

# Edward Snowden Interview – Die überarbeitete Abschrift

Quelle: <http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript>

Der Whistleblower spricht mit Alan Rusbridger und Ewen MacAskill über sein Leben in Russland, die NSA Kultur, seine Zeit bei der NSA und die Zukunft der Kommunikation

## ***EDWARD SNOWDEN ÜBER ...***

### **... seine Zeit in Hongkong**

Der ganze Zeitraum war sorgfältig geplant und orchestriert. Die Aktion war nicht gefährdet. Ich hätte am Arsch sein können, aber dass die Übergabe an Journalisten unterbunden worden wäre, das war absolut nicht möglich, außer der Journalist hätte das absichtlich an die Regierung weitergegeben.

Und ich habe meine Spuren nicht verdeckt. Ich habe nur versucht, im Vorfeld meiner Reise nicht erkannt zu werden, ich wollte nicht, dass man mir etwas untersagt. Auf der anderen Seite wollte ich schon, dass sie wissen, wo ich war. Ich wollte, dass sie es wissen. Aber deswegen hieß es dann gleich: „OK, der Junge ist nicht da, wo er sagt, dass er sein sollte. Er sollte medizinisch behandelt werden. Warum zum Teufel ist er in Hongkong?“ Und ich wollte nicht, dass sie der Sache vorgreifen und im wesentlichen versuchen, eine Spionage-Geschichte daraus zu machen. [Snowden wollte, dass die Enthüllungen schnellstmöglich veröffentlicht würden.] Deswegen war ich wegen all dieser Verzögerungen besorgt. Sie müssen wissen, ich kannte nichts von Pressearbeit, ich hatte noch nie mit einem Journalisten geredet ... Ich war im Grunde jungfräulich in der Hinsicht.

Es war eine nervenaufreibende Zeit. Man hat keine Vorstellung, was die Zukunft bringen wird, und mir ging es gut, weil ich wusste, dass die Dinge rauskommen würden, aber ich wollte, dass sie bestmöglich rauskommen sollten, und deshalb wollte ich keine Fehler machen. Ich nannte das damals zero fuck-ups policy, Null-Vergeigen-Ziel.

### **Warum er sicherstellte, dass die Dokumente in verschiedene Länder verteilt wurden**

Das ist das Konzept der Herdenimmunität. Die einen bieten Schutz für die anderen. Insbesondere, wenn man die Dokumente über unterschiedliche Rechtsprechungen etc. verteilt, wird es sehr viel schwieriger, die Absicht zu untergraben. Niemand konnte es aufhalten.

Aber als Ingenieur, besonders als jemand, der mit Telekommunikation und solchen Dingen an diesen Systemen gearbeitet hat, hat man immer große Angst vor dem SPOF (single point of failure), einer nicht abgesicherten Schwachstelle, verstehen Sie?

Das habe ich den Journalisten gesagt: „Wenn die Regierung denkt, dass Sie der single point of failure sind, werden sie Sie umbringen.“

### **Warum er nicht lieber direkt nach Ecuador statt nach Hongkong ging**

Ja, das ist was, was niemand so richtig wahrnimmt. Alle denken, da hätte es so eine Art Masterplan gegeben, um sicher herauszukommen und alle Konsequenzen zu vermeiden. Darum soll es in

Hongkong gegangen sein. Ging es aber nicht. Das Ziel meiner Mission war, die Information an Journalisten zu übergeben. Als das geschafft war, war ich fertig.

Deswegen war ich danach so ruhig, weil es egal war, was passieren würde ... nach Ecuador zu reisen und dort Asyl zu bekommen, wäre großartig gewesen ... Und wäre ein Bonus gewesen. Die Tatsache, dass ich jetzt hier so sicher gelandet bin, ist reiner Zufall. Wie Sie sagen, es hätte wahrscheinlich nicht so kommen sollen. Wenn man jemandem danken muss, dann wohl dem Außenministerium. Der Schlüssel zum Ganzen ist, dass es das Außenministerium ist, das mich nach Russland gelotst hat.

### **Das letzte Jahr**

Es war unerwartet und herausfordernd, aber es macht Mut. Es hat mich bekräftigt, die Reaktion der Öffentlichkeit zu erleben. Es hat die Sache gerechtfertigt, wenn ich die Reaktionen von Parlamentsabgeordneten, Richtern und öffentlichen Verwaltungen auf der ganzen Welt sehe, und Bürgerrechtsaktivisten, die sagen, dass es stimmt, dass wir wenigstens im Groben wissen sollten, was unsere Regierungen da in unserem Namen und gegen uns tun.

Teil davon zu sein, und wenn auch nur ein kleiner Teil, ist, denke ich, eine der größten Löhne für meine Arbeit in meinem bisherigen Leben.

Das Weiße Haus hat diese Programme [die Massenüberwachung möglich machten] aus zwei separaten Anlässen überprüft und beide Male festgestellt, dass sie überhaupt keinen Wert haben, und dennoch, obwohl beide Untersuchungen empfahlen, sie einzustellen, war es jeweils so, dass wenn das Weiße Haus die Gesetzgeber zum Handeln aufforderte, die Gesetzgebung dann sagte: „Ach, beenden wir die Programme doch nicht. Obwohl sie jetzt zehn Jahre laufen und nicht einen einzigen bevorstehenden Terroranschlag verhindert haben - komm, lassen wir sie weiter laufen.“

### **Das Leben bei der NSA**

Ich begann, von der reinen Betreuung der Systeme überzugehen zur aktiven Steuerung der Nutzung. Viele Leute verstehen nicht, dass ich tatsächlich ein Analyst war und Individuen und Gruppen bestimmt habe, die verfolgt werden sollten.

Ich erfuhr von früheren Programmen wie zum Beispiel Stellar Wind [das während der Präsidentschaft von George W. Bush genutzt wurde]. Das Anzapfen der Leitungen jedes einzelnen Bürgers der USA ohne jede gesetzliche Grundlage, einschließlich der Internetdaten – eine Verletzung gegen Verfassung und Gesetze der USA – verursachte einen Skandal und wurde deswegen beendet.

Als ich das sah, das war dann schließlich der erschütternde Moment, denn er zeigte, dass die Offiziellen, die diese Programme autorisierten, wussten, dass es ein Problem war, sie wussten, dass sie nicht die gesetzlich zugebilligten Befugnisse hatten für diese Programme. Aber die Regierung maßte sich stattdessen, im Geheimen, neue Exekutivgewalt an, ohne jede öffentliche Wahrnehmung oder öffentliches Einverständnis, und nutzte sie gegen die Bürgerschaft ihres eigenen Landes, um die eigene Macht zu stärken und die eigene Wahrnehmung zu verbessern.

Wir hören ständig „national security“, nationale Sicherheit, aber wenn der Staat beginnt, ... in großem Stile die Kommunikation abzuhören, sie an sich zu reißen ohne jede Grundlage, ohne jeden Verdacht, ohne jede juristische Mitwirkung, ohne jede Erklärung der wahrscheinlichen Hintergründe, schützen sie dann wirklich die nationale Sicherheit, oder schützen sie die Sicherheit des Staatsapparates?

Ich gewann den Eindruck – und ich denke, dass mehr und mehr Leute wenigstens das Potential dafür erkannt haben – dass ein System, das als „national security agency“ beschrieben wird, aufgehört hat, im öffentlichen Interesse zu sein und stattdessen angefangen hat, die Interessen der Staatssicherheit zu schützen und zu fördern. Und der Gedanke, dass eine westliche Demokratie

Staatssicherheitsämter hat, alleine dieser Begriff, dieses Wort „Staatssicherheitsamt“, lässt einen erschrecken.

Also, wenn wir an die Nation denken, denken wir an unser Land, unsere Heimat, denken wir an die Leute, die dort leben, an deren Werte. Wenn wir an den Staat denken, denken wir an eine Institution.

Der Unterschied dabei ist, dass wir jetzt ein Institut haben, das sich so mächtig fühlt, dass es sich wohl dabei fühlt, sich selbst mit neuen Rechten auszustatten, ohne Einbeziehung des Landes, ohne Einbeziehung der Öffentlichkeit, ohne volle Einbeziehung aller unserer gewählten Repräsentanten und ohne die volle Einbeziehung der Gerichte, und das ist beängstigend – jedenfalls für mich.

Im großen und ganzen sind es nicht die Leute auf der Arbeitsebene, um die man sich Sorgen machen muss. Es sind mehr die höheren Offiziellen, es sind Entscheidungsträger, die von der Rechenschaftspflicht entbunden werden, die der Aufsicht entzogen werden und die Entscheidungen treffen dürfen, die das Leben von uns allen betrifft, ohne jede öffentliche Einflussnahme, öffentliche Debatte und ohne Konsequenzen bei den Wahlen, weil ihre Entscheidungen und deren Konsequenzen niemals bekannt werden.

