REDLINE | VERLAG

Bruce Schneier

DATA UND GOLIATH

Die Schlacht um die Kontrolle unserer Welt

Wie wir uns gegen Überwachung, Zensur und Datenklau wehren müssen

Bruce Schneier

Data und Goliath
Die Schlacht um die Kontrolle unserer Welt

Bruce Schneier

Data und Goliath

Die Schlacht um die Kontrolle unserer Welt

Wie wir uns gegen Überwachung, Zensur und Datenklau wehren können

Übersetzung aus dem amerikanischen Englisch von Sigrid Schmid und Claudia Van Den Block

REDLINE | VERLAG

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über **http://d-nb.de** abrufbar.

Für Fragen und Anregungen:
lektorat@redline-verlag.de

1. Auflage 2015

Nymphenburger Straße 86
D-80636 München
Tel.: 089 651285-0
Fax: 089 652096

Die englische Originalausgabe erschien 2015 bei W. W. Norton & Company Inc. unter dem Titel *Data and Goliath*.

Übersetzung: Sigrid Schmid und Claudia Van Den Block
Redaktion: Desirée Šimeg, Gersthofen
Umschlaggestaltung: Melanie Melzer, unter Verwendung von iStockphoto.com
Satz: Carsten Klein, München
Druck: CPI books GmbH, Leck
Printed in Germany

ISBN Print 978-3-86881-596-2
ISBN E-Book (PDF) 978-3-86414-742-5
ISBN E-Book (EPUB, Mobi) 978-3-86414-743-2

Weitere Informationen zum Verlag finden Sie unter

www.redline-verlag.de

Inhalt

Einleitung

Wer noch nicht davon überzeugt ist, in einer Science-Fiction-Welt zu leben, der werfe einmal einen Blick auf sein Handy. Dieses nette, unglaublich nützliche Hochglanzteil nimmt mittlerweile einen derart zentralen Platz in unserem Leben ein, dass es für uns schon ganz selbstverständlich geworden ist. Anscheinend ist es völlig normal, dieses Gerät an jedem beliebigen Ort der Erde aus der Tasche zu ziehen und damit mit jemandem zu sprechen, ganz gleich wo auf dem Planeten derjenige sich gerade befindet.

Doch jeden Morgen, wenn wir unser Handy einstecken, lassen wir uns mit dem Betreiber auf einen stillen Handel ein: »Ich möchte mobil telefonieren und erreichbar sein, im Gegenzug erlaube ich diesem Unternehmen, immer zu wissen, wo ich mich befinde.« Diesen Handel regelt kein Vertrag, er gehört aber unabdingbar zum Service. Wahrscheinlich haben Sie sich darüber bisher gar keine Gedanken gemacht, doch nachdem ich Sie nun darauf aufmerksam gemacht habe, könnten Sie denken, dieser Handel sei eigentlich ziemlich gut. Handys sind schließlich echt toll, und damit sie funktionieren, muss die Mobilfunkgesellschaft ja wissen, wo Sie gerade stecken, also muss sie Sie überwachen.

Es handelt sich um eine sehr intime Form der Überwachung. Ihr Handy gibt an, wo Sie wohnen und wo Sie arbeiten. Es gibt an, wie oft Sie zur Kirche gehen (und in welche Kirche), wie viel Zeit Sie in Kneipen verbringen und ob Sie zu schnell fahren. Außerdem – da es all die anderen Telefone in Ihrer Umgebung ebenfalls kennt –, gibt es an, mit wem Sie tagsüber zu tun haben, wen Sie zum Mittagessen treffen und mit wem Sie ins Bett gehen.[1] Diese gesammelten Informationen geben wahrscheinlich exakter darüber Aufschluss, wie Sie Ihre Zeit verbringen, als Sie selbst das können, denn Daten sind nicht so lückenhaft wie die menschliche Erinnerung.[2] Im Jahr 2012 konnten Analysten anhand solcher Daten bis auf 20 Meter genau voraussagen, wo eine Person sich *in 24 Stunden* befinden würde.[3]

Wollte man vor dem Siegeszug der Handys all diese Informationen über Sie haben, hätte man Sie beschatten lassen müssen. Man hätte einen Privatdetektiv angeheuert, der Ihnen überallhin folgt und sich Notizen macht.

Das ist nun nicht mehr notwendig: Das Handy in Ihrer Tasche erledigt das ganz automatisch. Es ist natürlich nicht gesagt, dass jemand wirklich auf diese Informationen zugreift, doch sie stehen auf Abruf bereit.

Die Information, wo Sie sich befinden, ist wertvoll, und jeder möchte Zugriff darauf haben. Die Polizei ganz bestimmt. Die Analyse von Handystandortdaten ist in mehrfacher Hinsicht nützlich für polizeiliche Ermittlungen.[4] Die Polizei kann einem bestimmten Telefon eine stille SMS schicken, um es zu orten, sie kann anhand des Datenverlaufs feststellen, wo es war, und sie kann sämtliche Mobilfunkortungen eines bestimmten Gebiets analysieren, um zu ermitteln, wer sich wann dort aufgehalten hat.[5] Immer häufiger verwendet die Polizei diese Daten genau zu diesen Zwecken.[6]

Regierungen nutzen dieselben Daten zu Einschüchterungsversuchen und sozialer Kontrolle. Im Jahr 2014 schickte die ukrainische Regierung folgende wahrlich orwellianische SMS an Personen in Kiew, deren Handys sich zu einem bestimmten Zeitpunkt an einem bestimmten Ort befanden: »Sehr geehrter Kunde, Sie wurden als Teilnehmer an einem Massenaufruhr erfasst.«[7] Doch glauben Sie bloß nicht, so etwas beschränke sich auf totalitäre Staaten! Im Jahr 2010 holte die Polizei von Michigan Informationen über jedes eingeschaltete Mobiltelefon in der Nähe eines erwarteten Streiks ein[8] – einen richterlichen Beschluss hielt sie nicht für notwendig.

Ein ganzer Industriezweig hat sich darauf verlegt, zu orten, wo Sie sich gerade befinden. Firmen verwenden Ihr Handy, um Sie in Geschäften zu lokalisieren und zu verstehen, wie Sie einkaufen; um Sie auf der Straße zu orten und zu bestimmen, wie weit entfernt Sie sich von einem bestimmten Laden befinden; und um Ihnen passende Werbung auf Ihr Handy zu schicken, je nachdem, wo Sie gerade sind.[9] Ihre Standortdaten sind so wertvoll, dass Mobilfunkanbieter sie nun an Datenbroker weiterverkaufen,[10] die sie wiederum jedem Zahlungswilligen feilbieten. Firmen wie Sense Networks[11] sind darauf spezialisiert, anhand dieser Daten von jedem von uns ein persönliches Profil zu erstellen.

Mobilfunkbetreiber sind aber nicht die einzige Quelle für Mobilfunkdaten. Das US-Unternehmen Verint verkauft Ortungssysteme an Unternehmen sowie Regierungen weltweit.[12] Auf der Firmenwebsite heißt es, die Firma sei »ein weltweit führendes Unternehmen in Actionable-Intelligence-Lösungen für die Optimierung des Kundendialogs, Sicherheitsüberwachung

und Betrug, Risiko und Compliance« mit Kunden bei »mehr als 10 000 Organisationen in über 180 Ländern«.[13] Die britische Firma Cobham verkauft ein System, mit dem man still ein anderes Telefon anrufen kann – es klingelt nicht und der Anruf ist auch nicht zurückverfolgbar. Doch dieser stille Anruf zwingt das Mobiltelefon, auf einer bestimmten Frequenz zu senden, sodass der Anrufer das Telefon auf einen Meter genau orten kann.[14] Stolz brüstet sich das Unternehmen, dass Regierungen aus Algerien, Brunei, Ghana, Pakistan, Saudi-Arabien, Singapur und den Vereinigten Staaten zu seinem Kundenkreis zählen.[15] Das ominös in Panama registrierte Unternehmen Defentek verkauft ein System, das »jede Telefonnummer der Welt orten und verfolgen kann … ohne Spuren im Netzwerk, beim Betreiber oder der Zielperson zu hinterlassen«.[16] Das sind keine leeren Versprechungen, der Telekommunikationsexperte Tobias Engel demonstrierte genau dies 2008 bei einer Hackerkonferenz.[17] Heutzutage haben längst Kriminelle diese Technik für sich entdeckt.

