Einleitung

Zeit zu verschwinden

Ziemlich genau zwei Jahre nach dem Tag, an dem ein gewisser Edward Joseph Snowden, ein Auftragnehmer der IT-Beratungsfirma Booz Allen Hamilton, Geheimdokumente der NSA[1] veröffentlicht hatte, führte der US-Comedian John Oliver für seine Show eine Umfrage auf dem Times Square in New York durch. Er stellte zufällig ausgewählten Passanten jeweils zwei einfache Fragen: Wer ist Edward Snowden? Und was hat er getan?[2]

In den Interviewausschnitten, die in Olivers Show zu sehen waren, schien das keiner zu wissen. Manche hatten den Namen zwar schon einmal gehört, konnten aber nicht so genau sagen, was Snowden eigentlich getan hatte und warum. Sie wussten nicht, dass Edward Snowden als externer Mitarbeiter der NSA Tausende als »top secret« eingestufte Daten und Geheimdokumente an verschiedene Journalisten übergeben hatte, damit diese sie der Weltöffentlichkeit zugänglich machen konnten. Oliver hätte daraufhin die Folge seiner Show zum Thema Überwachung einfach mit der deprimierenden Erkenntnis beenden können, dass es den Amerikanern offenbar auch nach Jahren ausführlicher medialer Berichterstattung egal war, dass die Regierung sie in ihrer Privatsphäre bespitzelte. Doch das tat er nicht. Stattdessen flog er nach Russland, wo Snowden im Exil lebt, um ein Interview mit ihm zu führen.[3]

Olivers erste Frage an Snowden war: »Was wollten Sie mit diesen Enthüllungen erreichen?« Snowden antwortete, dass er der Welt zeigen wollte, was die NSA tut – nämlich über nahezu jeden Menschen Daten zu sammeln. Oliver zeigte Snowden die Interviews vom Times Square, in denen ein Passant nach dem anderen zugab, Snowden nicht zu kennen. Daraufhin sagte Snowden: »Na ja, es kann eben nicht jeder gut informiert sein.«

Aber warum sind wir nicht besser informiert über die Fragen des Datenschutzes, die Edward Snowden und andere Whistleblower aufgeworfen haben? Warum scheint es uns noch nicht einmal etwas auszumachen, dass

eine Regierungsbehörde unsere Telefonate abhört und unsere E-Mails und SMS-Nachrichten überwacht? Vielleicht, weil die NSA unser Leben nicht direkt beeinträchtigt, zumindest haben wir nicht das Gefühl, dass sie es tut, denn wir *spüren* ihre Eingriffe nicht unmittelbar.

Doch Oliver fand in seinen Interviews am Times Square auch heraus, dass die amerikanische Bevölkerung sehr wohl um ihre Privatsphäre besorgt ist, wenn es um intime Dinge geht. Er konfrontierte die Befragten mit einem geheimen (und erfundenen) Regierungsprogramm, bei dem Nacktaufnahmen gespeichert werden, sobald sie über das Internet versendet werden. Die New Yorker waren wieder weitgehend einer Meinung, nur dieses Mal waren alle absolut dagegen. Ein Passant gab sogar zu, kürzlich ein Nacktfoto versendet zu haben.

Jeder der Befragten stimmte der Ansicht zu, dass es den Menschen in den USA möglich sein sollte, einfach alles über das Internet vertraulich zu teilen – selbst ein Foto von einem Penis. Und genau das war Snowdens Kernaussage.

Tatsächlich ist ein Regierungsprogramm wie das erfundene, das Nacktaufnahmen speichert, gar nicht so weit hergeholt, wie man denken könnte. Wie Snowden im Interview mit Oliver erklärte, sind die Server von Firmen wie Google über die ganze Welt verteilt. Deshalb könnte auch eine einfache Nachricht (vielleicht mit einem Nacktfoto), die eine Frau ihrem Mann innerhalb einer Stadt in den USA sendet, über einen Server im Ausland gehen. Da die Daten also die USA verlassen, wenn auch nur für den Bruchteil einer Sekunde, wäre es der NSA aufgrund des Patriot Acts[4] erlaubt, sie zu erfassen und zu archivieren. Sie dürfte die Nachricht inklusive des anstößigen Fotos also speichern, weil sie rein technisch gesehen in dem Moment, in dem sie abgefangen wurde, vom Ausland in die USA kam. Was Snowden damit sagen möchte: Jeder durchschnittliche US-Bürger ist von der Großfahndung betroffen, die nach den Anschlägen des 11. September gestartet wurde – eine Fahndung, die eigentlich dazu gedacht war, ausländische Terroristen zu fassen, die jetzt aber so gut wie jeden Bürger überwacht.