Durch den Fortschritt der Technologie, Speicher wird Jahr für Jahr billiger und billiger, und wenn unsere Fähigkeit, Daten zu speichern, schneller ist als der Aufwand, diese Daten überhaupt zu erzeugen, dadurch kommen wir immer mehr in die Lage, dass Daten nicht mehr nur kurzzeitig gehalten werden, sondern über einen längeren Zeitraum, und dann für immer längere Zeiträume. Bei der NSA zum Beispiel werden Daten zu Individuen für fünf Jahre gespeichert. Und das ist möglich, ohne eine Ausnahmegenehmigung einzuholen, mit der der Zeitraum noch ausgeweitet werden kann.

Wir haben eine enorme Anzahl junger, vom Militär angeworbener Menschen, die, ohne dass es deren Fehler wäre, ... bisher vielleicht noch nicht so viel Lebenserfahrung haben, um das Gefühl zu kennen, missbraucht worden zu sein. Und wenn wir die Gefahren und Risiken des Missbrauchs unserer Privatsphäre und unserer Freiheiten noch nicht selbst gespürt haben, wie können wir erwarten, dass diese Menschen unsere Interessen bei der Ausübung ihrer Ämter auf vernünftige Art und Weise berücksichtigen?

## **Die Stasi**

Es hat, soweit wir wissen, noch kein System der Massenüberwachung in irgendeiner Art Gesellschaft gegeben, das nicht missbraucht worden wäre. Wenn wir zum Beispiel die deutsche Stasi anschauen, die war ein Amt für Staatssicherheit, gegründet um die Nation, die Stabilität des politischen Systems zu schützen, von der sie glaubten, dass sie bedroht sei. Sie waren normale Bürger wie jeder andere auch. Sie glaubten, dass sie das richtige tun, glaubten, dass sie was Gutes tun. Aber wenn wir mit historischen Maßstäben darauf schauen, was haben sie mit ihrem Volk gemacht? Was haben sie mit den angrenzenden Ländern gemacht? Was war der Effekt ihrer massenweisen, wahllosen Spionageaktivitäten? Und das sehen wir klarer.

## **Die Beziehungen zwischen der NSA und den Telekommunikations- und Internet-Firmen**

Die Details der finanziellen Abmachungen zwischen der Regierung und den Telekommunikationsanbietern wurden, was ungewöhnlich ist, selbst vor den Leuten geheim gehalten, die für diese Dienstleister arbeiteten. Und wir müssen uns fragen: warum? Warum werden die Detail darüber, wie ihre Zusammenarbeit bezahlt wird, strenger unter Verschluss gehalten als die Namen von Undercover-Agenten, die in Terroristengruppen eingeschleust sind?

Also Prism [das Programm, das das Verhältnis zwischen der NSA und den Internet-Firmen regelt] funktioniert so, dass die NSA direkten Zugriff auf die Inhalte der Server dieser privaten Unternehmen haben. Das heißt nicht, dass die Unternehmen oder die Geheimdienste, auf Ihre Daten zugreifen können, sondern es heißt, dass Facebook der Regierung erlaubt, Kopien Ihrer Facebook-

Nachrichten, Ihrer Skype-Unterhaltungen, Ihrer Gmail-Mailboxen etc. zu machen.

Das ist etwas anderes, als wenn die Regierung sich eigenen Zugang verschafft - sogenannte Upstream-Operationen - wo sie die Hauptleitungen anzapft, auf denen diese Kommunikationen verlaufen, und sie im Durchfluss abfängt. Sie gehen stattdessen zu den Firmen hin und sagen: „Gebt uns dies. Gebt uns das. Gebt uns das.“ Und das Unternehmen gibt ihnen all diese Informationen in kooperativer Zusammenarbeit.

Wenn Facebook alle Ihre Nachrichten, alle Ihre Pinnwand-Einträge, alle Ihre privaten Fotos und alle privaten Details von seinen Servern übergibt, braucht die Regierung nicht all die Übertragungen abzuhören, mit denen diese privaten Daten erstellt werden.

### **Warum Regierungen Verschlüsselung nicht mögen**

Die wichtigsten Ressourcen für Ermittlungen zur Strafverfolgung und zur Informationsgewinnung für Geheimdienste sind solche, die nicht gelöscht werden, egal ob sie ... in der Presse, das heißt gezielte Ausspähung von Computern. ... Es gibt ein globales Netzwerk das geografisch verteilt ist in alle Länder der Welt, unter allen Ozeanen der Welt.

Und die Regierung sagt, wir müssen in der Lage sein, all diesen Datenaustausch abzuhören ... Und deswegen mag sie den Einsatz von Verschlüsselung nicht. Sie sagt, dass Verschlüsselung, die die Privatsphäre von Individuen spezifisch schützt, und solche, die im Gegensatz dazu vertrauliche Daten auf breiterer Basis schützt, dass also Verschlüsselung per se gefährlich ist, weil sie dadurch diese Mittelpunktkommunikation verliert, diese Mittelpunkt-Informationsgewinnung.

In Wirklichkeit kommt jede Kommunikation von einem Quellpunkt und endet an einem Zielpunkt. Und diese beiden Punkte sind Computer, sind Apparate, Mobiltelefone oder Laptops, und die können gehackt werden. Die können auskundschaftet werden, was Strafverfolgungsbehörden und Geheimdiensten direkten Zugriff auf diese Systeme gibt, um diesen Datenaustausch mitzulesen.

### **Über die NSA-Kultur, Weitergabe sexuell kompromittierenden Materials**

Wenn man als NSA-Analyst Rohdaten untersucht, stellt man fest, dass der Großteil der Kommunikation in unseren Datenbanken nicht Kommunikation von Zielpersonen ist, sondern von ganz normalen Leuten, von Nachbarn, Freunden von Nachbarn, Verwandten, der Kassiererin vom Supermarkt. Es sind die tiefsten und intensivsten und intimsten und schädlichsten privaten Momente aus deren Leben, und wir reißen sie an uns ohne jede Erlaubnis, ohne jeden Grund, Aufzeichnungen all ihrer Aktivitäten – die Aufenthaltsorte ihrer Mobiltelefone, ihre Einkaufsdaten, ihre privaten SMS, ihre Anrufe, unter bestimmten Umständen den Inhalt dieser Anrufe, Geschäftsvorgänge – und daraus erzeugen wir eine perfekte oder nahezu perfekte Aufzeichnung der Aktivitäten jedes einzelnen, und diese Aktivitäten werden mehr und mehr dauerhafte Aufzeichnungen.

Viele der Leute, die die Heuhaufen durchsuchen, waren junge, angeworbene Männer und ... 18 bis 22 Jahre alt. Sie wurden plötzlich in eine Position mit außergewöhnlicher Verantwortung versetzt, wo sie nun Zugang zu all Ihren privaten Daten haben. Im Laufe ihrer täglichen Arbeit stoßen sie auf etwas, das mit ihrer eigentlichen Arbeit absolut nichts zu tun hat, zum Beispiel ein intimes Nacktfoto eines Menschen in einer sexuell kompromittierenden Situation, der aber sehr attraktiv ist. Was machen sie also? Sie drehen sich mit ihrem Stuhl um und zeigen es einem Kollegen. Und der Kollege sagt: „Oh, das ist cool. Schick das mal an Bill hinten im Gang.“ Und dann sendet Bill es an George, George an Tom, und früher oder später haben all diese Leute das ganze Leben dieser Person gesehen. Da geht mehr oder weniger alles. Du sitzt wie unter einer Glocke. Jeder hat irgendwie ähnliche Arbeitsfelder, jeder kennt jeden. Die Welt ist klein.

Das wird nie gemeldet, niemals erfährt jemand davon, denn die Kontrolle dieser Systeme ist extrem schwach. Obwohl man jetzt einwenden kann, halb so schlimm, diese Person weiß ja noch nicht mal, dass ihr Bild angeschaut wurde, ist es doch ein Grundprinzip, dass kein einziger Missbrauch

geduldet werden darf. Das reine Festhalten der Kommunikation an sich war bereits Missbrauch. Die Tatsache, dass Ihre privaten Bilder, Aufzeichnungen Ihres Privatlebens, Aufzeichnungen Ihrer intimen Momente aus dem privaten Datenstrom oder dem beabsichtigten Empfänger entrissen wurden ohne spezielle Erlaubnis, ohne spezifische Notwendigkeit, ist in sich eine Verletzung Ihrer Rechte. Warum ist das in der Datenbank der Regierung?