Diese Form der Standortbestimmung basiert auf dem Mobilfunknetz, doch in Ihrem Smartphone ist noch ein ganz anderes und viel exakteres Ortungssystem integriert: GPS. Damit werden die verschiedenen Apps auf Ihrem Telefon mit Standortdaten versorgt. Manche Apps benutzen diese Informationen, um eine Dienstleistung zu erbringen: Google Maps, Uber, Yelp. Andere, wie Angry Birds, wollen sie nur sammeln und verkaufen.[18] Auch Sie selbst können diese Technologie nutzen: Hello Spy ist eine App, die Sie heimlich auf dem Smartphone einer anderen Person installieren können, um diese dann regelmäßig zu orten.[19] Ideal für die ängstliche Mutter, die ihrem Teenager hinterherspionieren will – oder für den eifersüchtigen Mann, der Ehefrau oder Freundin überwachen will.[20] Arbeitgeber haben solche Apps auch schon zur Überwachung ihrer Angestellten genutzt.[21]

Die nationale Sicherheitsbehörde der USA (National Security Agency, kurz NSA) und ihr britisches Äquivalent, das Government Communications Headquarters (GCHQ), verwenden Standortdaten, um Menschen zu überwachen. Die NSA sammelt Mobilfunkdaten verschiedener Quellen: von den Mobilfunktürmen, mit denen sich Mobilfunkgeräte vernetzen, vom Standort von Wi-Fi-Netzwerken, in die sich Handys einloggen, und von GPS-Daten von Internet-Apps.[22] Zwei interne NSA-Datenbanken mit den Decknamen Happyfoot und Fascia enthalten umfangreiche Stand-

ortdaten von Mobilfunkgeräten weltweit. Die NSA nutzt diese Datenbanken, um die Bewegungen von Menschen zu überwachen, um Personen zu identifizieren, die mit für die NSA interessanten Personen Umgang haben, und um Drohnenangriffe zu steuern. Angeblich kann die NSA Handys auch dann orten, wenn sie abgeschaltet sind.[23]

Bisher ging es nur um Standortdaten aus einer Quelle – dem Handy –, doch das ist noch längst nicht das Ende der Fahnenstange. Die Computer, die Sie nutzen, generieren ständig ganz intime, persönliche Informationen über Sie. Das beginnt mit Ihren Vorlieben bei Lektüre, Filmen und Musik, geht weiter damit, mit wem Sie kommunizieren und was Sie sagen, und hört damit auf, worüber Sie sich Gedanken machen – zumindest wenn diese Gedanken Sie ins Internet und zu Suchmaschinen führen. Wir leben im goldenen Zeitalter der Überwachung.[24]

Der CEO von Sun Microsystems, Scott McNealy, sagte es bereits 1999 geradeheraus: »Du hast sowieso keine Privatsphäre. Gewöhn dich dran.«[25] Natürlich hat er nicht recht damit, wie wir auf diese Überwachung reagieren sollten, doch dass es immer schwieriger wird, Überwachung zu umgehen und die eigene Privatsphäre zu wahren, stimmt. »Überwachung« ist ein politisch und emotional sehr aufgeladener Begriff, dennoch verwende ich ihn ganz bewusst. Das US-Militär definiert Überwachung als »systematisches Beobachten«.[26] Wie ich später noch ausführen werde, ist die moderne elektronische Überwachung genau das. Jeder von uns ist sowohl für Regierungen als auch für Unternehmen ein offenes Buch; ihre Möglichkeiten, unser kollektives persönliches Leben zu durchleuchten, sind umfangreicher denn je.

Der Handel, auf den Sie sich immer wieder mit verschiedenen Firmen einlassen, heißt Überwachung im Austausch für kostenlose Dienste. Eric Schmidt, Chairman bei Google, und Jared Cohen, Direktor von Google Ideas, erklärten dies ausführlich in ihrem 2013 erschienenen Buch *Die Vernetzung der Welt*. Ich paraphrasiere: Wenn ihr uns all eure Informationen überlasst, zeigen wir euch Werbung, die euch interessiert, dazu geben wir euch eine kostenlose Suchmaschine, E-Mail und alle möglichen anderen Dienste.[27] Im Grunde geht es um Bequemlichkeit. Wir sind soziale Wesen, und nichts ist wirkungsvoller und erfüllender für uns, als mit anderen zu kommunizieren. Am einfachsten und besten kommuniziert man mittlerweile eben digital.

Und warum gewähren wir den Regierungen Zugang? Aus Angst vor Terroristen, vor Fremden, die unsere Kinder entführen, vor Drogendealern – und welche Bösewichte eben sonst gerade angesagt sind. Das ist die Rechtfertigung der NSA für die Programme zur Massenüberwachung: Wenn ihr uns all eure Informationen überlasst, befreien wir euch von dieser Angst.[28] Das Problem ist, dass dieser Handel weder gut noch gerecht ist, zumindest nicht, wie er sich heute darstellt. Wir haben uns zu leichtfertig darauf eingelassen, ohne die Bedingungen auch nur ansatzweise richtig zu verstehen.

Die Wahrheit ist: Die heutige Technologie ermöglicht Regierungen und Unternehmen fundamentale Massenüberwachung. Massenüberwachung ist gefährlich. Sie öffnet der Diskriminierung in jeder Hinsicht Tür und Tor: Rasse, Religion, soziale Herkunft, politische Überzeugungen. Sie wird benutzt, um zu kontrollieren, was wir sehen, was wir tun können und letztlich auch was wir sagen. Sie wird durchgeführt, ohne dass der Bürger Regressansprüche oder auch nur die Möglichkeit hätte, sich dagegen zu entscheiden. Wirkungsvolle Kontrollinstanzen gibt es nicht.

Massenüberwachung beschneidet unsere Sicherheit. Sie beschneidet unsere Freiheit. Die Regeln, die wir einst unter früheren Vorzeichen aufgestellt haben, um uns vor diesen Gefahren zu schützen, genügen längst nicht mehr, sie greifen nicht. Das müssen wir korrigieren, und zwar schleunigst.

Das zeige ich im vorliegenden Buch in drei Teilen.

Teil I beschreibt die Überwachungsgesellschaft, in der wir leben. Kapitel 1 betrachtet die verschiedenen persönlichen Informationen, die wir tagein, tagaus generieren. Nicht nur die Mobilfunkstandortdaten, von denen bereits die Rede war, sondern auch Informationen über unsere Telefongespräche, E-Mails und SMS und alle Websites, die wir besuchen, unsere finanziellen Transaktionen und vieles mehr. Den meisten von uns ist gar nicht richtig klar, wie sehr alles, was wir tun, von Computern geprägt ist, oder dass das Speichern von Daten so billig geworden ist, dass alles, was wir von uns geben, auf ewig aufbewahrt werden kann. Zudem unterschätzen die meisten von uns, wie einfach es ist, uns anhand von Informationen zu identifizieren, die wir für anonym halten.

Kapitel 2 zeigt auf, wie all diese Informationen zur Überwachung eingesetzt werden. Das geschieht überall, es geschieht automatisch und ohne menschliche Interaktion – und größtenteils ohne dass wir davon Kenntnis nehmen. Es handelt sich um allgegenwärtige Massenüberwachung.

