrtümlich annehmen, niemand würde sich für sie interessieren. Die Geschichte zeigt, dass allein schon die Existenz eines Apparats zur Massenüberwachung, ganz unabhängig davon, wie er eingesetzt wird, ausreicht, um Andersdenkende zum Schweigen zu bringen.

Eine Untersuchung der inländischen Ausspähaktivitäten des FBI durch das Church Committee Mitte der 1970er Jahre ergab, dass der Geheimdienst eine halbe Million Amerikaner als potenziell »subversiv« einschätzte und routinemäßig Menschen allein auf der Grundlage ihrer politischen Überzeugungen ausspionierte. (Die Liste der Überwachungsziele des FBI reichte von Martin Luther King bis John Lennon, vom Women's Liberation Movement bis zur antikommunistischen John Birch Society.) Doch nicht nur die amerikanische Geschichte ist gezeichnet von der Pest des Überwachungsmissbrauchs. Jede skrupellose Macht neigt zur Massenüberwachung. Und dabei ist das Motiv stets dasselbe: die Unterdrückung jeglicher abweichenden Meinung und die Förderung von Wohlverhalten.

Überwachung ist etwas, das Regierungen ansonsten auffallend unterschiedlicher politischer Ausrichtungen gemeinsam ist. An der Wende zum 20. Jahrhundert schufen das britische Empire und Frankreich eigens Überwachungsministerien, um der Bedrohung durch antikolonialistische Bewegungen entgegenzuwirken. Nach dem Zweiten Weltkrieg war das Ministerium für Staatssicherheit der DDR, allgemein als Stasi bekannt, der Inbegriff für staatliches Eindringen in das persönliche Leben. Und um ein Beispiel aus jüngerer Zeit zu nennen: Als die Volksaufstände im arabischen Frühling die Macht der Diktatoren bedrohten, spionierten die Regime in Syrien, Ägypten und Libyen die Kommunikation ihrer Gegner im Internet aus.

Recherchen der *Bloomberg News* und des *Wall Street Journal* haben gezeigt, dass diese Diktaturen, als sie sich von den Protesten überwältigt sahen, buchstäblich bei westlichen Technologieunternehmen auf Shoppingtour gingen, um Überwachungsinstrumente zu erwerben. Das Assad-Regime in Syrien ließ Angestellte der italienischen Firma Area SpA einfliegen, weil die Regierung, wie ihnen mitgeteilt wurde, »dringend Personen nachspüren müsste«. Die Geheimpolizei des ägyptischen Präsidenten Mubarak kaufte Software, um die Verschlüsselung von Skype zu knacken und Telefonate von Aktivisten abzuhören. Und wie das *Journal* berichtete, standen Journalisten und Rebellen, die 2011 ein Überwachungszentrum der Regierung betraten, vor »einer Wand schwarzer Geräte von der Größe eines Kühlschranks«. Sie stammten von der französischen Firma Amesys. Diese Apparate »kontrollierten den Internet-Verkehr« des wichtigsten Internet-Providers Libyens, »öffneten E-Mails, hackten Passwörter, spionierten in Online-Chats und zeichneten Verbindungen unter Verdächtigen auf«.

Die Kommunikation von Menschen verfolgen zu können verschafft enorme Macht. Und wenn diese Macht nicht durch

eine rigorose Beaufsichtigung und Rechenschaftspflicht unter Kontrolle gehalten wird, wird sie mit allergrößter Wahrscheinlichkeit missbraucht. Zu erwarten, dass die amerikanische Regierung unter vollständiger Geheimhaltung eine riesige Überwachungsmaschine unterhält, ohne ihren Verlockungen zu erliegen, widerspricht einfach den Erfahrungen der Geschichte und der menschlichen Natur.

Schon vor Snowdens Enthüllungen war klar, dass es naiv war zu glauben, in den Vereinigten Staaten gäbe es keine Überwachung. Bei einer Anhörung im Kongress im Jahr 2006 unter dem Titel »Internet in China: Instrument der Freiheit oder der Unterdrückung?« warf ein Redner nach dem anderen amerikanischen Technologieunternehmen vor, sie würden dem chinesischen Staat helfen, abweichende Meinungen im Internet zu unterdrücken. Der republikanische Abgeordnete des Repräsentantenhauses Christopher Smith (New Jersey), der das Hearing leitete, verglich Yahoos Zusammenarbeit mit der chinesischen Geheimpolizei mit dem Verrat, der Anne Frank der Gestapo auslieferte. Es war eine Moralpredigt, wie immer, wenn amerikanische Politiker über ein Regime sprechen, das nicht auf der Linie der Vereinigten Staaten ist.