Ich würde sagen, so etwas kann man alle zwei Monate beobachten. Das ist schon mehr als genug, je nach Bekanntenkreis hat, kann es öfter oder seltener sein. Aber diese Dinge werden als Zulagen zum Gehalt für Überwachungspositionen gesehen.

### **Warum die Kontrolle der NSA unangemessen ist**

Ein 29-jähriger kam zur NSA und ging mit allen deren privaten Aufzeichnungen wieder hinaus. Was sagt das über ihre Kontrolle? Sie wussten es nicht einmal.

Die Leute reden über die Dinge, die sie nicht hätten tun sollen, als ob es eine Kleinigkeit wäre, weil niemand irgendwelche Konsequenzen erwartet. Niemand erwartet, zur Rechenschaft gezogen zu werden. Es gibt keine Auditoren, die zu Dir kommen und was anderes sehen als Freunde. Wenn Du Dich selbst kontrollierst, mit welchen realen Konsequenzen muss gerechnet werden?

Die Realität der Arbeit in der Welt der Geheimdienst ist, dass man ständig zutiefst beunruhigende Dinge sieht. Ich habe Bedenken über diese Programme regelmäßig und in einem weiten Kreis geäußert, konkret gegenüber mehr als zehn verschiedenen Kollegen, mit denen ich gearbeitet habe – und zwar Kollegen und Vorgesetzten. Ich ging zu ihnen und zeigte ihnen die Programme und sagte: „Was denkst Du davon? Ist das ungewöhnlich? Wie können wir das tun? Ist das nicht gegen die Verfassung? Ist das keine Verletzung von Rechten?“ und „Warum hören wir mehr amerikanische Kommunikation ab als russische?“

Die Leute, die das Personal für diese Geheimdienst-Büros auswählen, sind ganz normale Leute wie du und ich. Sie sind keine Schnurrbart-zwirbelnden Bösewichte, die „ha ha ha, das ist großartig!“ ausrufen, sie reden so: „Du hast recht. Das überschreitet eine Grenze, aber du solltest besser nichts darüber sagen, denn dann ist deine Karriere beendet.“

Wir alle haben Hypotheken. Wir alle haben Familien. Und wenn du für ein national security System arbeitest, das diese offiziellen Geheimhaltungsregeln hat, dann heißt das, selbst wenn du zu einem ausgewählten Kongressabgeordneten gehst, und zwar einem, den ein Reporter ausgesucht hat, nicht einem, den einer aus der Geheimdienst-Gemeinde ausgewählt hat, die die Missetaten zu verantworten hat, dann heißt das, dass du dafür angeklagt werden kannst. Und wenn du nicht angeklagt wirst, kannst du deinen Job darüber verlieren.

Ich war ein privater Auftragnehmer, kein direkter Angestellter der National Security Agency. Und das bedeutete, dass die wenigen Schutzbestimmungen für Whistleblower, die wir in den USA haben, für mich nicht galten. Ich hätte gefeuert werden und keine Klage führen können gegen diesen Schlag. Ich hätte eingesperrt werden können. Und alle, die für diese Behörden arbeiten, sind sich dessen bewusst.

Thomas Drake, ein Amerikaner, der weitverbreitete Gesetzwidrigkeiten aufgedeckt hat ... [ein hochrangiger NSA-Mitarbeiter, der Bedenken gegen Programme der Behörde und deren Einfluss auf die Privatsphäre geäußert hatte] ... anstelle diese Behauptungen zu überprüfen und anstelle diese Fehlverhalten zu korrigieren, wurde ein Verfahren gegen ihn eingeleitet ... und alle seine Kollegen.

Sie holten sie mit vorgehaltener Waffe aus der Dusche, nackt, vor ihren Familien. Sie beschlagnahmten ihre komplette Kommunikation und elektronischen Geräte, verhörten sie, drohten ihnen, sie lebenslang ins Gefängnis zu stecken, für Jahre, Jahrzehnte, und zerstörten ihre Karrieren.

„Die Öffentlichkeit soll nichts von diesen Programmen wissen. Die Öffentlichkeit soll nicht mitzureden haben bei diesen Programmen und, um Gottes Willen, erfährt die Presse besser nichts

von diesen Programmen oder wir werden euch zerstören.“

### **GCHQ, der britische Partner der NSA, und ob der noch schlimmer ist**

Ihr Respekt für Datenschutzrecht, ihr Respekt für einzelne Bürger, ihre Fähigkeit, ohne Überwachung und Eingriff zu kommunizieren und sich auszutauschen ist nicht fest in Gesetze oder Verordnungen gefasst. Das Ergebnis davon ist, dass Bürger des Vereinigten Königreichs (United Kingdom, UK) und Bürger auf der ganzen Welt, die vom UK verfolgt werden, ob von der UK-Regierung, von UK-Systemen oder UK-Behörden, viel gefährdeter sind als sie es in den USA sind.

Man kann in ihren Dokumenten lesen, dass sie selbst zugeben, dass "wir viel lockerere Aufsichtsregeln haben als wir eigentlich sollten", Punkt, fertig. Darum geht es. Sie genießen Berechtigungen, die man ihnen eigentlich nicht zugestehen sollte. Das Problem dabei ist, wenn man einen ungezügelden Geheimdienst hat, der nicht gut kontrolliert wird, der nicht der Öffentlichkeit Rechenschaft schuldig ist, dass er weitergehen wird, als er muss. Er wird übergreifen. Er wird Systeme und Verfahren einsetzen und Leute verfolgen, die man nicht verfolgen muss.

Tempora [das Internet-Überwachungsprogramm des GCHQ] ist der Beweis ..., dass das GCHQ deutlich weniger strenge rechtliche Grenzen kennt als die Geheimdienste anderer westlicher Regierungen.

Die britische Regierung kann öffentlich sagen "Wir haben sehr strenge Regeln. Es gibt breit angelegte Kontrolle. Es gibt eine intensive Rechenschaftspflicht für alle Beamten, die diese Programme ausführen." Ihre eigenen geheimen Dokumente, klassifizierte Dokumente, von den sie nicht wollen, dass die Öffentlichkeit sie je sieht, sagen etwas ganz anderes, nämlich "Wir haben im Vergleich zu allen anderen westlichen Ländern sehr lockere Aufsichtsregeln."

Und das bedeutet, dass UK-Bürger und die Geheimdienst-Plattformen des UK als Testgelände für alle anderen "five eyes"-Partner genutzt werden – das UK, Kanada, die Vereinigten Staaten, Australien und Neuseeland.

Diese experimentelle Herangehensweise, Informationen zu sammeln, während wir die Öffentlichkeit gleichzeitig im unklaren darüber lassen, wie wir das machen, führt zu einer sehr ungewöhnlichen Situation. Anstelle ein geheimdienstliches Hinweissystem zu haben, das nur wo nötig und seine Befugnisse nur einem zur Bedrohung stehenden Verhältnis einsetzt, gehen wir es technologisch an: "Was ist möglich?" statt "Was müssen wir tun?"

### **Als er erfuhr, dass die britische Regierung die Festplatten des Guardian zerstören wollte**

Erstmal, muss ich zugeben, dass ich in die Hände geklatscht habe. Das ist unsinnig. Ich war schockiert, dass die UK-Regierung wegen einer solchen Kleinigkeit so weit gehen würde. Das sollte doch jedem, der mit Daten oder im Journalismus arbeitet, und jedem in den Geheimdiensten klar sein, dass man Festplatten nicht zermahlen kann.

Wissen Sie, man kann Daten in einem weltweit verbundenen Internet nicht final auslöschen, und besonders dann nicht, wenn ... die Journalisten, die dabei waren, noch immer da sind. Und trotzdem haben sie es getan. Es sah aus wie ein klarer Versuch, die Presse einzuschüchtern, damit die sich heraushalten und nicht berichten. Und ich denke, dass es genau darum zwar unangemessen, aber enorm förderlich für die öffentliche Diskussion war, weil sie allen, die sich über Machtmissbrauch Sorgen machten, ein klares Beispiel lieferten.

Was sind das für Länder, in denen Regierungsleute einfach in Redaktionsräume eindringen und die Zerstörung journalistischen Materials verlangen. Hoffentlich erleben wir so etwas nicht wieder.

### **Metadaten**

Man unterscheidet normalerweise Metadaten von Inhalt. Menschen verstehen unter Metadaten die

Details des Anrufs – wann man anrief, wen man anrief, wenn der Anruf zustande kam, wie lang er dauerte – im Gegensatz zum Inhalt des Anrufs - also was gesagt wurde. Als Analyst interessiert einen in neun von zehn Fällen bis ziemlich am Ende der Untersuchungskette nicht, was am Telefon gesagt wurde. Man kümmert sich um die Metadaten, denn die lügen nicht.