Es fällt leicht, sich darauf zu fokussieren, wie Daten von Unternehmen und Regierungen gesammelt werden, doch dabei entsteht ein verzerrtes Bild. Die eigentliche Geschichte handelt davon, wie die verschiedenen Datenströme verarbeitet, miteinander verbunden und analysiert werden. Dabei geht es nicht nur um die Informationen einer einzelnen Person, sondern um die Daten aller. Allgegenwärtige Massenüberwachung unterscheidet sich fundamental von der Summe vieler Einzelüberwachungen, und sie geschieht in einem ungekannten Ausmaß. Darum geht es in Kapitel 3.

Überwachungsdaten werden vor allem von den Firmen gesammelt, mit denen wir entweder als Kunden oder als Benutzer interagieren. Kapitel 4 handelt von der Überwachung als Geschäftsmodell, vor allem über personalisierte Werbung. Ein ganzer Industriezweig ist rund um Informationsbroker entstanden. Dabei profitiert man von unseren Daten, unsere persönlichen Informationen werden ohne unser Wissen und Einverständnis ge- und verkauft. Vorangetrieben wird dies durch ein neues Computerverfahren, bei dem unsere Daten in einer Cloud gespeichert und von verschiedenen Geräten wie dem iPhone abgerufen werden, die sich unter der strikten Kontrolle des Herstellers befinden. So kommt es, dass Unternehmen in völlig neuem Ausmaß Zugang zu und Kontrolle über unsere intimsten Informationen haben.

In Kapitel 5 wenden wir uns der staatlichen Überwachung zu. Weltweit überwachen Regierungen ihre Bürger und verschaffen sich sowohl im eigenen Land als auch international Zugang zu Computern. Sie möchten jeden ausspähen, um Terroristen und Verbrecher zu finden, und – abhängig von der Regierung – politische Aktivisten, Dissidenten, Umweltaktivisten, Verbraucherschützer und Freidenker. Ich konzentriere mich vor allem auf die NSA, weil wir diesen Nachrichtendienst dank der von Edward Snowden veröffentlichten Dokumente am besten kennen.

Sowohl Unternehmen als auch Regierungen haben einen unersättlichen Appetit auf unsere Daten, und in Kapitel 6 erläutere ich, wie sie zusammenarbeiten. Ich nenne das eine »öffentlich-private Überwachungspart-

nerschaft«, und diese Allianz ist tief verwurzelt. Sie ist der Hauptgrund dafür, dass die Überwachung sich durch alle Bereiche zieht, und sie verhindert sämtliche Versuche, das System zu reformieren.

All das ist wichtig, selbst wenn man den Unternehmen, mit denen man zu tun hat, und der Regierung, unter der man lebt, vertraut. Mit diesen Informationen im Hinterkopf wendet sich Teil II den vielen miteinander verwobenen Schäden zu, welche die allgegenwärtige Massenüberwachung verursacht.

In Kapitel 7 geht es um Schäden, die von der Überwachung seitens der Regierung verursacht werden. In der Vergangenheit konnte man immer wieder sehen, wie gefährlich es ist, Regierungen unkontrolliert Massenüberwachung ihrer Bürger durchführen zu lassen. Zu den möglichen Gefahren gehören Diskriminierung und Machtmissbrauch; die Auswirkungen auf freie Meinungsäußerung und Gedankenfreiheit lassen einen schaudern. Missbrauch von Massenüberwachung ist kaum zu vermeiden, Demokratie und Freiheit sind in Gefahr. Das Internet hat das Potenzial, die Freiheit weltweit zu fördern, doch wir vergeuden es, indem wir zulassen, dass Regierungen global Massenüberwachungen durchführen.

Kapitel 8 widmet sich dem Schaden, der von uneingeschränkter Überwachung durch Firmen verursacht wird. Private Unternehmen haben nun die Kontrolle über die »Orte« im Internet, an denen wir uns aufhalten, und sie beuten die Informationen, die wir hinterlassen, zu ihrem Vorteil aus. Wenn wir Firmen alles über uns wissen lassen, erlauben wir ihnen, uns in Schubladen zu stecken und uns zu manipulieren. Diese Manipulation geschieht größtenteils im Verborgenen und ohne jegliche Kontrolle, und sie wird immer effektiver, je besser die Technologie dahinter wird.

Allgegenwärtige Überwachung schadet zudem auf einer weiteren Ebene: Kapitel 9 diskutiert wirtschaftliche Schäden, insbesondere für US-Unternehmen, die entstehen, wenn Bürger verschiedener Länder versuchen, sich gegen die Überwachung durch die NSA und ihre Verbündeten zu wehren. Das Internet ist eine globale Plattform, und Versuche von Ländern wie Deutschland und Brasilien, nationale Mauern um die eigenen Daten zu bauen, kosten Firmen, die Überwachung durch die Regierung zulassen – insbesondere amerikanische Unternehmen – eine Menge Geld.

In Kapitel 10 geht es darum, welche Schäden der Verlust von Privatsphäre verursacht. Menschen, die Überwachung verteidigen – von der Stasi der DDR über den chilenischen Diktator Augusto Pinochet bis hin zu Eric Schmidt von Google –, berufen sich immer und immer wieder auf die alte Leier: »Wer nichts zu verbergen hat, hat nichts zu befürchten.« Doch der Wert von Privatsphäre wird auf diese Weise gefährlich reduziert. Privatsphäre ist ein menschliches Grundbedürfnis, für die Kontrolle über unsere Beziehungen zur Welt ist sie von zentraler Bedeutung. Jemandem seine Privatsphäre zu verwehren, kommt einer Entmenschlichung gleich. Ob die Überwachung von verdeckten Ermittlern durchgeführt wird, die uns verfolgen, oder von Computeralgorithmen, die jede unserer Bewegungen aufzeichnen, spielt dabei keine Rolle.

Kapitel 11 handelt davon, inwiefern Überwachung der Sicherheit schadet. Die Massenüberwachung durch Regierungen wird immer als Nutzen für die Sicherheit dargestellt, als Schutz vor Terrorismus. Doch es gibt keinen Beweis dafür, dass wir der Massenüberwachung tatsächlich Erfolge im Kampf gegen den Terrorismus zu verdanken hätten. Im Gegenteil! Es gibt signifikante Beweise dafür, dass sie sogar schadet. Für eine allgegenwärtige Massenüberwachung muss das Internet unsicher bleiben. Doch damit sind wir alle weniger geschützt vor fremden Regierungen, Kriminellen und Hackern.

Teil III widmet sich schließlich der Frage, was für den Schutz vor Überwachung durch die Regierung und Unternehmen nötig ist. Die Schutzmaßnahmen sind so kompliziert wie die Ausgangslage, und häufig muss man ganz genau hinsehen. Bevor ich mich auf spezifische technische und strategische Empfehlungen verlege, stelle ich in Kapitel 12 acht Grundprinzipien vor, die unser Denken leiten sollten.

In den beiden folgenden Kapiteln geht es dann um ganz konkrete Empfehlungen: für den Umgang mit Regierungen in Kapitel 13, für den Umgang mit Unternehmen in Kapitel 14. Einige dieser Empfehlungen sind detaillierter als andere, und manche präsentieren eher ein ideales Ziel als ein sofort umsetzbares Mittel. Doch alle sind von Bedeutung, und eine davon wegzulassen könnte die anderen Lösungen gefährden.

Kapitel 15 wendet sich dem zu, was jeder von uns im Einzelnen tun kann. Ich biete praktische technische Hilfestellungen an sowie Vorschläge für poli-

tische Aktionen. Wir leben in einer Welt, in der sowohl die Technologie die Politik übertrumpfen kann als auch umgekehrt die Politik die Technologie übertrumpft. Für wirkliche Sicherheit müssen sie Hand in Hand arbeiten.