Wenn man sich die vielen Nachrichten über Datenpannen und die Überwachungskampagnen der Behörden ansieht, sollte man doch meinen, dass sich viel mehr Menschen darüber aufregen würden. Man sollte meinen, dass wir angesichts der Tatsache, dass sich diese Vorfälle in so schneller Folge – innerhalb nur weniger Jahre – ereignen, erschüttert und schockiert sein und auf die Barrikaden gehen müssten. Doch genau das Gegenteil ist der

Fall. Viele Menschen, und sicher auch viele Leser dieses Buches, haben sich damit abgefunden, dass alles, was sie tun, ihre Telefonate, Nachrichten, E-Mails und Social-Media-Posts, von anderen mitgehört bzw. mitgelesen werden.

Und das ist wirklich enttäuschend.

Vielleicht haben Sie noch nie gegen das Gesetz verstoßen. Sie leben ein ganz normales, durchschnittliches, ruhiges Leben und haben das Gefühl, sich völlig unbeobachtet inmitten vieler anderer im Internet zu bewegen. Glauben Sie mir: Auch Sie sind nicht unsichtbar.

Zumindest noch nicht.

Ich liebe Zaubertricks, und man könnte auch sagen, dass ich fürs Hacken von Computern einige Taschenspielertricks beherrschen muss. Einer der berühmtesten Zaubertricks ist das Verschwindenlassen eines Gegenstands. Das Geheimnis dieses Tricks besteht darin, dass der Gegenstand nicht wirklich verschwindet oder unsichtbar wird. Stattdessen bleibt er einfach immer im Hintergrund – mal hinter einem Vorhang, mal im Jackenärmel oder in der Tasche –, egal, ob wir ihn dort sehen können oder nicht.

Und genauso ist es mit den Unmengen an persönlichen Daten von praktisch jedem Einzelnen von uns, die ohne unser Wissen gesammelt und gespeichert werden. Die meisten von uns wissen gar nicht, wie einfach es für andere ist, sich diese privaten Dinge anzusehen, oder wie man an sie herankommt. Und nur weil wir selbst diese Informationen nicht sehen, denken wir, wir wären unsichtbar für unsere Ex-Partner, unsere Eltern, die Schulen, unsere Chefs und sogar für die Regierung.

Doch tatsächlich sind diese Daten für jeden zugänglich, der weiß, wo er suchen muss.

Immer wenn ich vor einer Gruppe spreche, ganz egal, wie groß der Raum ist, gibt es darunter jemanden, der eben diese Tatsache anzweifelt. Nach einem Vortrag in einer größeren Stadt in den USA sprach mich beispielsweise eine skeptische Journalistin an. Ich saß an einem Tisch in der Hotelbar, als sie zu mir kam und mir erklärte, sie sei noch nie Opfer einer Datenpanne gewesen. Da sie noch jung sei, habe sie noch nicht viel veröffentlicht und dementsprechend gäbe es kaum Einträge zu ihrem Namen. Sie ließe niemals etwas Persönliches in ihre Beiträge einfließen und sei auch in den sozialen Medien zurückhaltend – alles auf professioneller Ebene. Sie glaubte, sie sei unsichtbar. Also fragte ich sie, ob ich ihre Sozial-

versicherungsnummer und andere persönliche Informationen über sie online suchen dürfe. Etwas zögerlich stimmte sie zu.

Und so saß sie neben mir, als ich mich auf einer speziellen Seite für private Ermittler einloggte. Ich gelte als ein solcher, weil ich weltweit Hackerangriffe untersuche. Ihren Namen kannte ich schon, nun fragte ich sie noch, wo sie wohnt. Das hätte ich aber auch über eine andere Internetseite herausfinden können, wenn sie es mir nicht gesagt hätte.