Dabei hatte, wie selbst den Teilnehmern nicht entgangen war, die *New York Times* erst zwei Monate zuvor über das umfassende illegale Abhörprogramm der Bush-Regierung im Land berichtet. Im Licht dieser Enthüllungen klang die Anprangerung der Überwachungspraxis anderer Länder ziemlich hohl. Der demokratische Abgeordnete Brad Sherman (Kalifornien), der im Anschluss an Smith sprach, meinte denn auch, die Technologieunternehmen, die aufgefordert würden, sich dem chinesischen Regime zu widersetzen, sollten auch gegenüber der eigenen Regierung skeptisch sein. »Sonst«, warnte er prophetisch, »könnte es sein, dass wir, während in China die Privatsphäre aufs schändlichste verletzt wird, hier

in den Vereinigten Staaten vielleicht eines Tages feststellen müssen, dass sich ein Präsident diese großzügige Auslegung der Verfassung zu eigen macht und unsere E-Mails liest. Und ich möchte nicht, dass so etwas ohne richterlichen Beschluss geschieht.«

In den vergangenen Jahrzehnten ist die Angst vor dem Terrorismus – geschürt durch ständige Übertreibung der tatsächlichen Bedrohung – von der amerikanischen Führung missbraucht worden, um ein breites Spektrum extremistischer Maßnahmen zu rechtfertigen. Sie hat zu Angriffskriegen geführt, ein weltweit organisiertes Foltersystem entstehen lassen und ermöglicht, dass Ausländer wie amerikanische Bürger ohne Gerichtsverhandlung festgenommen oder sogar umgebracht werden. Aber das allgegenwärtige System der Überwachung ohne Verdachtsanlass, das sich unter Ausschluss der Öffentlichkeit ausgebreitet hat, erweist sich am Ende womöglich als dauerhaftes Erbe dieser Politik. Und zwar deshalb, weil der derzeitige NSA-Überwachungsskandal trotz aller historischen Parallelfälle eine wirklich neue Dimension hat – bedingt durch die Rolle des Internets im alltäglichen Leben.

Insbesondere für die jüngere Generation ist das Internet keine Domäne, die nur für bestimmte Zwecke benutzt wird. Es ist nicht nur unser Postamt und unser Telefon, sondern das Epizentrum unserer Welt – der Ort, wo sich praktisch das ganze Leben abspielt. Im Internet werden Freundschaften geschlossen, Lektüre und Filme ausgewählt, politische Aktionen organisiert, die privatesten Daten erstellt und gespeichert. Dort entwickeln wir unsere Persönlichkeit und unser Selbstgefühl und bringen es zum Ausdruck.

Aus *diesem* Netzwerk ein System zur Massenüberwachung zu machen hat Folgen, die bislang mit den Überwachungsprogrammen keines Landes vergleichbar sind. Alle vorherigen Ausspähsysteme waren zwangsläufig begrenzt,

und man konnte sich ihnen entziehen. Wenn wir zulassen, dass die Überwachung fest im Internet verankert wird, werden mehr oder weniger alle Formen des menschlichen Austauschs, Planens und sogar Denkens einer umfassenden staatlichen Kontrolle unterworfen.

Als das Internet breite Nutzung zu finden begann, sprachen ihm viele ein großes Potenzial zu: die Möglichkeit, Hunderte Millionen Menschen durch die Demokratisierung des politischen Diskurses zu befreien und die Machtlosen auf Augenhöhe mit den Mächtigen zu bringen. Die Freiheit des Internets – die Möglichkeit, dieses Netzwerk ohne institutionelle Einschränkungen, soziale oder staatliche Kontrolle und angstfrei zu nutzen – ist für die Erfüllung dieses Versprechens unabdingbar. Die Umwandlung des Internets in ein Überwachungssystem raubt ihm genau dieses entscheidende Potenzial – ja, es macht das Internet zu einem Instrument der Unterdrückung und droht, die schrecklichste und repressivste Waffe staatlicher Einmischung zu werden, die es in der Geschichte der Menschheit je gegeben hat.