Ich ende in Kapitel 16 mit der Überlegung, was wir kollektiv als Gesellschaft tun müssen. Für die meisten Empfehlungen in Kapitel 13 und 14 müssen wir zunächst einmal unsere Wahrnehmung von Überwachung und vom Wert der Privatsphäre verändern, denn ernst zu nehmende Gesetzesreformen wird es erst geben, wenn die Gesellschaft sie fordert. Denn Daten für medizinische Forschung, die Verbesserung des Bildungssystems und andere gesellschaftlich bedeutende Aufgaben zu sammeln, ist beispielsweise durchaus nützlich. Wir müssen also einen Weg finden, wie wir diesen Nutzen bewahren und gleichzeitig die Gefahren minimieren können. Das ist der Grundgedanke, auf dem alles in diesem Buch basiert.

Data und Goliath behandelt viele Punkte und dabei ist es notwendig, nicht zu lange bei einem Thema zu verweilen. In den Anmerkungen finden diejenigen, die tiefer eintauchen möchten, Links und Literaturhinweise. Diese sind auch auf der Webseite des Buchs zu finden: www.schneier.com/dg.html.

Ich schreibe von einer stark amerikanischen Warte aus. Die meisten Beispiele stammen aus den USA und die meisten meiner Empfehlungen sind besonders für die USA geeignet. Zum einen kenne ich dieses Land am besten. Doch ich glaube auch, dass die Vereinigten Staaten sich gut als Beispiel eignen, um aufzuzeigen, was schiefgelaufen ist. Zudem haben die USA die einzigartige Möglichkeit, die Dinge zum Besseren zu verändern.

Ich komme aus dem Sicherheits- und Technologiebereich. Seit Jahren schreibe ich schon darüber, welche Auswirkungen Sicherheitstechnologie auf Menschen hat und umgekehrt. Ich habe miterlebt, wie im Informationszeitalter Überwachung immer zentraler wurde, und kenne die vielen Bedrohungen und Sicherheitslücken in dieser neuen Welt. Sicherheitsprobleme zu durchdenken und soziale Themen im Hinblick auf diese zu betrachten, ist mir in Fleisch und Blut übergegangen. Aus dieser Perspektive verstehe ich sowohl die Probleme als auch die Lösungen ausgezeichnet.

Weder ich noch dieses Buch sind technologiefeindlich. Das Internet und das Informationszeitalter allgemein haben der Gesellschaft enorm viel ge-

bracht. Ich glaube daran, dass dies auch weiterhin der Fall sein wird. Ich bin nicht einmal überwachungsfeindlich. Dass Computer wissen, was wir tun, hat unser Leben positiv verändert. Überwachung hat traditionelle Produkte und Dienstleistungen revolutioniert und völlig neue Märkte geschaffen. Für die Polizei ist sie ein wertvolles Instrument. Sie hilft Menschen überall auf der Welt in vielerlei Hinsicht, und das wird auch so bleiben.

Trotzdem sind die Bedrohungen, die von Überwachungsmaßnahmen ausgehen, echt, und sie werden nicht ausreichend diskutiert. Unsere Reaktion auf das gruselige Überwachungsthema war bislang ziemlich passiv. Wir denken über die Verträge, die wir eingehen, nicht nach, weil sie uns nicht schwarz auf weiß vor die Nase gelegt wurden. Technologischer Wandel geschieht, und größtenteils akzeptieren wir ihn. Man kann uns schwerlich einen Vorwurf machen; der Wandel ging so schnell vonstatten, dass wir seine Auswirkungen noch gar nicht richtig evaluiert haben. So sind wir in eine Überwachungsgesellschaft geraten. Die Überwachungsgesellschaft hat sich leise angeschlichen.

So muss es nicht sein, aber dazu müssen wir die Zügel in die Hand nehmen. Anfangen können wir, indem wir die Verträge, die wir bezüglich unserer Daten eingehen, neu durchdenken. Wir müssen selbst aktiv bestimmen, wie wir mit neuen Technologien umgehen. Wir müssen uns Gedanken darüber machen, wie unsere technologische Infrastruktur aussieht und welche Werte sie verkörpern soll.[29] Den Wert, den unsere Daten für die Gesellschaft haben, müssen wir damit in Einklang bringen, dass sie persönlich sind. Wir müssen unsere Ängste analysieren und uns entscheiden, wie viel Privatsphäre wir für unsere Bequemlichkeit opfern wollen. Wir müssen uns der vielen Gefahren bewusst sein, die von übermächtiger Überwachung ausgehen.

Und wir müssen uns zur Wehr setzen.

– Minneapolis, Minnesota und Cambridge, Massachusetts, Oktober 2014

Teil I
Die Welt, die wir erschaffen

1. Daten als Nebenprodukt von Computern

Computer produzieren unaufhörlich Daten. Sie werden mit Daten gefüttert und spucken wiederum Daten aus, aber Daten entstehen auch als Nebenprodukt sämtlicher Berechnungen. Normalerweise dokumentieren Computer ständig, was sie tun. Sie erfassen mehr, als uns bewusst ist.

Ihr Textverarbeitungsprogramm speichert beispielsweise alles, was Sie schreiben, auch die Entwürfe und Korrekturen. Wenn Sie auf »Speichern« klicken, speichert das Textverarbeitungsprogramm die neue Version, doch Ihr Computer löscht alte Versionen erst dann, wenn er den Speicherplatz für etwas anderes benötigt. Das Textverarbeitungsprogramm speichert ein Dokument in regelmäßigen Abständen automatisch; Microsoft Word speichert meine Dokumente beispielsweise alle 20 Minuten. Außerdem speichert Word, wer das Dokument erstellt hat, und oft auch, wer sonst noch daran gearbeitet hat.

Sobald man eine Internetverbindung herstellt, multiplizieren sich die Daten, die man produziert: Gespeichert wird, welche Websites Sie besuchen, welche Werbung Sie anklicken, welche Wörter Sie eingeben. Ihr Computer, die Websites, die Sie besuchen, und die Computer im Netzwerk produzieren allesamt Daten. Ihr Browser sendet Daten zu Websites, welche Software Sie haben, wann sie installiert wurde, welche Funktionen Sie aktiviert haben et cetera. In vielen Fällen genügen diese Daten, um Ihren Computer eindeutig zu identifizieren.[30]

Die Kommunikation mit Familie, Freunden, Kollegen und Bekannten findet zunehmend über den Computer statt. Bei diesem sozialen Kontakt über E-Mail, SMS, Facebook, Twitter, Instagram, Snapchat, WhatsApp und was sonst noch aktuell angesagt ist entstehen als Nebenprodukt Daten. Diese Systeme übermitteln nicht nur Daten, sie kreieren auch Datenprotokolle von Ihrer Interaktion mit anderen.

Wenn Sie draußen spazieren gehen, denken Sie vermutlich, dass Sie keine Daten produzieren, doch das stimmt nicht. Ihr Handy berechnet stets seine Position anhand der nächsten Mobilfunktürme. Ihrem Anbieter ist es

zwar ziemlich egal, wo Sie sich aufhalten, doch wo Ihr Handy sich befindet, muss er wissen, um Ihre Telefonanrufe dorthin leiten zu können.

Natürlich produzieren Sie, wenn Sie das Handy wirklich benutzen, noch mehr Daten: gewählte Telefonnummern, empfangene Anrufe, gesendete und empfangene SMS, Anrufdauer et cetera. Handelt es sich um ein Smartphone, ist es zugleich ja auch ein Computer, und sämtliche Apps produzieren bei der Nutzung Daten – manchmal sogar, wenn sie gar nicht benutzt werden. Ihr Handy hat wahrscheinlich einen GPS-Empfänger, der noch genauere Informationen über Ihren aktuellen Standort produziert, als es anhand der Mobilfunktürme alleine möglich wäre. Der Mobilfunkturm grenzt Ihren Aufenthaltsort auf einige Hundert Meter ein, doch der GPS-Empfänger Ihres Smartphones lokalisiert Sie bis auf 5 bis 8 Meter.[31]

Mit jedem Einkauf in einem Laden produzieren Sie weitere Daten. Die Kasse ist ein Computer, der speichert, was Sie an welchem Tag und zu welcher Uhrzeit gekauft haben. Diese Daten fließen in das Computersystem des Händlers. Wenn Sie nicht bar bezahlt haben, ist Ihre Kredit- oder Bankkarteninformation mit diesem Einkauf verknüpft. Die Informationen werden auch an die Kreditkartenfirma gesendet, und einige davon gelangen mit der Monatsrechnung wieder zu Ihnen zurück.