Innerhalb weniger Minuten hatte ich ihre Sozialversicherungsnummer, ihren Geburtsort und den Mädchennamen ihrer Mutter ermittelt. Ich kannte außerdem alle Orte, an denen sie jemals gelebt hatte, und alle Telefonnummern, die sie je benutzt hatte. Überrascht starrte sie den Bildschirm an und bestätigte, dass all diese Informationen weitestgehend korrekt waren.

Die Nutzung dieser Website ist nur Firmen und Einzelpersonen gestattet, die zuvor überprüft wurden. Für den Zugang wird monatlich eine geringe Gebühr berechnet, pro Anfrage fallen zusätzliche Kosten an und gelegentlich wird kontrolliert, ob ein Nutzer einen legitimen Grund für eine bestimmte Suchanfrage hat.

Auf diese Art lassen sich vergleichbare Informationen über jede beliebige Person beschaffen. Es kostet nur eine kleine Gebühr, und es ist völlig legal.

Haben Sie je ein Online-Formular ausgefüllt oder Informationen an eine Hochschule oder Organisation übermittelt, die etwas online stellt? Oder haben Sie schon mal Fragen zu einem Rechtsfall im Netz gepostet? Falls ja, dann haben Sie diese Informationen aus freien Stücken Dritten zugänglich gemacht, die damit machen können, was sie wollen. Es ist gut möglich, dass einige dieser Daten – wenn nicht sogar alle – jetzt online sind und Unternehmen zur Verfügung stehen, deren Geschäftsmodell darin besteht, jede noch so kleine persönliche Information im Internet einzusammeln. Das Privacy Rights Clearinghouse[5] verzeichnet über 130 Firmen, die solche Daten (ob sie nun stimmen oder nicht) über die Bürger zusammentragen.[6]

Dann gibt es natürlich auch noch die Informationen, die Sie gar nicht freiwillig online veröffentlichen und die dennoch von Unternehmen und Regierungsbehörden regelrecht geerntet werden: an wen Sie E-Mails oder Nachrichten schicken, wen Sie anrufen, wonach Sie im Internet suchen, was Sie kaufen (sowohl online als auch in konventionellen Läden) und wohin Sie unterwegs sind, egal ob zu Fuß oder mit dem Auto. Die Menge an Daten, die über jeden Einzelnen von uns gesammelt wird, wächst jeden Tag exponentiell an.

Dennoch denken Sie jetzt vielleicht, dass Sie sich deswegen keine Sorgen machen müssen. Doch glauben Sie mir: Das müssen Sie. Nach der Lektüre dieses Buches wissen Sie hoffentlich, warum und was Sie dagegen tun können.

Wir leben in dem falschen Glauben, wir hätten so etwas wie Privatsphäre, und das wahrscheinlich schon seit Jahrzehnten.

Es bereitet uns zwar ein gewisses Unbehagen, wie viele Einblicke unsere Regierung, unser Arbeitgeber, unser Chef, unsere Lehrer und unsere Eltern in unser Privatleben haben. Doch da sich diese Situation nach und nach entwickelt hat und wir jede neue digitale Annehmlichkeit bereitwillig angenommen haben, ohne uns gegen die damit verbundenen Eingriffe in unsere Privatsphäre zu wehren, wird es immer schwerer, die Uhr zurückzudrehen. Wer möchte denn schon seine lieb gewonnenen Spielzeuge aufgeben?

Das Leben in einem digitalen Überwachungsstaat ist nicht deshalb gefährlich, weil die Daten gesammelt werden (das können wir sowieso kaum verhindern), entscheidend ist vielmehr die Frage, was mit diesen Daten gemacht wird.