Genau deshalb sind Snowdens Enthüllungen so ungeheuerlich und enorm wichtig. Indem er gewagt hat, die atemberaubenden Überwachungsmöglichkeiten der NSA und deren noch frappierendere Zielsetzungen ans Tageslicht zu bringen, hat er deutlich gemacht, dass wir uns an einem historischen Scheideweg befinden. Wird das digitale Zeitalter die Befreiung des Individuums und die politischen Freiheiten bringen, die das Internet in einzigartiger Weise realisieren kann? Oder wird es ein System omnipräsenter Überwachung und Kontrolle etablieren, das sich nicht einmal die schlimmsten Tyrannen der Vergangenheit hätten träumen lassen? Im Augenblick stehen uns beide Wege offen. Unser Handeln wird darüber bestimmen, wo wir am Ende landen.

1
Kontaktaufnahme

Am 1. Dezember 2012 erhielt ich zum ersten Mal eine Nachricht von Edward Snowden, obwohl ich damals noch nicht wusste, dass sie von ihm stammte.

Der Kontakt kam durch eine E-Mail zustande, die mir jemand mit dem Pseudonym Cincinnatus geschickt hatte – eine Anspielung auf Lucius Quinctius Cincinnatus, einen römischen Bauern, der im 5. Jahrhundert vor Christus zum Diktator Roms ernannt wurde mit dem Auftrag, die Stadt gegen die Angriffe von Nachbarvölkern zu verteidigen. In Erinnerung geblieben ist er der Nachwelt vor allem wegen dem, was er nach seinem Sieg über die Feinde Roms tat: Er legte unverzüglich und aus freien Stücken sein Amt nieder und bestellte wieder seine Felder. Gepriesen als »Vorbild bürgerlicher Tugendhaftigkeit« wurde Cincinnatus zum Symbol für den Einsatz politischer Macht im Sinne des Gemeinwohls, für die Beschränkung oder sogar Aufgabe der Macht des Einzelnen zugunsten der Allgemeinheit.

Die E-Mail begann mit den Worten: »Es liegt mir sehr am Herzen, dass Menschen sicher miteinander kommunizieren können«, und verfolgte den Zweck, mich zur Verwendung der PGP-Verschlüsselung zu bewegen; dann, so »Cincinnatus«, könne er mir Informationen zukommen lassen, die für mich sicherlich von Interesse seien. PGP steht für *pretty good privacy,* »ziemlich gute Privatsphäre«. Das ausgeklügelte Hilfsprogramm dient dazu, E-Mails und andere Formen der Online-Kommunikation vor Ausspähung und Hackeran-

griffen zu schützen. Durch das seit 1991 verfügbare Programm wird jede E-Mail praktisch mit einem Schutzschild umgeben, der aus einem Code mit Hunderten oder sogar Tausenden von zufälligen Zahlen und nach Groß-/Kleinschreibung unterschiedenen Buchstaben besteht.

Die modernsten Geheimdienste der Welt – zu denen die NSA zweifellos gehört – verfügen über Entschlüsselungssoftware, die eine Milliarde Codes pro Sekunde abfragen kann. Aber selbst die ausgefeilteste Software benötigt mehrere Jahre, um so lange, zufällig generierte Passwörter wie die der PGP-Verschlüsselung zu knacken. Personen, die sich vor einer Ausspähung ihrer Kommunikation besonders in Acht nehmen müssen – etwa Geheimdienstmitarbeiter, Spione, mit der nationalen Sicherheit befasste Journalisten, Menschenrechtsaktivisten und Hacker –, benutzen diese Form der Verschlüsselung zum Schutz ihrer Nachrichten. In seiner E-Mail schrieb »Cincinnatus«, er habe überall nach meinem »öffentlichen Schlüssel« von PGP gesucht – einer einzigartigen Codeliste, die den Empfang verschlüsselter E-Mails ermöglicht –, ihn aber nicht finden können. Daraus folgerte er, dass ich das Programm nicht benutzte, und meinte: »Damit setzen Sie jeden, der mit Ihnen kommuniziert, einem Risiko aus. Ich behaupte nicht, dass jede Information, die man austauscht, verschlüsselt sein muss, aber Sie sollten Ihren Kommunikationspartnern zumindest diese Möglichkeit geben.«

»Cincinnatus« verwies dann auf den Skandal um General David Petraeus, dessen außereheliche Affäre mit der Journalistin Paula Broadwell durch die über Google ausgetauschten E-Mails aufgedeckt wurde und den General seine Karriere kostete.