Im Geschäft könnte auch eine Videokamera installiert sein, die im Falle von Diebstahl oder Betrug Beweismaterial aufnehmen soll. Eine andere Kamera nimmt Sie auf, wenn Sie Geld am Geldautomaten abheben. Draußen gibt es noch mehr Kameras, die Gebäude, Gehwege, Straßen oder andere öffentliche Plätze im Auge behalten.

Auch im Auto produzieren Sie Daten. Moderne Autos sind vollgestopft mit Computern, die Informationen über Ihre Geschwindigkeit sammeln, wie stark Sie auf die Pedale treten, in welcher Position das Lenkrad ist und vieles andere mehr.[32] Vieles davon wird automatisch in einem Unfalldatenschreiber gespeichert, mit dem man im Falle des Falles den Unfallhergang rekonstruieren kann.[33] Selbst in den Reifen befindet sich je ein Computer, der Informationen über den Reifendruck sammelt. Bringt man sein Auto in die Werkstatt, wird der Kfz-Mechaniker dort zu Diagnosezwecken als Erstes all diese Daten abrufen. Ein selbst fahrendes Auto könnte pro Sekunde ein Gigabyte an Daten generieren.[34]

Bei jedem Schnappschuss ist es ebenso. Digitalfotos enthalten Informationen wie das Datum der Fotoaufnahme, die Uhrzeit und den Ort – ja, viele Kameras besitzen ein GPS; auch allgemeine Informationen über die Kamera, das Objektiv und die Einstellungen sowie eine ID-Nummer der Kamera selbst werden gespeichert.[35] Wenn das Foto dann ins Netz hochgeladen wird, sind diese Informationen häufig nach wie vor mit der Datei verknüpft.[36]

Das war nicht immer so. Im Zeitalter von Zeitung, Radio und Fernsehen erhielten wir zwar Informationen, doch dieser Vorgang wurde nirgends protokolliert. Nun beziehen wir Nachrichten und Unterhaltung aus dem Internet. Früher unterhielten wir uns mit anderen von Angesicht zu Angesicht, dann über das Telefon; heute kommunizieren wir über SMS oder E-Mail. Früher kauften wir mit Bargeld in einem Laden ein, heute mit Kreditkarten über das Internet. Früher steckte man noch Münzen in den Fernsprecher einer Telefonzelle oder in den Fahrkartenautomaten oder in die Parkuhr. Heute nutzen wir automatische Zahlungssysteme wie EZPass, die an unser Nummernschild und unsere Kreditkarte gebunden sind.[37] In Taxis konnte man früher nur bar bezahlen, später dann mit Kreditkarte und mittlerweile nutzen wir unser Smartphone, um auf vernetzte Taxisysteme wie Uber und Lyft zuzugreifen, die Daten zur Transaktion sowie über Start- und Endpunkt der Fahrt speichern. Mit einigen wenigen Ausnahmen sind Computer nun überall dort im Einsatz, wo wir mit Handel, und an den meisten Orten, an denen wir mit Freunden zu tun haben.

Letztes Jahr, als mein Kühlschrank kaputt war, wurde der Computer, der ihn regelt, vom Kundendienst ausgetauscht. Mir wurde schlagartig klar, dass ich meinen Kühlschrank bislang immer völlig falsch betrachtet hatte: Das ist kein Kühlschrank mit einem Computer, sondern ein Computer, der Lebensmittel kühlt. Und nach diesem Schema verwandelt sich immer mehr in einen Computer. Das Telefon ist ein Computer, mit dem man telefonieren kann. Das Auto ist ein Computer mit Rädern und einem Motor. Der Ofen ist ein Computer, der Lasagne backen kann. Die Kamera ist ein Computer, der fotografiert. Selbst unsere Haus- und Nutztiere bekommen nun regelmäßig einen Chip. Meine Katze ist also eigentlich auch ein Computer, der den ganzen Tag in der Sonne döst.

Computer werden in immer mehr Produkte eingebaut, die mit dem Internet verbunden werden können. Ein Unternehmen namens Nest, das Goog-

le für rund 3 Milliarden Dollar gekauft hat, stellt internetfähige Thermostate her. Das intelligente Thermostat passt sich an Ihr Verhalten an und reagiert auf erhöhte Aktivität in Ihrem Energienetz. Dafür muss es allerdings sowohl Ihren Energieverbrauch überwachen als auch die Temperatur, Luftfeuchtigkeit, Umgebungshelligkeit und sämtliche Bewegungen in der Nähe registrieren.[38] Man kann auch einen intelligenten Kühlschrank kaufen, der das Verfallsdatum von Lebensmitteln im Auge behält,[39] sowie eine intelligente Klimaanlage, die Ihre Vorlieben erlernen und die Energieffizienz optimieren kann.[40] Noch mehr dergleichen kommt auf den Markt: Nest verkauft nun einen intelligenten Rauch- und Kohlenmonoxidmelder und plant darüber hinaus eine ganze Serie intelligenter Haushaltsgeräte.[41] All dies brauchen wir, wenn wir ein intelligentes Stromnetz errichten wollen, das den Energieverbrauch und die Treibhausgasemission reduzieren soll.[42]

Mittlerweile sammeln und analysieren wir für unsere Gesundheit und unser Wohlergehen auch Daten über unseren Körper. Wenn Sie ein Gerät für Fitness-Tracking wie Fitbit oder Jawbone tragen, sammelt dieses Informationen über Ihre Bewegungen im Schlaf und im Wachzustand und analysiert anhand der Daten Ihre Schlaf- und Trainingsgewohnheiten. Es kann so feststellen, wann Sie Sex haben.[43] Wenn Sie dem Gerät mehr über sich verraten – wie viel Sie wiegen, was Sie essen –, dann erfahren Sie noch mehr.[44] All diese Daten, die Sie freiwillig teilen, sind natürlich online einsehbar.

Viele medizinische Geräte sind mittlerweile internetfähig. Sie sammeln und übermitteln eine ganze Reihe von biometrischen Daten.[45] Inzwischen gibt es schon – oder zumindest bald – Geräte, die ständig unsere Vitalfunktionen, unsere Laune und unsere Hirnströme messen können. Nicht nur spezielle Geräte tun das, auch Smartphones haben heutzutage ziemlich empfindliche Bewegungssensoren.[46] Wenn der Preis für DNA-Sequenzierungen weiterhin fällt, werden mehr Menschen diese nutzen und ihr Erbgut analysieren lassen. Firmen wie 23andMe wollen anhand der genetischen Informationen ihrer Kunden Gene ausfindig machen, die mit bestimmten Krankheiten verbunden sind, und so neue und sehr gewinnträchtige Medikamente dagegen auf den Markt bringen.[47] Sie sprechen auch von personalisiertem Marketing,[48] und Versicherungsgesellschaften könnten irgendwann Daten von ihnen kaufen, anhand derer sie unternehmerische Entscheidungen treffen.[49]

