"Kaum dreht man sich um, wollen sie schon wieder Geld"

Autor(en): **Bader, Stephan / Binney, William**

Objekttyp: **Article**

Zeitschrift: **Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur**

Band (Jahr): **96 (2016)**

Heft 1042

PDF erstellt am: **27.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-736418

«Kaum dreht man sich um, wollen sie schon wieder Geld»

Sicherheit und Privatsphäre gehen sehr wohl zusammen, meint der ehemalige Technikchef des US-Nachrichtendienstes NSA. An seinem Ex-Arbeitgeber lässt er kein gutes Haar.

Stephan Bader trifft William Binney

Herr Binney, die wichtigste Frage zuerst: Ist Datensammeln ein notwendiges Übel, wenn man einen funktionierenden Nachrichtendienst als Frühwarnsystem haben will?
Informationen zu sammeln, ist noch keine Aufklärung. Das Ergebnis der Sammlung sind nur Daten. Erst wenn man versteht, was die Daten bedeuten, werden daraus «Nachrichten», wie sie für einen Nachrichtendienst sinnvoll verwertbar sind. Dann lassen die Daten Muster menschlichen Verhaltens erkennen, und indem diese Muster für automatisierte Vorverfahren genutzt werden, können aus Daten teilweise automatisierte Voraussagen über menschliches Verhalten getroffen werden.

Mit der Digitalisierung wurde die Herausforderung für Analysten, die zur Verfügung stehenden Daten zu bewältigen, grösser.
Exponentiell grösser. In Grossbritannien sammelt der Geheimdienst 60 Milliarden Datensätze pro Tag! Wer soll das durchgehen?

Wie haben Sie versucht, dieses Problem zu lösen?
Schon in den 1990er Jahren, als die Möglichkeiten, Daten zu sammeln, deutlich geringer waren, ertranken die Analysten förmlich in Daten. Wie also konnte man Content in diesen Grössenordnungen in den Griff bekommen? Die Lösung war und ist, sich auf Metadaten zu beschränken.

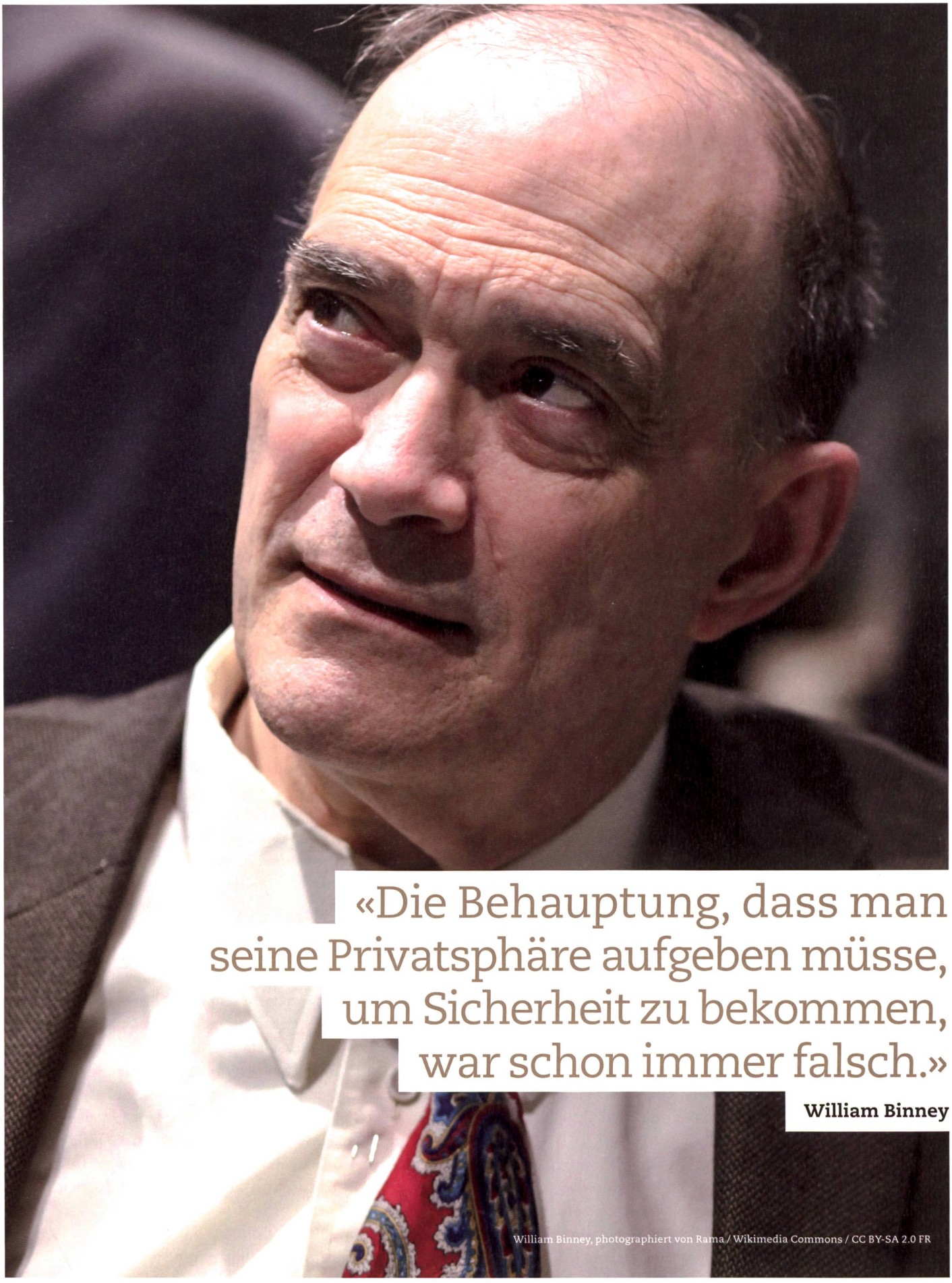
Sich also nicht auf den Inhalt eines Telefonanrufs, sondern auf die Informationen über Zeitpunkt, Dauer, Teilnehmer und Standorte zu konzentrieren.
Genau. Das ist viel, viel effizienter, als wenn man die ganzen Inhalte durchforsten müsste. Metadaten sind recht einfach zusammenzustellen, und sie erlauben es, Aufschlüsse über Beziehungen und Communities herauszuschälen. Wenn man weiss, wer mit wem Verbindungen hat, kann man relativ einfach soziale Netzwerke von Terroristen oder Drogenhändlern erkennen.