Hätte Petraeus seine E-Mails verschlüsselt, bevor er sie per Gmail verschickte oder in seinem Mailordner abspeicherte, wären sie für die Ermittler nicht zu lesen gewesen. »Verschlüsselung ist etwas Essenzielles, nicht nur für Spione und

Schürzenjäger«, so »Cincinnatus«. Das Verschlüsseln von E-Mails sei »eine absolut unerlässliche Sicherheitsmaßnahme für jeden, der sich mit Ihnen in Verbindung setzen will«.

Damit ich seinen Rat beherzigte, fügte er hinzu: »Da draußen gibt es Leute, von denen Sie gern hören würden. Sie werden aber niemals Kontakt zu Ihnen aufnehmen können, solange nicht gewährleistet ist, dass ihre Nachrichten bei der Datenübertragung nicht gelesen werden.«

Dann bot er an, mir bei der Installation des Programms behilflich zu sein. »Wenn Sie Hilfe brauchen, geben Sie mir bitte Bescheid oder suchen Sie sich alternativ jemanden über Twitter. Sie haben viele technisch versierte Follower, die Sie dabei jederzeit gerne unterstützen.« Er unterschrieb mit: »Danke, C.«

Eine Verschlüsselungssoftware zu benutzen hatte ich mir eigentlich schon lange vorgenommen. Ich schrieb seit Jahren über WikiLeaks, Whistleblower, das Hacktivisten-Kollektiv Anonymous und ähnliche Themen und kommunizierte gelegentlich auch mit Angehörigen der nationalen Sicherheitsbehörden. Die meisten von ihnen sind sehr auf sicheren Informationsaustausch bedacht und wollen unerwünschte Überwachung vermeiden.

Die Nutzung von PGP ist jedoch ziemlich kompliziert, vor allem für jemanden wie mich, der zu dem Zeitpunkt von Programmierung und Computern sehr wenig Ahnung hatte. So blieb es eben bei dem Vorsatz.

C.s E-Mail brachte mich auch nicht dazu, endlich aktiv zu werden. Da ich als investigativer Journalist bekannt bin, bieten mir ständig alle möglichen Leute eine »Riesenstory« an, die sich normalerweise als heiße Luft entpuppt. Außerdem arbeite ich praktisch immer an mehr Storys, als ich bewältigen kann. Ich brauche also schon etwas Konkretes, damit ich das, was ich gerade tue, stehen und liegen lasse und mich auf eine neue Fährte begebe. Trotz der vagen Andeutung von

»Leuten da draußen«, von denen ich »gern hören würde«, war nichts in C.s E-Mail, was mich wirklich locken konnte. Ich las die Mail, antwortete aber nicht darauf.

Drei Tage später hörte ich wieder von C., als er mich bat, den Empfang seiner ersten Nachricht zu bestätigen. Diesmal antwortete ich schnell: »Ich habe sie erhalten und arbeite daran. Ich habe noch keinen PGP-Schlüssel und weiß auch nicht, wie das geht, aber ich werde versuchen, jemanden zu finden, der mir helfen kann.«

Noch am selben Tag antwortete er mit einer einfachen Schritt-für-Schritt-Anleitung für PGP – im Prinzip eine Einführung in die Verschlüsselung für Anfänger. Am Ende des Textes, den ich ziemlich schwierig und verwirrend fand, was größtenteils meiner Unkenntnis geschuldet ist, schrieb C., das seien nur »die simpelsten Grundlagen. Wenn Sie niemanden finden, der Sie bei der Installation, Schlüsselerzeugung und Benutzung unterstützt, lassen Sie es mich bitte wissen. Ich kann fast überall auf der Welt Kontakt zu Leuten herstellen, die sich mit Kryptographie auskennen.«

Seine E-Mail endete diesmal etwas pointierter:

Mit kryptographischen Grüßen
Cincinnatus

Trotz meiner guten Vorsätze nahm ich mir nie die Zeit, mich mit Verschlüsselung zu beschäftigen. Sieben Wochen vergingen, und mein Versäumnis bereitete mir ein wenig Kopfzerbrechen. Was, wenn dieser Mensch wirklich eine wichtige Story hatte, die mir nur deshalb durch die Lappen ging, weil ich ein Computerprogramm nicht installiert hatte? Abgesehen davon: Selbst wenn Cincinnatus doch nichts Interessantes für mich hatte, könnte mir ein Verschlüsselungsprogramm künftig durchaus von Nutzen sein.