Das Extrem bei diesem Trend zum datenproduzierenden Ich ist wohl Lifelogging: Unaufhörlich werden dabei persönliche Daten erfasst. Man kann schon heute Lifelogging-Apps installieren, die die Aktivitäten auf dem Smartphone protokollieren, also wann man sich mit Freunden unterhält, Spiele spielt, Filme ansieht et cetera.[50] Doch das ist nur ein Schatten dessen, was Lifelogging einmal darstellen wird. In Zukunft wird ein Videotagebuch dazugehören.[51] Google Glass ist das erste tragbare Gerät mit diesem Potenzial, doch andere folgen auf dem Fuß.[52]

Einige Beispiele aus dem Internet der Dinge:[53] Umweltsensoren können den Verschmutzungsgrad bestimmen, intelligente Inventur- und Kontrollsysteme können Abfall vermeiden und Geld sparen, Computer mit Internetzugang werden überall eingebaut – intelligente Städte,[54] intelligente Zahnbürsten,[55] intelligente Glühlampen,[56] intelligente Gehwegpflaster,[57] intelligente Tablettenröhrchen,[58] intelligente Kleidung[59] – warum auch nicht?[60] Schätzungen zufolge sind 10 Milliarden Geräte derzeit mit dem Internet verbunden. Das sind bereits mehr, als Menschen auf diesem Planeten leben, und es gibt Prognosen, dass es bis 2020 bereits 30 Milliarden sein werden.[61] Um diese Geräte wird ein ziemlicher Hype gemacht[62] und es ist noch ungewiss, welche Anwendungen sich durchsetzen und welche im Sande verlaufen werden. Klar ist jedoch, dass sie alle Daten produzieren, und zwar eine Menge. Die Dinge um uns herum werden zu Augen und Ohren des Internets.[63]

Diese allgegenwärtige Konnektivität stellt ein gewaltiges Problem für die Privatsphäre dar. Zwar können diese intelligenten Anwendungen die CO_2-Emissionen reduzieren, doch ebenso sammeln sie Daten darüber, wie sich Menschen zu Hause bewegen und wie sie ihre Zeit verbringen. Intelligente Straßenlaternen werden Daten darüber sammeln, wie Menschen sich auf der Straße bewegen.[64] Die Kameras werden immer besser, kleiner und mobiler sein.[65] Raytheon möchte 2015 ein Prallluftschiff über Washington, D. C., und Baltimore fliegen lassen und testen, wie gut sich damit »Zielobjekte« – vermutlich Fahrzeuge – zu Wasser, zu Land und in der Luft verfolgen lassen.[66]

Letztlich haben wir täglich mit Hunderten von Computern zu tun und bald werden es Tausende sein. Jeder einzelne Computer produziert Daten. Nur sehr wenig davon ist wirklich interessant: was wir im Restaurant bestellt haben, unser Puls beim abendlichen Joggen oder unser letzter Liebesbrief.

Vielmehr gehört ein Großteil der Daten zu den sogenannten *Metadaten*. Das sind Daten über Daten – Informationen, mit denen ein Computer arbeitet, oder Daten, die ein Nebenprodukt dieser Berechnungen sind. Bei einer SMS gehört die Nachricht selbst zu den Daten, doch das Benutzerkonto, von dem sie gesendet wurde, und das Empfängerkonto sowie Datum und Uhrzeit der Nachricht sind alles Metadaten. Ein E-Mail-System ist ähnlich: Der Text der E-Mail ist ein Datensatz, doch Absender, Empfänger, Informationen zum Routing und die Länge der Nachricht sind Metadaten – über die Einordnung der Betreffzeile lässt sich streiten.[67] Bei einem Foto gehört das Bild selbst zu den Daten, das Datum und die Aufnahmezeit, die Kameraeinstellungen, die Seriennummer der Kamera und die GPS-Koordinaten des Fotos sind Metadaten. Diese Metadaten klingen vielleicht langweilig, doch das sind sie ganz und gar nicht – ich erkläre es Ihnen gleich genauer.

Der Datensmog, den wir produzieren, hat übrigens nicht unbedingt mit der Unaufrichtigkeit von irgendjemandem zu tun. Meist handelt es sich einfach um ein Nebenprodukt von Computern. So funktioniert Technologie heute eben. Daten sind die Abgase des Informationszeitalters.

Wie viele Daten?

Eine schlichte Rechenübung. Ihr Laptop hat wahrscheinlich eine 500-Gigabyte-Festplatte. Die große externe Festplatte, die Sie sich für Backups gekauft haben, kann vielleicht zwei oder drei Terabyte speichern. Das Netzwerk Ihrer Firma könnte tausendmal so viel Speicherplatz haben: 1 Petabyte. Es gibt auch Namen für noch größere Zahlen. 1000 Petabytes sind 1 Exabyte (eine Milliarde Milliarden Bytes), 1000 Exabytes sind 1 Zettabyte und 1000 Zettabytes 1 Yottabyte. Etwas anschaulicher ausgedrückt: Ein Exabyte Daten sind 500 Milliarden Seiten Text.[68]

So kommt einiges an Datenmüll zusammen. 2010 generierten wir Menschen mehr Daten pro Tag als vom Anbeginn der Zeiten bis 2003.[69] Ab 2015 dürften rund 76 Exabytes an Daten jährlich durch das Internet reisen.[70]

Beim Gedanken an diese Datenmenge lassen sich Bedenken über das Speichern und die Nutzung von Daten leicht mit dem Argument beiseitewischen, dass es zu viele Daten seien, um sie zu speichern, und es zu

schwierig wäre, sie auf winzige Goldkörnchen von aussagekräftigen Informationen zu durchsuchen. Das stimmte früher auch.

In den frühen Jahren des Computers wurden die meisten dieser Daten – und gewiss die meisten Metadaten – gelöscht, kurz nachdem sie erzeugt wurden. Sie zu speichern hätte zu viel Speicherkapazität gebraucht. Doch alles, was mit Computern zu tun hat, wurde im Laufe der Zeit immer billiger, und was man vor zehn Jahren noch schlecht speichern und verarbeiten konnte, stellt heutzutage kein Problem mehr dar. 2015 kostet 1 Petabyte Speicherkapazität in einer Cloud 100 000 Dollar, das sind 90 Prozent weniger als noch 2011, als es 1 Million Dollar kostete.[71] Als Konsequenz werden immer mehr Daten gespeichert.

Sie könnten wahrscheinlich jeden Tweet, der jemals gesendet wurde, auf der Festplatte Ihres Computers zu Hause speichern.[72] Um Mitschnitte aller Telefongespräche der USA zu speichern, braucht man weniger als 300 Petabyte oder 30 Millionen Dollar pro Jahr.[73] Ein Lifelogger bräuchte für seine ständigen Videoaufnahmen 700 Gigabytes pro Jahr. Multipliziert man das mit der Bevölkerungszahl der USA, bräuchte man 2 Exabyte pro Jahr, die momentan 200 Millionen Dollar kosten. Das ist zwar viel Geld, doch der Preis ist nachvollziehbar und wird noch weiter fallen. 2013 wurde das riesige Utah Data Center der NSA in Bluffdale fertiggestellt.[74] Es ist momentan das drittgrößte der Welt[75] und das erste von weiteren geplanten Datenzentren. Die Details sind geheim, doch Experten gehen davon aus, dass etwa 12 Exabyte Daten dort gespeichert werden können.[76] Bisher hat es 1,4 Milliarden Dollar gekostet.[77] Google hat weltweit eine Speicherkapazität von 15 Exabyte.[78]

Was für Organisationen gilt, gilt auch für Individuen. Nehmen wir mich als Beispiel. E-Mails schreibe ich seit 1993. Das E-Mail-Archiv kommt mir vor wie ein Teil meines Gehirns. Es sind meine Erinnerungen. Mindestens einmal pro Woche suche ich in diesem Archiv nach etwas: nach einem Restaurant, in dem ich vor Jahren war; einem Artikel, von dem mir jemand erzählt hat; dem Namen einer Person, die ich getroffen habe. Ständig schicke ich mir selbst E-Mails zur Erinnerung. Nicht nur um mich daran zu erinnern, etwas zu erledigen, wenn ich nach Hause komme, sondern auch Gedächtnisstützen für etwas, an das ich mich auch Jahre später noch erinnern möchte. Wer Zugang zu diesem Datenschatz hat, hat Zugang zu mir.