Menschen lügen am Telefon, wenn sie an echten kriminelle Aktivitäten beteiligt sind. Sie gebrauchen Codewörter. Sie reden drumherum. Man kann sich nicht auf das verlassen, was man hört, aber man kann den Metadaten vertrauen. Deshalb sind Metadaten oft zudringlicher.

Metadaten sind so wie die Details, die ein Privatdetektiv ... im Zuge seiner Ermittlungen herausfindet. Er kann Ihnen zum Beispiel zu einem Abendessen folgen, wo Sie einen Freund treffen, oder eine Geliebte. Er sieht, wen Sie treffen, wo Sie sich getroffen haben, er sieht, wann Sie da hingegangen sind und er kennt vielleicht auch die groben Details der Themen Ihrer Unterhaltung, aber er wird nicht den ganzen Inhalt mitbekommen haben. Er wird nicht nah genug herangekommen sein und sich zu erkennen geben haben, um alles zu hören, was sie gesagt haben.

Mit diesen Programmen ging es so, dass Regierungen, zum Beispiel des UK, der Vereinigten Staaten und anderer westlicher Regierungen, und auch weniger verantwortliche Regierungen überall auf der Welt, es auf sich genommen haben, Privatdetektive anzusetzen auf jeden einzelnen Bürger in ihrem Land und, soweit es ging, auf der ganzen Welt. Das geschieht automatisch, ist allgegenwärtig, und es wird in Datenbanken gespeichert, ob es nötig ist oder nicht.

## **Deutschland**

Ich finde es bedauerlich, dass in einigen Ländern – und das ist vor allem in Westeuropa sehr verbreitet der Fall – die Prioritäten der Regierungen sich sehr von denen des Volkes unterscheiden. Ich finde es bedauerlich, wenn zum Beispiel in Deutschland herausgekommen ist, dass die NSA Millionen deutscher Bürger ausgespäht hat ... und das kein Skandal ist. Aber wenn Angela Merkels Mobiltelefon abgehört wird und sie selbst zum Opfer wird, dann ändert sich das auf einmal.

Wir sollten hohe Amtsträger nicht erheben. Wir sollten Führer nicht über den durchschnittlichen Bürger nicht erheben, denn für wen arbeiten die denn schließlich? Wissen Sie, das öffentliche Interesse ist das Staatsinteresse. Wissen Sie, die Prioritäten der NSA sollten nicht Vorrang haben vor den Bedürfnissen der deutschen Bevölkerung.

Es besteht immer mehr Einigkeit, dass der Status Quo nicht länger zu halten ist, dass sich Dinge ändern müssen und dass die Öffentlichkeit mitreden können muss über die Art und Weise, wie die Regierung ihren Überwachungsapparat betreibt und darüber, wo die Grenzen um unsere Rechte gezogen werden.

Ich finde es überraschend, dass sie mich in Deutschland gebeten haben, als Zeuge auszusagen und ihnen bei den Ermittlungen zur Massenüberwachung zu helfen, mir aber gleichzeitig die Einreise nach Deutschland untersagt haben. Das hat zu der außergewöhnlichen Situation geführt, in der die Suche nach der Wahrheit den politischen Prioritäten untergeordnet wurde ... Ich denke, das erweist dem Volk einen schlechten Dienst. ... Das ist wahrscheinlich zu politisch. Ich hasse Politik. Wirklich, wissen Sie, ich will sagen, es geht nicht um mich. Ich hoffe, Sie können da den Unterschied sehen.

## **Gefährdung der Sicherheit des ganzen Netzes**

Eine Backdoor, Hintertür, in einem Kommunikationssystem, in einem Internet-System oder in einem Verschlüsselungsverfahren ist im Grunde eine geheime Methode, die Sicherheit dieser Systeme zu umgehen. Sie ist ein Weg, alle Datenschutz- und Sicherheitsversprechen zu untergraben, die eine Firma oder ein Verfahren den Menschen machen, die ein Produkt oder einen Dienst nutzen.

Die Gefahr des Einbaus solcher Backdoors, auf denen das ganze Internet beruht, zum Beispiel des

Bullrun Programms, wo sich herausgestellt hat, dass NSA und GCHQ zusammenarbeiten und die Verschlüsselungsmethoden schwächen, besteht darin, dass, wenn Sie online auf Ihr Bankkonto zugreifen, dort eine versteckte Schwäche bestehen könnte, die es den Geheimdiensten der westlichen Regierungen erlaubt, Ihre Kontodetails mitzulesen.

Was viele oft übersehen, ist die Tatsache, dass, wenn man eine Backdoor in ein System einbaut, diese von jedem auf der Welt entdeckt werden kann. Das kann ein Privatmann sein, ein Sicherheitsforscher an einer Universität, aber auch eine kriminelle Gruppe. Es kann auch ein fremder Geheimdienst sein, sagen wir ein der NSA entsprechender Dienst einer zutiefst unverantwortlichen Regierung in irgendeinem fremden Land. Und dieses fremde Land kann jetzt nicht nur Ihre Bankdaten genau untersuchen, nicht nur Ihre privaten Geschäfte, sondern Ihre gesamte Kommunikation im Internet und in jeder Institution ..., die diese Standards verwendet, ob es Facebook ist, Gmail, Skype oder Angry Birds. Auf einmal sind Sie elektronisch nackt, während Sie im Internet Ihren Aktivitäten nachgehen.

Diese Entscheidung wurde nicht in einer öffentlichen Einrichtung diskutiert, sie wurde von keinem Gesetzgeber legitimiert. Jedenfalls haben, wenigstens in den USA in den 1990ern, Strafverfolgungsbehörden speziell um diese Art von Backdoor-Zugang zu Internet-Datenübertragungen gebeten. Und unsere gewählten Repräsentanten im Kongress haben sie abgelehnt. Sie sagten, es sei eine Verletzung unserer Bürgerrechte und ein unnötiges Risiko für unsere Kommunikation, und deshalb haben sie sie abgelehnt.

Jetzt sehen wir sie zehn Jahre später, anstelle wieder zum Kongress zu gehen und anzufragen, einfach daran vorbeigehen, und die Geheimdienstler ... sagen: „Wir machen das. Egal, was der Kongress sagt. Egal, was die Öffentlichkeit denkt. Wir machen das, weil es uns einen Vorteil bringt.“

Und die Konsequenzen daraus sind heute unbekannt, denn fremde Widersacher könnten die Backdoors ausnutzen, die Geheimdienste in Ländern wie dem Vereinigten Königreich, wie der GCHQ, in unsere Kommunikationssysteme eingebaut haben ... und wir wissen nicht einmal, dass das geschieht.

Die Enthüllungen des letzten Jahres haben uns den unwiderlegbaren Beweis erbracht, dass unverschlüsselte Kommunikation im Internet nicht mehr sicher und vertrauenswürdig ist. Deren Integrität ist kompromittiert, und wir brauchen neue Sicherheitsprogramme, um die Kommunikation zu schützen. Jede Kommunikation, die über das Internet übertragen wird, oder über jede andere Netzwerk-Leitung, sollte standardmäßig verschlüsselt werden. Das hat das letzte Jahr uns gezeigt.

## **Privatsphäre**

Sicher können wir hypothetische Fälle konstruieren, in denen eine Art von Massenüberwachungs-System, von Gesichtserkennungs-System zur Verhinderung von Straftaten beitragen könnte. Genauso könnte man sich aber auch den hypothetischen Fall vorstellen, dass, wenn wir der Polizei freien Zutritt zu unseren Wohnungen gewähren und alles zu durchsuchen, während wir bei der Arbeit sind, dass dann allerlei Straftatbestände, Drogenkonsum und gesellschaftliche Missstände entdeckt würden. Aber wir ziehen die Grenze, wir müssen sie irgendwo ziehen. Die Frage ist, warum sollen unsere online übertragenen und auf unseren privaten Geräten gespeicherten persönlichen Daten irgendwie anders sein als die Details und privaten Aufzeichnungen, die wir in unseren Tagebüchern festhalten?

Es sollte keine Unterscheidung zwischen digitaler und gedruckter Information geben. Aber Regierungen in den Vereinigten Staaten und vielen anderen Ländern auf der Welt wollen zunehmend diese Unterscheidung machen, weil sie erkennen, dass das Ihre Ermittlungsmacht aktiv vergrößert.



## **Ob Technologie sich mit Privatsphäre verträgt**

Absolut. Technologie kann die Privatsphäre verbessern, aber nicht, wenn wir in neue Anwendungsgebiete hinein schlafwandeln, ohne die Implikationen dieser Technologien zu beachten.