Am 28. Januar 2013 mailte ich ihm, dass ich mir von jeman-

dem mit der Verschlüsselung helfen lassen würde und die Sache hoffentlich in ein oder zwei Tagen erledigt sei.

Er antwortete mir am nächsten Tag: »Das ist sehr erfreulich! Wenn Sie weitere Hilfe benötigen oder später noch Fragen haben, können Sie mich gerne kontaktieren. Meinen herzlichsten Dank dafür, dass Sie die Privatsphäre in der Kommunikation unterstützen! Cincinnatus.«

Aber wieder einmal tat ich nichts, denn ich hatte damals mehr Storys auf dem Schreibtisch, als ich erledigen konnte, und war noch immer nicht davon überzeugt, dass C. irgendetwas Lohnendes für mich hatte. Auf Geheiß einer mir unbekannten Person ein Verschlüsselungsprogramm zu installieren erschien mir nie vordringlich genug, um deshalb alles andere stehen und liegen zu lassen. So blieb es einfach einer der vielen Punkte auf meiner stets viel zu langen To-do-Liste.

C. und ich steckten also in einer Zwickmühle. Er war nicht bereit, mir etwas über seine Informationen zu verraten – ja nicht einmal zu enthüllen, wer er war und wo er arbeitete –, solange ich nicht die Verschlüsselungssoftware installiert hatte. Aber ohne den Anreiz näherer Details sah ich keine Notwendigkeit, seiner Bitte nachzukommen und mir die Zeit für die Installation des Programms zu nehmen.

Angesichts meiner Untätigkeit verstärkte C. seine Bemühungen. Er erstellte ein zehnminütiges Video mit dem Titel »PGP für Journalisten«. Mit Hilfe einer Software, die eine Computerstimme erzeugt, wurde ich ganz einfach und Schritt für Schritt durch den Installationsprozess der Verschlüsselungssoftware geführt, samt Bildern und Anschauungsmaterial.

Doch ich unternahm immer noch nichts. Zu diesem Zeitpunkt machte sich bei C., wie er mir später sagte, allmählich Enttäuschung breit. Er dachte sich: »Da riskiere ich meine Freiheit, vielleicht sogar mein Leben, um diesem Mann Tausende streng vertraulicher Dokumente des verschwiegensten

Geheimdienstes des Landes zu übergeben – ein Leak, aus dem sich Dutzende, wenn nicht gar Hunderte von sensationellen journalistischen Knüllern machen lassen –, und er rafft sich nicht mal dazu auf, ein Verschlüsselungsprogramm zu installieren.«

So knapp war ich also davor, eine der größten und folgenreichsten Enthüllungen um die Nationale Sicherheit, die es in der Geschichte der Vereinigten Staaten je gegeben hat, an mir vorbeigehen zu lassen.

Bis ich in dieser Angelegenheit wieder etwas hörte, vergingen zehn Wochen. Am 18. April flog ich von Rio de Janeiro, wo ich wohne, nach New York, um über die Gefahren staatlicher Geheimhaltungspolitik und Verstöße gegen die Bürgerrechte zu sprechen, die im Namen des Antiterrorkriegs begangen wurden.

Nach der Landung auf dem John-F.-Kennedy-Flughafen sah ich, dass ich eine E-Mail von der Dokumentarfilmerin Laura Poitras erhalten hatte. Sie schrieb: »Bist du vielleicht zufällig kommende Woche in den USA? Ich würde mich gern mal wegen einer bestimmten Sache mit dir in Verbindung setzen, aber am liebsten persönlich.«

Nachrichten, die ich von Laura Poitras bekomme, nehme ich grundsätzlich sehr ernst. Sie ist einer der zielstrebigsten und furchtlosesten Menschen, die ich kenne, und hat unter den riskantesten Umständen zahlreiche Filme gedreht, ohne eine Filmcrew oder den Rückhalt einer Nachrichtenagentur, nur mit einem bescheidenen Budget, einer Kamera und ihrer Entschlossenheit. Als der Irakkrieg am heftigsten tobte, wagte sie sich ins sunnitische Dreieck, wo sie *My Country, My Country* drehte – die unverbrämte Darstellung eines Alltags unter amerikanischer Besatzung, die für einen Oscar in der Sparte Dokumentarfilm nominiert wurde.