Und dann gezielt die Inhalte analysieren.
Ja, so sind die Analysten in der Lage, ein Gebiet von Informationen genauer zu betrachten. Sie sind nun nicht mehr abgelenkt durch Leute, die mit ihrer Grossmutter telefonieren und dabei Wörter benutzen, die irgendwie als verdächtig angesehen werden. Die sogenannte «Keyword Selection» oder «Dictionary Selection» ist nämlich immer noch ein Standard, wenn es darum geht, «Verdächtiges» zu erkennen. Man kann damit viel Zeit verschwenden, schliesslich erhält man nichts anderes, als wenn man Begriffe in eine Suchmaschine eintippt. Die ersten 10 von 100 000 Suchergebnisseiten zu durchforsten, schafft man vielleicht noch, aber das war's dann. Wie hoch ist die Wahrscheinlichkeit, dass man etwas Wichtiges verpasst? Ziemlich hoch. Und genau so ist es nun schon mehrfach geschehen. Deshalb konnte niemand diese ganzen Anschläge stoppen.

Aber die Informationen sind doch da, und die Analysten auch.
Wie viele Anschläge gab es denn mittlerweile? In Europa Paris, Brüssel, Madrid und London, in den USA Orlando und Boston. Trotz enormen Mengen an gesammeltem Datenmaterial scheitern die Geheimdienste kontinuierlich dabei, Anschläge zu unterbinden. Nehmen wir den Attentäter in Orlando am 12. Juni 2016, der 49 Menschen tötete und 53 verletzte. Dieser Mann hatte bereits verlauten lassen – und das FBI hatte ihn zwei Jahre zuvor beobachtet –, dass er beabsichtige, Menschen etwas anzutun. Unser Programm hätte «Absichten» erkannt: der Typ wird zur Zielperson und sollte beobachtet werden. Als er dann ein Gewehr kaufte, hätten «Absichten» und «Potenzial» zusammen eine «Warnung» ergeben. Dieser Mann hätte sofort ganz nach oben auf die Überwachungsliste gesetzt werden müssen. Aber das hat niemand getan.

William «Bill» Binney
arbeitete über 30 Jahre für den US-Nachrichtendienst NSA, zuletzt als Technikchef. Er entwickelte das Programm ThinThread, das Kommunikationsüberwachung und Grundrechte vereinte. Anstelle von ThinThread wurde aber das kostspieligere, datengierigere Programm Trailblazer realisiert. Angesichts des Datensammelwahns nach 9/11 wurde Bill Binney zum Whistleblower, heute ist er Beirat der Courage Foundation und unterstützt Menschen, die Geheimdienstübergriffe vor Gericht bringen. Und: «Ohne Bill Binney gäbe es keinen Edward Snowden», das sagt der aktuell bekannteste NSA-Whistleblower über den vielleicht wichtigsten.