Jede neue Technologie erzeugt, sobald sie in einem bestimmten Maße angewendet und vernetzt wird, ein Netz neuer Sensoren in unserem Leben, die etwas erfassen – das könnten Wetteränderungen sein, unsere Telefoniergewohnheiten, die Art, wie wir Dinge einkaufen, Dinge, die wir mögen, die Temperatur, bei der wir gerne baden.

Wenn wir nicht an die Implikationen dieser Technologien denken, während wir sie entwickeln und anwenden, kann es gefährlich werden. Aber in dem Maße, wie wie unser Erkenntnisniveau über Bedrohungen wächst, die in neuen Technologien stecken, wenn sie eingeführt werden, in dem Maße können wir die Möglichkeiten dieser Technologien mit eingebauten Schutzmechanismen versehen, die dafür sorgen, dass die Details über uns, unser Leben, über die Art, wie wir leben, nur von denen gesehen werden, die wirklich Zugriff darauf haben sollen.

Die meisten vernünftigen Menschen würden der Aussage zustimmen, dass Privatsphäre in einem Abhängigkeitsverhältnis zur Freiheit steht. Und wenn wir die Privatsphäre abschaffen, machen wir uns weniger frei. Wenn wir in offenen und liberalen Gesellschaften leben wollen, brauchen wir sichere Orte, wo wir mit neuen Gedanken experimentieren können, mit neuen Ideen, und [wo] wir herausfinden können, was wir wirklich denken und woran wir wirklich glauben, ohne beurteilt zu werden. Wenn wir nicht die Privatsphäre unserer Schlafzimmer haben können, nicht die der Notizen auf unserem Computer, nicht die unserer elektronischen Tagebücher, dann haben wir überhaupt keine Privatsphäre.

## **Wann er das letzte Mal 1984 gelesen hat**

Das ist schon einige Zeit her. Im Gegensatz zur allgemeinen Meinung glaube ich nicht, dass wir uns im 1984-Universum befinden. Die Gefahr ist, dass wir sehen können, wie einfallslos und altmodisch [Orwells] Technologien aus [dem Buch] 1984 jetzt erscheinen. Die sprachen von Dingen wie Mikrofonen in Büschen und Kameras in Fernsehern, die uns zuschauen. Heutzutage haben wir Webcams, die uns überall hin begleiten. Wir kaufen Mobiltelefone, das ist dasselbe wie ein Netzwerk-Mikrofon, das wir in unseren Taschen freiwillig mit uns herumtragen, während wir von hier nach da und durch unser Leben gehen.

1984 ist ein wichtiges Buch, aber wir sollten uns nicht zu eng an die Grenzen der Vorstellungskraft des Autors halten. Die Zeit hat gezeigt, dass die Welt viel unvorhersehbarer und gefährlicher ist.

## **Die Politik und die Kontrolle der Geheimdienste**

Das ist wahrscheinlich ... der allerwichtigste Faktor, um das Scheitern der Kontrolle zu erklären, die wir in fast allen westlichen Regierungen sehen. Normalerweise sind es die ältesten Mitglieder der öffentlichen Verwaltungen, die die Geheimdienste kontrollieren, die Beamten, die schon länger dabei sind als die Möbel, auf denen sie sitzen. Und das ist so, weil man spürt, dass man diesen Leuten vertrauen kann, die kennen sich aus, die haben einen klaren Kopf.

Aber wir müssen den Maßstab der Fachkenntnis anlegen, denn die Technologie ist eine neue Art der Kommunikation, ein neues Alphabet von Symbolen, die die Menschen intuitiv verstehen müssen. Das ist wie etwas, das man lernt ... gerade so, wie man in der Schule Buchstaben schreiben lernt. Sie haben gelernt, wie man Computer nutzt, wie diese interagieren, wie sie kommunizieren. Und technische Fachkenntnis ist in unserer Gesellschaft eine knappe und wertvolle Ressource. Deshalb verdienen so viele IT-Berater, die im Grunde nur Drucker reparieren, richtig gutes Geld, weil sich nicht jeder mit dem Zeug auskennt. Und das brauchen wir in der Regierung, wir brauchen Rechtsanwälte, wir brauchen Spezialisten, wir brauchen Experten, [die] diesen älteren Bediensteten

zuarbeiten und so weiter, und die können helfen und erklären und übersetzen genau so wie ein Dolmetscher.

Die entscheidende Frage ist, wollen wir, dass die öffentliche Politik die Geheimdienste reglementiert, oder wollen wir, dass die Geheimdienste ihre eigene Politik machen, ihr eigenes Reglement, über das wir keine Kontrolle und Überblick haben? Und das denke ich, ist der entscheidende Unterschied.

### **Ob er Beweise an den britischen Geheimdienstausschuss liefern wird**

Im allgemeinen, glaube ich, dass es jedem gesetzgebenden Gremium gut ansteht, jemanden ... persönlich anzuhören. Es gibt natürlich Umstände, unter denen das nicht möglich ist. Aber wenn es um echte Zeugenaussagen geht und nicht um Expertenmeinungen, dann denke ich, dass es wichtig ist, sicherzustellen, dass sie persönlich vorgetragen werden, im Parlamentssaal, um die Zeugen nicht unbeabsichtigt oder zufällig unnötiger gesetzlicher Haftung auszusetzen.

### **Der Vorfall, weshalb das Flugzeug des bolivianischen Präsidenten Evo Morales landen musste**

Nachdem ich mir alles angehört hatte, dachte ich erst „wow“, ihr Geheimdienst ist echt scheiße ... Aber dann dachte ich, werden sie wirklich so weit gehen, den Präsidenten einer lateinamerikanischen Nation so total zu demütigen, den Repräsentanten so vieler Leute, den einzigen indigenen Präsidenten, den es gibt? Es war einfach nur schockierend schlecht ausgedacht, aber sie haben es trotzdem getan, und sie machen weiter solche Fehler ... Ich fühlte mich beinahe, als ob ich einen Freund in der Regierung hätte, der sagt „Oh ja, mach das, unbedingt, das ist klasse.“

### **Sein Leben in Russland und ob die Leute ihn erkennen**

Das ist nicht so viel anders. Wissen Sie, ich glaube, es gibt Typen, die einfach nur hoffen, mich traurig zu sehen. Und die werden weiter enttäuscht sein ... Ich lebe nicht ganz im geheimen. Ich lebe ein ziemlich offenes Leben. Aber ... ich will keine Berühmtheit sein, ich will nicht irgendwo hingehen und dass die Leute mir Beachtung schenken, so wie ich das auch nicht in den Medien will. Es gibt auf der Welt viel wichtigere Themen als mich und was in meinem Leben passiert, und wir sollten uns darauf konzentrieren.

Was ich im Lebensmittelladen kaufe, sollte echt niemanden interessieren. Und wenn ich erkannt werde, werde ich eben erkannt. Mein alltägliches Leben, schätze ich, interessiert niemanden.

Ich werde erkannt. Manchmal ist es ein bisschen unangenehm, weil mein Russisch nicht so gut ist, wie es sein sollte. Ich lerne noch. Aber ja, hin und wieder erkennt mich jemand. [Er weigert sich, etwas auf Russisch zu sagen.] Das allerletzte, was ich will, ist, dass Videoclips von mir durch das Internet geistern, in denen ich Russisch spreche.

[Darüber, dass er auf einem Moskauer Touristenschiff fotografiert wurde] Richtig, auf dem Bild sah ich nicht glücklich aus. [Darüber, einen vollen Einkaufswagen über eine Straße zu schieben] Wissen Sie, ich weiß gar nicht, weil es so weit weg und verschwommen war. Also, das könnte ich gewesen sein.

[Darüber, angeblich verkleidet vor die Türe zu gehen] Bevor ich in den Supermarkt gehe, setze ich meine Groucho Marx-Brille auf, die Nase und den Schnurrbart... Nein, ich laufe nicht verkleidet herum.

Ich bin hier in Russland viel glücklicher, als wenn ich einem unfairen Gerichtsverfahren ausgesetzt wäre, in dem ich nicht einmal einer Jury aus Fachleuten eine Verteidigung des Staatsinteresses präsentieren kann. Wir haben [die] Regierung wieder und wieder um einen fairen Prozess gebeten, aber sie haben abgelehnt. Und ich bin sehr froh, Asyl bekommen zu haben. Russland ist ein

modernes Land, und es hat mich gut behandelt, also ja, ich lebe ein ziemlich normales Leben und ich würde sehr gerne wieder reisen können wie in der Vergangenheit. Ich würde gerne wieder nach Westeuropa reisen, aber das kann nicht ich entscheiden, das müssen das Volk und die Regierungen jedes einzelnen dieser unabhängigen Länder.