Ihr nächster Film, *The Oath,* führte Laura Poitras in den

Jemen, wo sie über Monate hinweg zwei jemenitische Männer begleitete: Osama bin Ladens Leibwächter und seinen Fahrer. Seitdem arbeitete Poitras an einer Dokumentation über die Überwachung durch die NSA. Diese drei Filme, angelegt als Trilogie über das Verhalten der USA im Antiterrorkampf, machten sie zur ständigen Zielscheibe von Schikanen seitens der US-Behörden, wann immer sie ein- oder ausreiste.

Durch Laura lernte ich eine wichtige Lektion. Als wir uns 2010 erstmals begegneten, war sie bei der Einreise in die oder der Ausreise aus den Vereinigten Staaten mehr als drei Dutzend mal von Beamten des Heimatschutzministeriums festgehalten worden – man verhörte sie, drohte ihr, beschlagnahmte ihre Materialien einschließlich Laptops, Notebooks und Kameras. Dennoch entschied sie sich immer wieder dagegen, diese ständigen Belästigungen an die Öffentlichkeit zu bringen, aus Angst vor Konsequenzen, die ihre Arbeit unmöglich machen würden. Das änderte sich erst nach einem besonders verletzenden Verhör am Flughafen Newark. Laura hatte die Nase voll. »Es wird nur schlimmer, nicht besser, wenn ich den Mund halte.« Nun war sie damit einverstanden, dass ich darüber schrieb.

In dem Artikel, veröffentlicht im Online-Magazin *Salon,* schilderte ich ausführlich die permanenten Verhöre, denen sich Poitras ausgesetzt sah. Er sorgte für beträchtliches Aufsehen; viele Leser bekundeten ihre Solidarität und verurteilten diese Schikanen. Als Poitras nach der Veröffentlichung wieder aus den Vereinigten Staaten ausreiste, wurde sie nicht vernommen – auch ihr Filmmaterial wurde nicht beschlagnahmt. In den nächsten Monaten gab es keinerlei Schikanen mehr. Zum ersten Mal seit Jahren konnte sie wieder unbehelligt reisen.

Wir waren uns einig, welche Lehre sich daraus ziehen ließ: Die Beamten der Nationalen Sicherheit scheuen das Licht.

Sie werden ausfallend und brutal, wenn sie sich unbeobachtet glauben, im Dunkeln. Geheimhaltung, so stellten wir fest, ist der Dreh- und Angelpunkt für Machtmissbrauch, er wird dadurch erst ermöglicht. Das einzig wirksame Gegenmittel ist Transparenz.

Als ich Lauras E-Mail am John-F.-Kennedy-Flughafen gelesen hatte, antwortete ich sofort: »Bin tatsächlich gerade heute Morgen in den Staaten gelandet. Wo bist du?« Wir verabredeten uns für den nächsten Tag in der Lobby meines Hotels in Yonkers und setzten uns ins Restaurant. Auf Lauras Drängen hin wechselten wir vor Beginn unseres Gesprächs zweimal den Tisch, um sicherzugehen, dass uns niemand belauschte. Laura kam gleich zur Sache. Sie habe eine »enorm wichtige und heikle Angelegenheit« zu besprechen, sagte sie, und Sicherheitsmaßnahmen seien unerlässlich.

Da ich mein Handy dabeihatte, bat Laura mich, entweder den Akku herauszunehmen oder es in meinem Hotelzimmer zu lassen. »Es hört sich paranoid an«, sagte sie, aber die Regierungsbehörden hätten die Möglichkeit, Mobiltelefone und Laptops ferngesteuert zu Abhörgeräten umzufunktionieren. Das Ausschalten der Geräte genüge nicht, man müsse den Akku entfernen.

Davon hatten mir auch schon Transparenz-Aktivisten und Hacker erzählt, aber ich neigte dazu, es als übertriebene Vorsichtsmaßnahme abzutun. Diesmal nahm ich es jedoch ernst, weil es von Laura kam. Nachdem ich festgestellt hatte, dass sich der Akku meines Handys nicht herausnehmen ließ, brachte ich es auf mein Zimmer und kehrte anschließend ins Restaurant zurück.