Stephan Bader
ist freier Journalist und lebt in Berlin.



«Die Behauptung, dass man seine Privatsphäre aufgeben müsse, um Sicherheit zu bekommen, war schon immer falsch.»

William Binney

William Binney, photographiert von Rama / Wikimedia Commons / CC BY-SA 2.0 FR

Weil das jetzige System ineffizient ist?
Oder weil es nicht dafür entwickelt ist. Es ist dafür gemacht, zu scheitern. So dass weiter Menschen sterben. So dass Geheimdienste die Tatsache, dass Menschen sterben, weiter dafür benutzen können, noch mehr Mittel zu erhalten. Um dieses riesige Programm weiter zu unterhalten, möglichst viele Daten zu sammeln und Macht über andere zu erlangen. Für uns mag das eine schwer nachvollziehbare Logik sein, wenn man in einer Machtposition ist, ergibt sie in gewisser Weise schon Sinn. Und wenn man darüber nachdenkt, ist das doch genau, was passiert ist: Kaum dreht man sich um, wollen sie schon wieder mehr Geld. Immer nachdem Leute sterben mussten.

Die Geheimdienste werden also immer mächtiger, aber nicht effizienter?
Jedes Mal, wenn ein Anschlag passiert, benutzen das die Geheimdienste als Hebel, um mehr Mittel zu verlangen, mehr Leute. Und zu behaupten, sie bräuchten mehr Daten. Doch so verschlimmern sie das Problem nur.

Einverstanden. Aber wie ginge es denn besser?
Nur wer gezielt ansetzt und von Beginn an eine intelligente Auswahl trifft, erhält eine Datenmenge, die auch zu bewältigen ist. Mit einer Kombination aus deduktiven, induktiven und abduktiven Methoden ergeben sich dabei zudem mehr eindeutige Identifizierungskennzeichen für Zielpersonen, und man erkennt schneller und sicherer, wenn sich neue Leute Terroristen- oder Drogenschmuggelnetzwerken anschliessen. Durch den Metadaten-basierten Ansatz ergeben sich Verdachtsmomente, die auf dem Verhalten beruhen. Wenn jemand im Internet zum Beispiel wiederholt Dschihad-Anwerbungsseiten besucht oder mit Terroristen kommuniziert, dann könnte das bedeuten, dass sich diese Person radikalisiert und überwacht werden sollte. Weil ihr Verhalten nahelegt, dass sie möglicherweise etwas Böses plant, jedenfalls mit einer Wahrscheinlichkeit, die es sinnvoll macht, sie sich näher anzusehen, und die auch gegenüber einem Gericht zu rechtfertigen ist. So wollten wir vorgehen: die Datenselektion sollte komplett auf Verhaltenseigenschaften beruhen, die eine Absicht zeigten, kriminelle Taten zu begehen. In unser Programm ThinThread bauten wir diese Auswahl ganz vorne in die Echtzeitdatenauswahl mit ein.

Sie haben ThinThread an drei NSA-Standorten unter echten Bedingungen getestet. Die Resultate waren sehr erfolgreich.
Ja, und das ist auch in einem Bericht des Department of Defense Office of Inspector General festgehalten, der aber nicht öffentlich einsehbar ist.

Es gab also mit ThinThread eine Lösung, die demokratische Erfordernisse, Menschenrechte und die Gesetze achtete, aber auch Leute erkannte, die der Gesellschaft möglicherweise schaden wollten. Was könnte ein Grund sein, diese Möglichkeiten nicht zu nutzen?
Salopp gesagt: Sie würden damit ja ein Problem lösen. Und so dem Motto «Keep the problem going to keep the money flowing» entgegenlaufen. Wenn du ein Problem löst, kannst du die ständig steigenden Gelder nicht mehr rechtfertigen. Wir sprechen hier von Dutzenden von Milliarden Dollar, die letztlich der Grund sind, warum Interessen bestehen, das Ganze am Laufen zu halten.