### **Russisch lernen und Dostojewski lesen**

Mein Russisch und meine Beherrschung von Dostojewski sind beide weniger entwickelt als sie sein könnten, aber ich habe Freude daran. Die Brüder Karamasow sind glaube ich als nächstes dran. Ich lerne gerne, und das macht richtig Spaß.

Ich lese zur Zeit viele politische Bücher. Ich versuche, meine Kultiviertheit auf die meiner Umgebung anzuheben. Im Moment lese ich eine Denkschrift von Dan Ellsberg, Secrets, über seine Veröffentlichung der Pentagon-Papiere.

### **Unter Beobachtung zu stehen**

Ich erkenne keine bedrückende, aktive Überwachung, aber ich denke, es ist angemessen, anzunehmen, dass ich unter Beobachtung stehe. Jeder in meiner Lage wird sicher irgendwie überwacht, aber man trifft so gut man kann Vorkehrungen, um sicherzustellen, dass man selbst unter Beobachtung keine heiklen Informationen herausgibt.

### **Wie er seine Zeit verbringt**

Zuletzt habe ich viel Zeit damit verbracht, über Pressefreiheitsthemen nachzudenken, in Ergänzung zur privaten Kommunikation des Normalbürgers, und ich habe Partnerschaftsbeziehungen aufgebaut zu Bürgerrechtsorganisationen, um zu schauen, wo wir beitragen können und versuchen, neue Werkzeuge, neue Techniken, neue Technologien herzustellen, die den Schutz unserer Rechte sicherstellen, egal wie die gesetzliche Situation in einem bestimmten Rechtssystem gerade ist

Stellen Sie sich eine App oder ein Mobiltelefon oder ein Betriebssystem für ein Mobiltelefon oder ein kleines Gerät vor, irgendwas, das Menschen einen kostenlosen und betriebsbereiten Zugang zu einer wirklich sicheren Kommunikationsplattform ermöglicht, etwas, das keine besonderen Kenntnisse erfordert, um es zu nutzen und zu bedienen.

Wir können vielleicht auf die Möglichkeit einer Reform in den Vereinigten Staaten, dem Vereinigten Königreich oder einer anderen modern entwickelten Demokratie vertrauen. Aber es gibt viele Leute an vielen Orten, die darauf nicht vertrauen können. Und also werde ich künftig mehr und mehr Zeit darauf verwenden, zu versuchen, neue Werkzeuge zu entwickeln, die ihnen ihre Rechte garantieren, die nicht durch gesetzliche Garantien abgedeckt sein könnten. Denn eines wird oft vergessen im Dialog von Sicherheit versus Privatsphäre, und das ist die falsche Darstellung des Themas, das nämlich Freiheit versus Sicherheit lautet.

### **Die Bombenexplosion beim Boston Marathon**

Trotz der Tatsache, dass in Amerika im Moment die Kommunikation aller abgehört wird, sind die Bombenleger von Boston nicht erwischt worden, und das trotz der Tatsache, dass russische Geheimdienste das FBI gesondert darauf hingewiesen hatten, dass diese Personen als mit islamistischen Terrorgruppen assoziiert bekannt waren.

Wir haben sie einfach nicht komplett überprüft, wir haben nur mal oberflächlich darüberschaut, und sind wieder zu unseren Tastaturen, zur Tagesordnung zurückgekehrt, jedermanns E-Mails und SMS-Nachrichten zu lesen.

Die Frage der Bombenexplosion von Boston ist nicht, unter welche Art der Massenüberwachung stellen wir die gesamte Gesellschaft, um jedes auch nur eben wahrnehmbare Verbrechen zu

verhindern, das in Zukunft geschehen könnte, die Frage ist, warum sind wir der Sache nicht nachgegangen, ... als wir explizit vor diesen Personen gewarnt wurden und die sich dann später als echte Bedrohung herausstellten. Was wir im letzten Jahrzehnt in Terrorismus-Fallstudien gelernt haben ... ist, dass fast jeder terroristische Akt, der aufgedeckt wird, fast jeder, der überführt, verurteilt und ins Gefängnis gesteckt wird, jeder Plan, der vereitelt wird, nicht ein Resultat der Massenüberwachung ist, nicht ein Resultat dieser Art von unterschiedsloser Überwachung, wie wir sie heute kennen. Alle Erfolge sind Resultat von gezielter Überwachung, traditioneller Überwachung, ganz klassisch vor Ort, ermitteln und Schlüsse ziehen, von echten Ermittlern, die echte Menschen verhören und erfolgversprechende Spuren verfolgen, die sich im Verlauf der Ermittlungen ergeben. Kein einziger terroristischer Akt, die Bomben in Boston eingeschlossen, wurde jemals als Resultat einer Massenüberwachung in den Vereinigten Staaten abgefangen.

Es erscheint vernünftig, anzunehmen, dass, wenn es klare Hinweise darauf gibt, dass diese Programme ineffektiv sind, dass wir dann die Ressourcen aus diesen ineffektiven Massenüberwachungsprogrammen abziehen und sie in Richtung der Art traditioneller, zielgerichteter Überwachung verschieben sollten, die sich seit hunderten Jahren als effektiv erwiesen hat.

### **Technologie im allgemeinen**

[Nutzt er Dropbox?] Sie haben gerade Condoleeza Rice in den Vorstand berufen, die wahrscheinlich Privatsphäre-feindlichste Beamtin, die man sich vorstellen kann. Sie ist eine von denen, die Stellar Wind angeschaut und es für eine gute Idee gehalten haben. Sie stehen der Privatsphäre also feindselig gegenüber. Obwohl wir im Moment noch nicht unmittelbar revolutionäre Veränderungen sehen, sieht die Wirklichkeit wohl so aus, dass Technologie-Mitarbeiter eine wichtige Gruppe sind, die der Gesellschaft einen wichtigen Dienst erweisen.

Sie besitzen ein einzigartiges Niveau technologischer Kenntnisse, das es ihnen erlaubt, für oder gegen unsere natürlichen Rechte zu arbeiten. Und was ich das letzte Jahr über gesehen habe, ist, dass da eine ungemein große Einigkeit unter ihnen darüber besteht, dass unsere private Kommunikation auch privat bleiben soll, dass wir den Schutz gegen diese Art Übergriffe und Missbrauch durch Geheimdienste erhöhen sollten, und dass Massenüberwachung kein Thema sein sollte.

[Warum wir Google mehr trauen sollten als dem Staat?] Zunächst mal müssen Sie das nicht. Sich Google anzuschließen ist freiwillig. Aber es stellt sich eine wichtige Frage. Und ich würde sagen, dass, obwohl da ein Unterschied ist – Google kann Sie nicht ins Gefängnis stecken, Google kann keine Drohne programmieren, eine Bombe auf Ihr Haus abzuwerfen – wir ihnen nicht trauen sollten ohne zu überprüfen, welche Aktivitäten sie unternehmen und wie sie unsere Daten nutzen.

Wir sollten eine Art Zivilschutz haben, eine Art ziviler Maßnahmen, auf die wir zurückgreifen können und die überprüfen, wie Firmen unsere Daten nutzen. Und wir sollten wenigstens eine breite gesellschaftliche Übereinkunft haben darüber, wo die Grenze zu ziehen ist, ohne unnötig neue Geschäftsmodelle und Dienste zu beschädigen, die wir zwar heute noch nicht voraussehen können, morgen aber brauchen werden ... Ich nutze Google nicht. Ich habe Skype und Google Hangouts genutzt, die klasse sind, aber leider in ihrer Sicherheit kompromittierte Dienste. Ich habe sie für öffentliche Diskussionen eingesetzt, wenn es erforderlich war, aber ich würde sie nicht für private Kommunikation nutzen.

Ich denke, dass jeder in seinem Leben irgendwie mit proprietärer Software in Kontakt kommt, selbst wenn er sich dessen nicht bewusst ist. Auf Ihren Mobiltelefonen laufen Unmengen proprietären Codes der verschiedenen Chiphersteller und Mobilfunkanbieter.

Wir bewegen uns langsam aber sicher in die Richtung freier und offener Software, die überprüfbar ist, oder wenn Sie es selbst nicht können, gibt es eine Programmierer-Community, die sich anschauen kann, was diese Geräte tatsächlich tun, und sagen, ob das sicher und angemessen ist,

oder ob da was bösartiges oder merkwürdiges drin steckt? Das verbessert das Sicherheitsniveau für jeden in unseren Gemeinschaften.

Wir wollen keine Fragmentierung des Internet. Das nützt niemandem, weder in Brasilien, noch in Deutschland, noch in irgendeinem anderen Land der Welt. Was wir brauchen, sind gemeinsame Protokolle, die Daten und Übertragungen schützen unabhängig von den Rechtssystemen, durch die sie geleitet werden.