Jetzt begann Laura zu reden. Sie hatte mehrere anonyme E-Mails von jemandem erhalten, der sowohl ehrlich als auch glaubwürdig zu sein schien. Er behauptete, Zugang zu Dokumenten der höchsten Geheimhaltungsstufe zu haben, aus

denen hervorgehe, dass die amerikanische Regierung ihre eigenen Bürger und den Rest der Welt bespitzle. Er beabsichtige, diese Dokumente zu enthüllen, und habe ausdrücklich darum gebeten, dass sie, Laura, bei der Veröffentlichung und bei der Berichterstattung darüber mit mir zusammenarbeiten sollte. In diesem Moment stellte ich noch keinen Zusammenhang zu den längst vergessenen E-Mails her, die ich vor Monaten von Cincinnatus bekommen hatte.

Dann zog Laura ein paar Blätter Papier aus ihrem Rucksack, zwei Ausdrucke der E-Mails, die der anonyme Informant geschickt hatte. Ich las sie am Tisch durch, von Anfang bis Ende – und war gefesselt.

Die zweite E-Mail, einige Wochen nach der ersten verschickt, begann so: »Bin noch da.« Bezüglich der Frage, die Laura am meisten interessierte – wann werden Sie in der Lage sein, uns Dokumente zukommen zu lassen? – schrieb er: »Ich kann nur sagen: bald.«

Nachdem der Informant Laura eingeschärft hatte, vor jedem Gespräch über sensible Themen immer den Akku aus dem Handy zu nehmen – oder es zumindest in einen Kühlschrank zu legen, wo es nur noch begrenzt zum Abhören taugte –, teilte er ihr mit, dass sie bei diesen Dokumenten mit mir zusammenarbeiten sollte. Dann kam er zum Kern dessen, was er als seine Mission betrachtete:

Der Schock dieser Anfangsphase [nach den ersten Enthüllungen] wird für den nötigen Rückhalt sorgen, um ein auf mehr Parität basierendes Internet aufzubauen, aber dieses wird keine Vorteile für den Durchschnittsmenschen bringen, sofern nicht die Wissenschaft schneller voranschreitet als das Gesetz.

Wir können gewinnen, wenn wir begreifen, durch welche Mechanismen unsere Privatsphäre verletzt wird. Mit Hilfe universeller Gesetze können wir sicherstellen, dass alle Menschen den gleichen Schutz gegen eine unzumutbare Überwachung genießen, jedoch nur, wenn die Tech-

niker- und Entwickler-Community bereit ist, sich dieser Gefahr zu stellen, und sich verpflichtet, Overengineering-Lösungen einzusetzen. Letztlich müssen wir ein Prinzip durchsetzen, durch das die Mächtigen nur so viel Privatsphäre genießen können, wie auch den gewöhnlichen Menschen zugestanden wird: ein den Gesetzen der Natur, nicht der Politik des Menschen unterworfenes Prinzip.

»Es ist echt«, sagte ich, nachdem ich das gelesen hatte. »Ich kann nicht erklären, warum, aber ich spüre einfach intuitiv, dass es ihm ernst ist und dass er wirklich derjenige ist, als der er sich ausgibt.«

»Sehe ich auch so«, erwiderte Laura. »Ich habe kaum Zweifel.«

Vernünftig und rational betrachtet, war Laura und mir durchaus klar, dass unser Vertrauen in die Aufrichtigkeit des Informanten möglicherweise fehl am Platz war. Wir hatten keine Ahnung, wer ihr da geschrieben hatte. Es konnte jeder x-Beliebige sein. Jemand, der sich das alles nur aus den Fingern gesogen hatte. Denkbar war auch, dass uns eine Regierungsbehörde damit eine Falle stellen und uns zur Zusammenarbeit mit einem kriminellen Informanten verleiten wollte. Vielleicht steckte auch jemand dahinter, der unsere Glaubwürdigkeit erschüttern wollte, indem er uns gefälschte Dokumente zur Veröffentlichung zuspielte.

Wir gingen all diese Möglichkeiten durch. Wie wir wussten, hatte die US Army im Jahr 2008 in einem geheimen Bericht WikiLeaks zum Staatsfeind erklärt und empfohlen, die Enthüllungsplattform »zu schädigen, gegebenenfalls auch zu vernichten«. Der Bericht (der ironischerweise an WikiLeaks durchgesickert war) erwähnte auch die Weitergabe gefälschter Dokumente als eine Möglichkeit. Wenn WikiLeaks sie als authentisch veröffentlichte, würde das die Glaubwürdigkeit der Organisation massiv beeinträchtigen.