Früher habe ich meine E-Mails sorgfältig sortiert. Ich musste mich entscheiden, welche ich behalten und welche ich löschen wollte. Die verbleibenden E-Mails landeten in Hunderten von verschiedenen Ordnern, sortiert nach Personen, Firmen, Projekten et cetera. 2006 hörte ich damit auf. Nun ist alles in einem riesigen Ordner gespeichert. Seit 2006 ist es für mich einfacher zu speichern und zu suchen, als zu sortieren und zu löschen.

Um zu verstehen, was dieses Anhäufen von Daten für die Privatsphäre des Einzelnen bedeutet, sollten Sie sich den österreichischen Jurastudenten Max Scherms vor Augen führen. Scherms verlangte 2011 von Facebook die Rückgabe aller Daten, die die Firma über ihn besaß.[79] Nach EU-Recht ist diese Forderung rechtsgültig. Zwei Jahre später, nach vielen gerichtlichen Auseinandersetzungen, schickte Facebook ihm eine CD mit einem 1200 Seiten langen PDF: Es enthielt nicht nur die Freunde, die er sehen konnte, und die Einträge auf seinem Newsfeed, sondern auch alle Fotos und Seiten, die er je aufgerufen hatte, und alle Werbung, die er angesehen hatte.[80] Zwar nutzt Facebook nicht alle diese Daten, doch statt zu überlegen, welche Daten gespeichert werden sollten, ist es für das Unternehmen einfacher, schlicht alles zu speichern.

2. Daten als Überwachung

Regierungen und Unternehmen sammeln, speichern und analysieren die gewaltigen Mengen unserer Daten, die wir in unserem digitalisierten Alltag unaufhörlich produzieren. Oftmals geschieht dies ohne unser Wissen und typischerweise ohne unsere Zustimmung. Anhand dieser Daten ziehen sie Rückschlüsse auf uns, denen wir widersprechen würden oder gegen die wir uns wehren würden, und das kann weitreichende Folgen für unser Leben haben. Wir geben es vielleicht nicht gerne zu, doch wir stehen unter Massenüberwachung.

Unser Wissen über die NSA-Überwachung stammt zu einem großen Teil von Edward Snowden, obwohl vor und nach ihm auch andere Menschen Geheimnisse dieses Nachrichtendienstes veröffentlichten.[81] Als Mitarbeiter der NSA sammelte Snowden Zehntausende Dokumente, die viele der Überwachungsaktivitäten der NSA aufzeigen. 2013 floh er nach Hongkong und übermittelte die Dokumente einigen ausgewählten Journalisten.

Ich habe eine Zeit lang in Zusammenarbeit mit Glenn Greenwald und dem *Guardian* bei der Analyse einiger eher technischer Dokumente geholfen.

Die erste auf Snowdens Dokumenten basierende Nachrichtenmeldung berichtete davon, dass die NSA die Daten von Mobilfunkgesprächen aller Amerikaner sammelt.[82] Die von da an in Dauerschleife wiederholte Verteidigung der Regierung lautete, dass »nur Metadaten« gesammelt würden.[83] Gemeint ist damit, dass die NSA nicht den Wortlaut der Telefonate sammelt, sondern nur die Telefonnummern der Gesprächspartner sowie Datum, Uhrzeit und Dauer der Telefonate.[84] Dies besänftigte offenbar viele Leute, doch das ist nicht gerechtfertigt. Wenn Metadaten von Menschen gesammelt werden, heißt das, dass sie überwacht werden.[85]

Ein einfaches Gedankenspiel demonstriert dies. Stellen Sie sich vor, Sie würden einen Privatdetektiv engagieren, um jemanden zu belauschen. Der Detektiv würde die Wohnung, das Büro und das Auto der Zielperson verwanzen. Er würde das Telefon und den Computer der Person überwachen. Und Sie bekämen einen Bericht über die Gespräche der Zielperson.

Nun stellen Sie sich vor, Sie würden den Detektiv beauftragen, diese Person zu überwachen. Sie bekämen einen anderen, aber dennoch umfangreichen Bericht: wohin sie ging, was sie tat, mit wem sie sich unterhielt und wie lange, wem sie schrieb, was sie las und was sie kaufte. Das versteht man unter Metadaten.

Ein Lauschangriff verschafft einem die Gespräche; Überwachung liefert einem alles Weitere. Die Verbindungsdaten von Telefonaten verraten bereits eine Menge über uns. Zeitpunkt, Länge und Häufigkeit unserer Telefonate enthüllen einiges über unsere Beziehungen zueinander: von unseren engsten Freunden bis hin zu unseren Geschäftspartnern und allen dazwischen. Metadaten der Telekommunikation geben Aufschluss darüber, wofür und für wen wir uns interessieren und was uns wichtig ist, ganz gleich wie persönlich das ist.[86] Sie sind ein Fenster zu unserer Persönlichkeit.[87] Sie fassen im Detail zusammen, was bei uns zu jedem beliebigen Zeitpunkt gerade passiert.[88]

Ein Experiment der Universität Stanford untersuchte über mehrere Monate hinweg die Telefonmetadaten von rund 500 Freiwilligen. Es überraschte

selbst die Wissenschaftler, wie persönlich die daraus gewonnenen Erkenntnisse waren. Der Bericht ist es durchaus wert, zitiert zu werden:[89]

- Versuchsperson A sprach mit mehreren lokalen Neurologiegruppen, einer spezialisierten Apotheke, einem Managementdienst für seltene Krankheiten, einer Hotline für ein Medikament, das ausschließlich zur Behandlung von schubförmig remittierender multipler Sklerose eingesetzt wird.
- Versuchsperson B führte lange Gespräche mit Kardiologen einer großen Klinik, sprach kurz mit einem Medizinlabor, wurde von einer Apotheke angerufen und tätigte kurze Anrufe bei einer Hotline für ein medizinisches Gerät, mit dem man Herzrhythmusstörungen überwacht.
- Versuchsperson C rief mehrmals bei einem auf halb automatische Sturmgewehre spezialisierten Waffengeschäft an. Es folgten lange Gespräche mit dem Kundendienst eines Waffenherstellers, der verschiedene Sturmgewehre herstellt.
- In einem Zeitraum von drei Wochen kontaktierte Versuchsperson D einen Baumarkt, Schlossereien, einen Hydrokulturhändler und einen Headshop.
- Versuchsperson E führte früh am Morgen ein langes Gespräch mit ihrer Schwester. Zwei Tage später rief sie mehrmals beim örtlichen Familienplanungszentrum an. Zwei Wochen danach folgten weitere kurze Anrufe und ein Monat später ein letzter Anruf.

Allein anhand der Metadaten konnte man also einen Multiple-Sklerose-Patienten, ein Herzinfarktopfer, einen Besitzer von halb automatischen Feuerwaffen, jemanden, der zu Hause Marihuana anbaut, und eine Frau, die gerade abgetrieben hatte, identifizieren.