Stellen Sie sich doch nur mal vor, was ein übereifriger Staatsanwalt mit einem umfassenden Dossier über Sie alles anfangen könnte, das aus Rohdaten besteht, die einige Jahre zurückreichen. Daten, die vielleicht in völlig anderen Zusammenhängen gesammelt wurden, existieren heute für immer. Selbst Stephen Breyer, Richter am Obersten Gerichtshof der Vereinigten Staaten, räumte ein, dass es schwer vorherzusehen sei, ob eine Reihe bestimmter Äußerungen einem Staatsanwalt später einmal im Rahmen einer Ermittlung relevant erscheinen könnte.[7] Mit anderen Worten: Ein Foto, das Sie betrunken zeigt und das jemand auf Facebook postet, ist vielleicht noch Ihr kleinstes Problem.

Sie denken, Sie haben nichts zu verbergen, sind sich aber nicht ganz sicher? In einem sehr überzeugenden Gastbeitrag im Magazin *Wired* argumentierte der angesehene IT-Sicherheitsexperte Moxie Marlinspike, dass selbst etwas so Banales wie der Besitz eines kleinen Hummers in den USA einen Verstoß gegen ein Bundesgesetz darstellt.[8] »Es spielt dabei keine Rolle, ob man ihn in einem Lebensmittelgeschäft gekauft oder von einer anderen Person bekommen hat, ob er tot ist oder lebendig, ob man ihn gefunden hat, nachdem er eines natürlichen Todes gestorben ist, oder ob man ihn in Notwehr getötet hat.«[9] Marlinspike will darauf hinaus, dass es jede Menge kleiner, gemeinhin vernachlässigter Gesetze gibt, die man möglicherweise bricht, weil man sie gar nicht kennt. Doch heute ist die zugehö-

rige Beweiskette aus Daten jederzeit nur ein paar Klicks entfernt und jedem zugänglich, der Interesse daran hat.

Datenschutz ist ein komplexes Thema. Hier gibt es keine Universallösungen. Wir alle haben unterschiedliche Gründe dafür, bestimmte persönliche Informationen offen mit Fremden zu teilen, während wir andere Bereiche unseres Lebens geheim halten. Möglicherweise möchten wir einfach nicht, dass unsere bessere Hälfte gewisse persönliche Dinge liest, oder wir wollen unserem Arbeitgeber keine Einblicke in unser Privatleben geben, oder vielleicht haben wir auch wirklich Angst davor, dass Geheimdienste uns ausspionieren.

Das sind sehr unterschiedliche Szenarien, und so kann es nicht die eine Empfehlung geben, die in allen Fällen die richtige ist. Weil unsere Einstellungen zum Thema Privatsphäre also komplex und damit auch individuell unterschiedlich sind, zeige ich Ihnen einfach all das, was wichtig ist – das heißt, was heute mit den heimlich gesammelten Daten geschieht –, und überlasse es dann Ihnen, zu entscheiden, wie Sie persönlich am besten damit umgehen.

In erster Linie soll dieses Buch Ihnen Wege aufzeigen, sich in der digitalen Welt unbeobachtet zu bewegen. Es wird Ihnen Lösungen anbieten, die Sie übernehmen können oder auch nicht. Privatsphäre ist eine persönliche Entscheidung, also wird auch der Grad der Anonymität, den Sie erreichen möchten, individuell verschieden sein.

In diesem Buch stelle ich die These auf, dass jeder Einzelne von uns beobachtet wird, sei es zu Hause oder draußen – egal, ob wir die Straße entlanggehen, in einem Café sitzen oder auf der Autobahn fahren. Ihr Computer, Ihr Telefon, Ihr Auto, Ihre Alarmanlage, ja, sogar Ihr Kühlschrank sind potenzielle Zugangspunkte zu Ihrem Privatleben.

Die gute Nachricht ist, dass ich Ihnen nicht nur Angst machen will, sondern Ihnen auch zeigen möchte, was Sie gegen diesen Mangel an echter Privatsphäre unternehmen können – ein Zustand, der zur Norm geworden ist.

In diesem Buch werden Sie lernen, wie Sie

- E-Mails verschlüsseln und sicher verschicken,
- durch ein gutes Passwort-Management Ihre Daten schützen,
- Ihre echte IP-Adresse vor den Websites, die Sie besuchen, verbergen,
- verhindern, dass Ihr Computer getrackt werden kann,
- anonym bleiben
- und vieles mehr.

Machen Sie sich bereit, die Kunst der Anonymität zu erlernen!