Man möchte zum Beispiel nicht, dass, wenn ein ein Franzose etwas über ein Netzwerk an einen Dienst in die USA schickt, dieser Versand in jedem der Länder, durch die er läuft, überwacht, manipuliert oder überprüft wird. Und umgekehrt genauso. Und wenn das für europäische Ländern gilt, dann sollte das für lateinamerikanische genauso gelten und ebenso für asiatische und afrikanische.

Und das kann nur klappen, wenn wir die Sicherheit unserer gemeinsamen Basis verbessern, es geht um die Art, wie wir allgemein im Internet kommunizieren, die Basisinfrastruktur, über die wir alle kommunizieren.

### **Kritik wegen des Schadens, den er angerichtet habe**

Dass Leute wissen, dass man Kommunikation überwachen kann, hält sie nicht davon ab, zu kommunizieren ... denn sie können nur wählen, ob sie das Risiko annehmen, überwacht zu werden, oder gar nicht kommunizieren. Und wenn wir über Dinge wie terroristische Zellen sprechen oder Atomwaffenhändler – das sind organisierte Zellen. Das sind Dinge, die kann ein einzelner gar nicht alleine. Wenn die also aufhören, miteinander zu kommunizieren, dann haben wir schon gewonnen. Wenn wir es geschafft haben, den Terroristen auszureden, unsere modernen Kommunikationsnetzwerke zu nutzen, haben wir doch, was unsere Sicherheit angeht, gewonnen – nicht verloren.

[Über Vorwürfe, er schwäche die Demokratie, die er zu schützen beteuert] Was diese Geheimdienstler sagen, ist, dass das Demokratie-Modell als solches nicht aufrecht zu erhalten ist, dass man dem Volk nicht zutrauen kann, die richtigen Entscheidungen zu treffen, dass wir damit aufhören und zu einem autoritären Regierungssystem übergehen sollen. Ich glaube aber, wenn wir es als Volk unabhängig anschauen und Entscheidungen treffen, dann erschüttern uns diese geschwollenen Klagelieder nicht, für die es auch keine stützenden Beweise gibt. Was uns diese Geheimdienste in Wirklichkeit fragen, ist: Wollen wir in einer Demokratie leben, in der wir gelegentlich dem Risiko eines Unglücks ausgesetzt sind, das wir nicht voraussehen und vor dem wir uns nicht schützen können? Oder würden wir lieber in einem chinesischen oder russischen Modell leben, in einer Kontrollgesellschaft, die aber weniger frei ist?

Es geht nicht darum, von welchen Überwachungsprogrammen die Öffentlichkeit wissen darf, sondern bis zu welchem Detail. All die Spionagechefs sind aufgetreten und haben verkündet, dass die Atmosphäre verglühen wird, ... die Welt endet, der Himmel uns auf den Kopf fällt, und doch ist bisher nichts davon eingetreten. Die einzigen Leute, die sich vor Freude die Hände reiben, sind die Reformer, die mehr und mehr Beweise dafür sehen, dass die Regierungen hier übers Ziel hinausgeschossen sind und unfähig, die Behauptungen aufrecht zu erhalten, die sie immer und immer und immer wieder machen, seit die Veröffentlichungen begonnen haben.

Ich kann ihnen jetzt hier sagen, dass auch nach dem letzten Jahr noch immer Terroristen festgenommen werden, es wird noch immer Kommunikation abgehört. Es gibt noch immer Erfolge von Geheimdienstoperationen, die auf der ganzen Welt stattfinden.

### **Kritik, er sei heuchlerisch und empöre sich selektiv**

Die Leute sagen, entweder bist du naiv oder du hast eine Doppelmoral. Das machen doch alle Länder. Aber das stimmt nicht. Es hat sicher nicht jedes Land die Kapazitäten für einen

Geheimdienst. Sagen wir also: Ok, was ist mit den Top-Geheimdiensten? Machen die alle dasselbe? Die Antwort ist: nein.

Jemand muss anfangen, muss eine Technologie entwickeln, muss sie anwenden, und das sehen wir. Wir sehen, dass die Vereinigten Staaten und andere Länder der Five-Eyes-Allianz neue Wege einschlagen, um in das Privatleben einzudringen sowohl von legitimen Zielpersonen als auch in das aller anderen, die im Schleppnetz der Massenüberwachung mitgefangen werden.

Wir wissen außerdem auch, dass einige Länder nicht in der gleichen Art spionieren wie wir. Leute können behaupten, meine Empörung sei selektiv, aber wenn wir ... in Deutschland Woche für Woche einen CIA-Spion nach dem anderen entdecken, aber keinen deutschen Spion in den Vereinigten Staaten, und die deutsche Regierung sagt, sie habe keine solchen Spione, dann gibt es keinen Anlass, solche Dinge zu behaupten.

Nochmal, wenn wir sagen wollen, dass das der Fall ist, dann sollten wir einen Beweis haben, irgendeine Art Beleg, wenigstens einen winzigen Fetzen, einfach einen Hinweis, dass es vorkommt, bevor wir es als eine Tatsache hinstellen. Es könnte sein, dass wir einen terroristischen Plan aufdecken oder mehr Verbrecher entdecken könnten, wenn wir alle Aufzeichnungen privater Aktivitäten beschlagnahmen, uns auf Schritt und Tritt überwachen, jedes Wort analysieren, das wir sagen, abwarten und Urteile fällen über jede Assoziation, die wir haben, und alle Menschen, die wir lieben. Aber ist das die Art Gesellschaft, in der wir leben wollen? Das ist die Definition eines Sicherheitsstaates.

Wollen wir in einer Kontrollgesellschaft leben oder wollen wir in einer freien Gesellschaft leben? Das ist die fundamentale Frage, die uns gestellt wird.

### **Kritik an seinen Verbindungen zu Russland**

Da ich keinerlei klassifiziertes Material mit nach Russland gebracht habe, heißt das, obwohl das hier ein Gulag-Staat ist, wo mir jede Nacht die Finger gebrochen und ich mit Ketten geschlagen werde, dass es für sie nichts zu gewinnen gibt. Ich meine, die Ängste sind überzogen. Was viele Menschen nicht verstehen, ist, dass wir Geheimdienst-Leute nicht eine endliche Liste von Quellen und Methoden haben, wo wir zum Regal gehen, etwas herausnehmen, es nutzen und dann wieder zurückstellen. Und wenn es kaputt geht, fehlt da für immer was, das man nie zurückbekommen kann.

Die Geheimdienste in den Vereinigten Staaten, genaugenommen jeder Geheimdienst ist viel eher mit einer Fabrik zu vergleichen, die Methoden zur Informationsgewinnung ... erzeugt. Wenn ich etwas tolles wüsste über ein Geheimdienst-Programm und geschlagen oder gefoltert würde oder irgendwie anders kompromittiert, diese Information preiszugeben, wäre die nur eine kurze Zeit lang gültig. Und da die Regierungen, für die ich gearbeitet habe, wussten, worauf ich Zugriff hatte, werden sie in der Lage sein, diese Programme abzuschalten. Sie wären in der Lage, eine Gefährdung zu erkennen.

Die Geheimdienstler wissen, dass ich für keine ausländische Regierung arbeite. Sie haben in der Washington Post anonym ausgesagt, dass ich kein Agent einer fremden Macht sei, sie haben keinen Haftbefehl deswegen ausgestellt. Und das ist so, weil die US-Geheimdienstler in der Lage wären, es zu bemerken, wenn ich Informationen an andere Regierungen weitergeben würde, die ich habe, die in meinem Kopf sind. Sie würden Änderungen erkennen in der Art der Informationen, die bei ihnen durchlaufen. Sie würden Quellen erlöschen sehen, die zuvor produktiv waren. Sie würden neue Quellen von Desinformation sehen auf den entsprechenden Kanälen, und das ist aber nicht geschehen.

[Es] sieht nur blöd aus, in Russland zu sein. Was Sie also als erstes verstehen müssen, ist, dass ich niemals nach Russland wollte. Ich habe hier nie aktiv Schutz gesucht. Das Außenministerium hat mich in Russland stranden lassen auf meiner Durchreise nach Lateinamerika. Aber ich würde sagen, wenn es meinem Ansehen schadet, dass ich hier bin, oder dort, oder irgendwo anders, dann ist das

egal, denn da geht es nicht um mich.

Meine Reputation ist egal ... Worum es geht, ist, wie die Leute über diese Dinge denken, egal, wie sie über mich denken. Worum es geht, das sind ihre Rechte und wie gegen sie verstoßen wird.