Das wäre schockierend. Klar, Menschen wollen Geschäfte machen, auch mal schmutzige. Aber hier geht es um Menschen, die deswegen sterben müssen.
Ich sehe keine andere Erklärung: Die Priorität dieser Leute sind nicht die Menschenrechte oder ihre Mitbürger zu schützen. Kommt noch dazu, dass die ganze Datensammlerei ihnen Macht über andere gibt. Und diesen Menschen gefällt es, Macht zu besitzen. Ich habe das mal «J. Edgar Hoover auf Supersteroiden» genannt. J. Edgar Hoover stand dem FBI über 40 Jahre lang vor – warum? Weil er brisante Informationen über alle wichtigen Persönlichkeiten des Landes hatte. Im Kongress, im Weissen Haus, überall liessen sie ihn in Ruhe. Über einige hatte er vielleicht gar keine Informationen. Aber sie glaubten, er habe sie.

Und heute?
Heute haben die US-Geheimdienste Daten über alle Menschen auf dem Planeten, also grosse, reale Macht. Arabische Prinzen zum Beispiel kann man hervorragend damit unter Druck setzen, dass sie Pornoseiten besucht haben, weil das in ihren Ländern verpönt ist. Und schon hat man einen Hebel. So einen Hebel hat die NSA praktisch über jedes Parlamentsmitglied der Welt.

Ist eine parlamentarische Kontrolle von Nachrichtendiensten denn überhaupt möglich?
Sie versagte jedenfalls bisher auf der ganzen Linie. Nicht ein einziges Land hat eine funktionierende Aufsicht über seine Nachrichtendienste. Man bemüht sich stattdessen, eine Fassade von Kontrollmechanismen und Legitimierung aufrechtzuerhalten.

Noch einmal: wie könnte es besser gemacht werden?
Im Januar 2014, als Barack Obama Veränderungen bei der NSA ankündigte, kamen alle NSA-Whistleblower und weitere Fachleute zusammen, um Reformideen zu sammeln. Unser erster Vorschlag war, Daten nur zielgerichtet zu sammeln. Denn Daten, die nicht gespeichert werden, können nicht missbraucht werden. Alleine das würde viel missbräuchliche Überwachung verhindern, gegenüber der Tea-Party-Bewegung, den Occupy-Gruppen und vielen Journalisten zum Beispiel. Und generell gegenüber unbescholtenen Bürgern, die nicht Teil eines Netzes von Terroristen, Drogenschmugglern oder sonstigen Zielgruppen sind. Ist das nicht der Fall, bist du nicht in der Verdachtszone und niemand sieht deine Daten.

Und der zweite Vorschlag?
Wir wollten, dass den Kontrollinstanzen eine Gruppe technisch

hochqualifizierter Personen zur Seite gestellt wird: Computerexperten also, Hacker, die wirklich effizient und kompetent sind in diesen Fragen. Diese Gruppe wäre nicht nur gegenüber dem Parlament und den Gerichten verantwortlich, sondern auch gegenüber der Regierung und der Verwaltung. Sie wäre berechtigt, in jeder nachrichtendienstlichen oder geheimdienstlichen Behörde alle gewünschten Daten von allen Personen, Computern und Datenbanken einzusehen, um kontrollieren zu können, was da gemacht wurde. Ob das, wovon der Nachrichtendienst sagt, dass er es tut, auch das ist, was er tatsächlich tut.

Eine schöne Idee, in der Theorie. Kann das in der Praxis funktionieren?
Im Parlament müsste diese Gruppe jedem Repräsentanten auskunftspflichtig sein, nicht nur einer spezialisierten Kommission. Solche Kommissionen wurden ja ursprünglich gegründet, um sicherzustellen, dass die Nachrichtendienste keine Inlandsspionage ohne richterlichen Beschluss betrieben. Denn das ist die Grundlage: um im Inland zu überwachen, brauchst du einen Richterbeschluss. Das Problem ist, dass die parlamentarischen Kommissionen mit der Zeit selbst zu Anwälten der Inlandsspionage wurden und auch das Parlament über die Vorgänge in den Nachrichtendiensten anlogen. Das verstösst gegen ihren eigentlichen Auftrag, gegen Gesetze und gegen mehrere Zusatzartikel der Verfassung.