Laura und ich waren uns all dieser Fallstricke bewusst,

doch wir ließen uns davon nicht beirren und vertrauten auf unsere Intuition. Diese E-Mails strahlten etwas Nichtgreifbares, aber Energisches aus, was uns davon überzeugte, dass ihr Urheber es ehrlich meinte. Er schrieb aus einer tief empfundenen Haltung heraus, die seine Besorgnis gegenüber geheimdienstlichem Treiben und zunehmender Überwachung erkennen ließ. Intuitiv spürte ich, welche politische Leidenschaft in ihm brannte; ich fühlte mich ihm verwandt in seiner Weltsicht und der Dringlichkeit seines Anliegens.

In den letzten sieben Jahren hatte mich die gleiche Überzeugung angetrieben; beinahe täglich hatte ich gegen die gefährlichen Entwicklungen in der Geheimhaltungspolitik der USA angeschrieben, gegen radikale Rechtsauslegungen der Exekutivgewalten, grundlose Festnahmen und Bespitzelungen, Militarismus und Beschneidung bürgerlicher Rechte. Es gibt einen bestimmten Ton, eine Denkweise, die Journalisten, Aktivisten und meine Leser verbindet – Menschen, die über diese Entwicklungen alle gleichermaßen besorgt sind. Für jemanden, der diese Betroffenheit nicht wirklich spüren und nachvollziehen kann, so dachte ich mir, wäre es schwierig, sie so genau und authentisch nachzuahmen.

Gegen Ende seiner E-Mails an Laura schrieb der Verfasser, dass er die letzten notwendigen Maßnahmen ergreifen werde, um uns die Dokumente zukommen zu lassen. Er brauche noch vier bis sechs Wochen. Wir sollten warten, bis wir Nachricht von ihm bekämen; er würde sich melden, darauf könnten wir uns verlassen.

Drei Tage später trafen Laura und ich uns wieder, diesmal in Manhattan und mit einer weiteren E-Mail des anonymen Informanten. Darin teilte er uns mit, dass er bereit sei, seine Freiheit aufs Spiel zu setzen und das Risiko einer höchstwahrscheinlich sehr langen Haftstrafe auf sich zu nehmen, um diese Dokumente an die Öffentlichkeit zu bringen. Jetzt hatte ich keine Zweifel mehr: Unser Informant meinte es

ernst. Aber auf dem Rückflug nach Brasilien sagte ich zu meinem Lebensgefährten David Miranda, ich wolle nicht allzu viele Gedanken daran verschwenden. »Vielleicht wird ja gar nichts daraus. Er könnte ja seine Meinung ändern – oder erwischt werden.« David ist ein Mensch mit einer ausgeprägten Intuition, und er war seltsam zuversichtlich. »Er meint es ernst. Daraus wird was«, erklärte er, »und es wird eine Riesengeschichte.«

Nach der Rückkehr nach Rio herrschte drei Wochen lang Funkstille. Ich verschwendete nicht allzu viele Gedanken an unseren Informanten, weil ich ohnehin nur abwarten konnte. Am 11. Mai bekam ich dann eine E-Mail von einem Technikexperten, mit dem Laura und ich früher zusammengearbeitet hatten. Seine Worte klangen kryptisch, aber die Bedeutung war klar: »Hallo Glenn, ich wollte nachhaken wegen Ihres Einstiegs in PGP. Haben Sie eine Adresse, an die ich Ihnen etwas schicken kann, damit Sie nächste Woche anfangen können?«

Ich war mir sicher, dass die angekündigte Lieferung das enthielt, was ich brauchte, um mit der Arbeit an den Dokumenten des Informanten beginnen zu können. Folglich musste Laura inzwischen von unserem unbekannten E-Mail-Schreiber gehört und das bekommen haben, worauf wir gewartet hatten.

Der Techniker versandte daraufhin ein Päckchen per Federal Express, das ich binnen zwei Tagen erhalten sollte. Ich wusste nicht, was mich erwarten würde: ein Programm oder gleich die Dokumente? In den nächsten 48 Stunden konnte ich mich auf nichts anderes mehr konzentrieren. Aber am angekündigten Liefertag wartete ich bis 17.30 Uhr, ohne dass irgendetwas ankam. Ich rief bei FedEx an und erfuhr, das Päckchen sei »aus unbekannten Gründen« vom Zoll zurückgehalten worden.