Weitere intime Informationen, die der Überwachung dienen, lassen sich aus den Daten der Internetsuche gewinnen.[90] (Man kann sich darüber streiten, ob es sich hier um Daten oder Metadaten handelt. Die NSA sagt, es seien Metadaten, da die Suchbegriffe in den URLs integriert sind.[91]) Die Suchmaschine lügen wir nicht an. Ihr gegenüber sind wir offener als unseren Freunden, Liebhabern und Familienmitgliedern gegenüber. Ihr teilen wir genau mit, woran wir gerade denken, und zwar mit möglichst eindeutigen Worten. Google weiß, nach welcher Art von Pornos jeder

von uns sucht, an welche früheren Beziehungen wir noch denken, wofür wir uns schämen, worüber wir uns Sorgen machen und welche Geheimnisse wir haben. Wenn Google wollte, könnte es herausfinden, wer von uns um seine geistige Gesundheit besorgt ist, wer über Steuerbetrug nachdenkt oder wer überlegt, gegen bestimmte Entscheidungen der Regierung zu protestieren. Früher sagte ich, dass Google meine Gedanken besser kennt als meine Frau. Doch das ist nicht weitreichend genug. Google kennt meine Gedanken besser als *ich*, denn Google erinnert sich an alle Gedanken, und zwar ohne dass sie verblassen, für immer und ewig.

Ich führte ein schnelles Experiment mit der Google-Funktion der automatischen Vervollständigung durch. Diese Funktion bietet sofort bei der Eingabe die Vervollständigung eines Suchbegriffs anhand der von anderen eingegebenen Suchbegriffe an. Für meine Eingabe von »soll ich meiner Fr« schlug Google vor »soll ich meiner Frau sagen, dass ich sie betrogen habe« und »soll ich meiner Frau verzeihen« als eine der beliebtesten Vervollständigungen an.[92] Google weiß, wer solche Vorschläge anklickt, und auch, wonach sonst der- oder diejenige jemals gesucht hat.[93] Eric Schmidt, CEO von Google, gab 2010 so viel zu: »Wir wissen, wo Sie sich befinden. Wir wissen, wo Sie waren. Wir wissen mehr oder weniger, woran Sie denken.«[94]

Wenn Sie ein Google-Konto haben, können Sie das selbst überprüfen. Sie können den Suchverlauf für jeden Zeitpunkt, zu dem Sie eingeloggt waren, abrufen. Das geht bis zur Erstellung Ihres Google-Kontos zurück, vermutlich Jahre. Versuchen Sie es – Sie werden überrascht sein. Es ist intimer, als wenn Sie Google Ihr Tagebuch geschickt hätten. Und auch wenn Google Ihnen das zeigt, haben Sie keinerlei Rechte, irgendetwas davon zu löschen, das Sie dort lieber nicht sehen würden.

Es gibt noch andere Quellen für persönliche Daten und Metadaten. Protokolle über Ihr Kaufverhalten sagen eine Menge über Sie aus. Ihre Tweets verraten der Welt, wann Sie morgens aufwachen und abends zu Bett gehen.[95] Ihre Freundschaftslisten und Adressbücher lassen Rückschlüsse auf politische Einstellung und sexuelle Orientierung zu.[96] Die Kopfzeilen Ihrer E-Mails eröffnen, wer für Sie im Berufsleben, im Freundeskreis und im Liebesleben an erster Stelle steht.[97]

Man könnte Daten als Inhalt und Metadaten als Kontext betrachten. Metadaten können erhellender als Daten sein, vor allem wenn sie geballt gesammelt werden.[98] Wenn man eine Person überwacht, können die Inhalte von Gesprächen, SMS und E-Mails bedeutender sein als die Metadaten. Doch wenn man die gesamte Bevölkerung überwacht, sind die Metadaten wesentlich aussagekräftiger, wichtiger und nützlicher.[99] Wie der ehemalige NSA-Justiziar Stewart Baker meinte: »Metadaten verraten einem absolut alles über das Leben einer Person. Mit genügend Metadaten braucht man wirklich keinen Inhalt.«[100] Im Jahr 2014 erklärte der frühere NSA- und CIA-Direktor Michael Hayden: »Anhand von Metadaten bringen wir Leute um.«[101]

In Wahrheit ist es doch so, dass der Unterschied ziemlich schwammig ist. Letztlich sind es alles Daten über uns.

Billigere Überwachung

Früher war Überwachung schwierig und kostspielig. Nur wenn es wirklich wichtig war, griff man darauf zurück: wenn die Polizei einen Verdächtigen beschatten musste oder wenn ein Unternehmen zur Rechnungsstellung den detaillierten Verlauf von Einkäufen brauchte. Es gab Ausnahmen, und die waren extrem und teuer. Die außergewöhnlich paranoide DDR-Regierung setzte 102 000 Stasimitarbeiter zur Überwachung einer Bevölkerung von 17 Millionen ein: Auf einen Spion kamen so 166 Bürger, wenn man die zivilen Informanten dazuzählt sogar nur 66.[102]

Bei der Überwachung durch Unternehmen wurden früher so wenige Daten wie nötig erhoben – mittlerweile werden so viele wie möglich gesammelt. Firmen haben schon immer Daten über ihre Kunden gesammelt, doch früher waren es nicht so viele und sie wurden nur so lange wie nötig aufbewahrt. Kreditkartenunternehmen sammelten nur die Informationen über die Transaktionen ihrer Kunden, die sie für die Abrechnung benötigten. Geschäfte sammelten so gut wie keine Informationen über ihre Kunden; Versandhäuser sammelten Namen und Adressen und führten eventuell eine Liste, was bisher alles gekauft wurde, damit sie wussten, wen sie aus der Kundenkartei streichen konnten. Selbst Google sammelte zu Beginn weit weniger Informationen über seine Benutzer als heute. Als

es noch teuer war, Überwachungsinformationen zu erheben und zu speichern, beschränkten sich die Unternehmen darauf, mit möglichst wenigen auszukommen.

In den letzten zehn Jahren sind die Preise für Computertechnologie enorm gefallen. Das ist an sich eine wirklich positive Entwicklung. Es ist nun billiger und einfacher zu kommunizieren, eigene Gedanken zu veröffentlichen, Informationen abzurufen et cetera. Doch gleichzeitig fielen auch die Preise für die Überwachung. Dank verbesserter Computertechnologie konnten Firmen Informationen über alle sammeln, mit denen sie geschäftlich Kontakt hatten. Da Speicherplatz billiger wurde, konnten sie mehr Daten über einen längeren Zeitraum speichern. Dank effektiverer Software zur Datenanalyse brachte es mehr Profit, mehr Informationen zu speichern. Daraus entstanden Geschäftsmodelle, die auf Überwachung basierten. Darauf komme ich dann in Kapitel 4 zurück.

Bei der staatlichen Überwachung wurden früher über möglichst wenige Menschen Daten gesammelt. Als Überwachung noch Handarbeit und teuer war, ließ sie sich nur in extremen Fällen rechtfertigen. Die Reglementierung von Durchsuchungsbefehlen limitierte die polizeiliche Überwachung, und knappe Mittel sowie das Risiko, entdeckt zu werden, limitierten die geheimdienstliche Überwachung. Nur ganz bestimmte Zielpersonen wurden überwacht, über sie – und nur über sie – wurden möglichst viele Informationen gesammelt. Es gab auch strenge Regeln, die untersagten, Informationen über andere Personen zu sammeln. Wenn das FBI beispielsweise das Telefon eines Verbrechers abhörte, musste der Spitzel auflegen und die Aufnahme abrechen, wenn dessen Frau oder Kinder am Telefon waren.

Als die Technologie immer ausgefeilter und zugleich immer billiger wurde, weiteten die Regierungen ihre Überwachung aus. Die NSA konnte nun große Gruppen überwachen – die Sowjetregierung, chinesische Diplomaten, linke politische Organisationen und Aktivisten – statt wie früher nur Einzelpersonen. Dank mobiler Telekommunikationsüberwachung konnte das FBI Personen abhören, egal welches Gerät sie zur Kommunikation benutzten.[103] Schließlich konnten US-Geheimdienste ganze Bevölkerungen ausspionieren und die Daten jahrelang speichern. Dies ging einher mit einer sich verändernden Bedrohung und die Nachrichtendienste setzten ihre Spionagearbeit gegen bestimmte Staaten fort. Zugleich weiteten sie die