Was sind die Voraussetzungen, um eine richterliche Erlaubnis zu bekommen, jemanden im Inland ausspionieren zu dürfen?
Es muss eine «Probable Cause», also eine wahrscheinliche Ursache, für eine zukünftige Tat geltend gemacht werden. Wenn etwa die Al-Kaida-Basis im Jemen jemanden in den USA angerufen hat, durften wir beide Seiten dieser Unterhaltung zunächst erfassen. Dann hatten wir 72 Stunden lang Zeit, einen Richterbeschluss zu erhalten, um die Überwachung fortzusetzen. Erhielten wir ihn nicht, mussten wir die Überwachung fallenlassen und die Daten löschen. Die Al-Kaida-Basis war ja nun eine terroristische Einrichtung und als solche ziemlich bekannt. In diesem Fall genügte den Richtern die Kommunikation mit dieser Einrichtung als Rechtfertigung, auch zu überwachen, was jemand am anderen Ende der Leitung in den USA in einem solchen Gespräch sagte. Oder wenn plötzlich jemand auftaucht, der in den Bergen von Afghanistan ein Satellitentelefon benutzt. In den 72 Stunden zeigte sich dann in der Regel, ob aus den Verdachtsmomenten konkrete Hinweise wurden oder ob man die Beobachtung wieder fallenliess. Jedenfalls hatte man eine begrenzte Zeit, zunächst zu beobachten, dann einen Richterbeschluss zu beantragen oder eben die Person als Ziel fallenzulassen. Das war fair, vernünftig und fokussiert.

Dennoch scheint in vielen Staaten, jüngst gerade auch in Europa, eine Mehrheit der Parlamentarier weiterhin der Meinung zu sein, dass der Geheimdienst nur dann seine Aufgaben wahrnehmen kann, wenn er alle Freiheiten hat und dabei nicht kontrolliert wird.
Die Behauptung, dass man seine Privatsphäre aufgeben müsse, um Sicherheit zu bekommen, war schon immer falsch. Das wissen auch die Verantwortlichen in den Nachrichtendiensten. Aber sie brauchen und nutzen diese Lüge, um die Menschen glauben zu lassen, dass für ihre Sicherheit möglichst viele Daten gesammelt werden müssten. Nur so konnten sie die Erlaubnis für die Massenüberwachung bekommen und riesige Summen an öffentlichen Geldern dafür zugesprochen erhalten. Allein die USA haben seit dem 11. September 2001 mehr als eine Billiarde US-Dollar für nachrichtendienstliche Tätigkeiten ausgegeben, also jedes Jahr um die 100 Milliarden! Dahinter stecken Interessen von einflussreichen Konzernen, die damals nicht umsonst beim Kongress für die Einstellung unseres deutlich schlankeren ThinThread-Programms innerhalb der NSA lobbyiert haben. Sie sahen es als Konkurrenz. Es hätte ein Problem gelöst und damit ihre lukrativen Verträge und den weiteren Geldfluss gefährdet. Für mich ist klar: diese Seilschaften haben die Leben und die Sicherheit der US-Amerikaner und aller Menschen in der freien Welt gegen Geld eingetauscht.

Können sich also Bürger überhaupt vor dem Zugriff der Geheimdienste schützen?
Kaum. Man befindet sich nun mal mit seinem Computer, Telefon oder Handy dort, wo man sich befindet. Über IP-Pakete kann letztlich bei jeder Übertragung nachverfolgt werden, von wo Daten kommen und wohin sie gehen. Diese Information ist in jedem Paket enthalten. Sonst würden sie nicht ankommen. Das bedeutet aber auch, dass Sender und Empfänger nachverfolgt werden können.

Und was ist mit Verschlüsselungstechniken wie dem TOR-Browser oder dem Messenger «Signal»?
Verschlüsselungen machen vielleicht ein paar Schritte mehr nötig, aber ändern daran nichts Grundsätzliches. Auch diese sogenannten Key Exchanges werden geloggt und protokolliert und sind zumindest für Fortgeschrittene nachvollziehbar. Der einzige Weg ist es, elektronischen Datenaustausch ganz zu vermeiden, Hardware abzuschirmen und untereinander per physische Post zu verschicken. Oder zumindest die Verschlüsselung offline in einer Art Faradaykäfig vorzunehmen, dann online zu gehen, die verschlüsselten Daten zu verschicken, und die andere Person macht das Umgekehrte.

Der übermächtige Geheimdienst und der weitgehend machtlose Bürger – wird das ewig so weitergehen?
Die Geheimdienste tun das Falsche aus den falschen Gründen. Offenbar sind sich die Menschen dessen immer noch zu wenig bewusst, und die Regierungen tun auch viel dafür, solche Informationen vor der Bevölkerung zurückzuhalten. Aber solange die Massenüberwachung weiter wie bisher betrieben wird, werden die Nachrichtendienste an ihrer Aufklärungsaufgabe scheitern, und weitere Menschen werden sterben. Bis die Bevölkerung anfängt, wirklich zu revoltieren – gegen diese falsche Prämisse. ‹