Ich habe nie einen Hehl daraus gemacht, dass ich die Mehrzahl der neuen Gesetze in Russland zur Internet-Zensur und Überwachung missbillige. Ich finde es absolut unangebracht für jede Regierung in jedem Land, sich in die Regulierung einer freien Presse einzuschalten.

Wir wollen nicht, dass Regierungsbeamte darüber entscheiden, was wir als Volk wissen dürfen oder nicht, was wir drucken dürfen oder nicht und wie wir leben dürfen oder nicht, und dazu stehe ich.

[Über Edward Lucas, der ihn einen „nützlichen Idioten“ nennt] Ja. Er ist verrückt. Er ist überhaupt nicht glaubwürdig ... Wir haben einen neuen Direktor der National Security Agency, Michael Rogers, der gerade angefangen hat. Der hat vollen Zugang zu allen geheimen Informationen. Der hat vollen Zugang zu allen Ermittlungen zu meiner Person.

Er hat öffentlich schlussgefolgert und gesagt, ich glaube sowohl der Presse als auch dem Kongress gegenüber, dass ich wahrscheinlich kein russischer Spion sei. Dafür gibt es überhaupt keine Anhaltspunkte.

Falls die Regierung das kleinste Indiz, den kleinsten Fetzen eines Beweises hätte, noch nicht einmal, dass ich für die russische Regierung arbeite, nur dass ich mit der Russischen Regierung in Kontakt wäre, dann wäre das bis Mittag auf der Titelseite der New York Times.

Es wird immer Verschwörungstheorien geben. Menschen werden immer abfällige Bemerkungen über andere Menschen machen, egal was diese auch tun, wenn sie an einem Ort sind, der einer unbeliebten Regierung untersteht. Ich verstehe das, weil ich selbst viele der politischen Entscheidungen der russischen Regierung missbillige. Aber es ist elementar unverantwortlich und journalistisch unehrlich, jemanden zu beschuldigen, für eine fremde Regierung zu arbeiten als Agent fremder Mächte, wenn es dafür überhaupt keinen Hinweis gibt, der diese These unterstützt. Und ich werde nicht auf jede einzelne Verschwörungstheorie antworten, die diese Spinner online hochkochen.

Schlussendlich ergibt es keinen Sinn. Wenn ich ein russischer Spion wäre, wäre ich von Hawaii nach Moskau geflogen. Warum hätte ich nach Hongkong gehen sollen? Warum ging er nach Indien [It. Lucas' Verschwörungstheorie]? Da gibt es eine ganze Geschichte, dass ich da unerlaubterweise hingegangen wäre. Das ist Schwachsinn, ich war offiziell zu Besuch, arbeitete in der US-Botschaft. Es ist nicht so, dass niemand wusste, dass ich dort war ... und der Sechs-Tage-Kurs danach – das war kein Sicherheits-Kurs, es war ein Programmierkurs, aber das tut nichts zur Sache.

### **Ob er alle Dokumente gelesen hat**

Ich habe meine eigene Entschiedenheit kundgetan darüber, wo Grenzen gezogen werden sollten, aber ich war der Ansicht, dass es wichtig war, dass Journalisten in die Lage versetzt würden, eine unabhängige Einschätzung vorzunehmen, welche Informationen von öffentlichem Interesse wären. Und das können sie nicht, wenn sie nicht Belege haben sowohl für Programme, [die] gerechtfertigt sind, als auch für Programme, [die] ungerechtfertigt [sind].

Wenn sie nur Informationen über Programme hätten, die eindeutig kriminell sind, könnte das ein irreführendes Bild über die Aktivitäten unserer Geheimdienste zeichnen und eine verzerrte Wahrnehmung, die sie alle als solche Bösewichte darstellt, die sie nicht sind. Sie sind gute Leute, die versuchen, schwierige Arbeit unter harten Bedingungen zu machen.

### **Warum so viele Dokumente**

Wenn Journalisten nur über Programme berichten, die Bürgerrechte oder Menschenrechte verletzen und offenbar nicht legitime, gerechtfertigte Programme sind, die uns helfen, sicher zu leben, die uns

in Kriegszeiten helfen, die kritische Infrastruktur schützen, und wieder solche, die zwar nicht in jedem Detail, aber im großen und ganzen ausreichend zeigen, dass sie guten Sinn und Zweck haben, dann würden wir von der Presse in die Irre geführt, und nicht von ihr unterstützt.

Mir ist klargeworden, dass ich nicht die Entscheidung treffen kann über die Eindrücke, die wir geben sollten. Das sollen Journalisten, unabhängig, ihre Institutionen oder Redakteure.

### **Die Pflicht für Geschäftsleute, andere digitale Wege zu gehen**

Ein unglücklicher Nebeneffekt der Entwicklung all dieser neuen Überwachungstechnologien ist, dass die journalistische Arbeit unermesslich schwieriger geworden ist als sie es in der Vergangenheit je war. Journalisten müssen besonders aufmerksam sein für jede Art Netzwerk-Übermittlung, jede Art Verbindung, jede Art Autokennzeichen-Lese-Einheit, an der sie auf dem Weg zu ihrem Treffpunkt vorbeifahren, jede Stelle, an der sie ihre Kreditkarte nutzen, jeden Ort, an den sie ihr Mobiltelefon mitnehmen, jeden E-Mail-Kontakt, den sie mit ihrer Quelle haben, denn der erste Kontakt, noch bevor die Verschlüsselung der Kommunikation aufgebaut ist, reicht schon aus, um alles zu verraten.

Egal wie vorsichtig Sie von diesem Zeitpunkt an sind, egal wie kenntnisreich Ihre Quelle, Journalisten müssen sicher sein, dass sie vom ersten bis zum letzten Moment der Beziehung zu ihrer Quelle überhaupt keine Fehler machen, sonst gefährden sie die Leute. Rechtsanwälte sind in der gleichen Lage. Und Ermittler. Und Ärzte.

Die Liste wächst konstant, und wir sind uns bis heute noch nicht einmal bewusst, dass es so eine Liste gibt. Ich würde sagen Rechtsanwälte, Ärzte, Ermittler, womöglich sogar Buchhalter. Jeder, der die Pflicht hat, die Privatsphäre seiner Klienten zu schützen, sieht sich einer neuen und herausfordernden Welt gegenüber, und wir brauchen neue Schulungen und neue berufliche Standards, um sicherzustellen, dass wir Mechanismen haben, die sicherstellen, dass der durchschnittliche Bürger unserer Gesellschaft in annehmbarem Maße Vertrauen in die Fähigkeiten aller Mitglieder dieser Berufe haben kann.

Wenn wir unserem Priester in einer Kirche etwas beichten, dann ist das geheim, aber ist das anders, wenn wir unserem Pastor eine private E-Mail schicken, in der wir ihm eine Lebenskrise beichten?

### **Seine Zukunft**

Ich habe sehr klar geäußert, dass ich gerne in die Vereinigten Staaten zurückkehren würde, und wenn die Möglichkeit eines fairen Gerichtsverfahrens gegeben wäre, dann könnte man das machen.

[Über seine Stelle als Rektor der Universität Glasgow?] Ich bin gerade in Gesprächen, um eine Methode zu finden, wie ich Rektoren-Sprechstunden abhalten kann, wie ich direkt mit den Studenten reden kann und sehen, was ich tun kann, wenn überhaupt, um zu helfen, deren Belange vorzubringen und sicherzustellen, dass sie von der Universität in vollem Maße angegangen werden. Leider hat es meine persönliche Situation, meine Sicherheitssituation, schwierig gemacht, direkt hinzufahren, aber wir versuchen, einen Weg zu finden, dass ich nicht wirklich an einen Bildschirm gefesselt bin, sondern hinreisen und direkt mit Leuten sprechen kann.

### **Ob er sich fit hält**

[Ich stehe] wahrscheinlich kurz vor dem Tod. Also ich esse nicht sehr viel. Ich halte mich an einen skurrilen Plan. Ich war früher sehr aktiv, aber gerade in der letzten Zeit hatte ich zu viel Arbeit, auf die ich mich konzentrieren musste.

### **Die Zukunft der Geheimdienste**

Ich bin übermäßig idealistisch, weil ich nicht sicher bin, ob es politische Reformen schaffen



werden, unsere Rechte in Hinsicht auf digitale Kommunikation in Zukunft effektiv zu schützen. Ich bin nicht sicher, dass die Regierung viel Lust dazu hat, diese Schutzmechanismen gesetzlich zu verankern. Ich denke, dass technische Systeme diese Lücke in weitem Maße füllen können, weil wir unsere Systeme und Werte in die Übertragungsprotokolle einbauen können, die wir nutzen, um [unsere] Beziehungen zu schützen.

Es wird wahrscheinlich vor dem Obersten Gericht landen ... und in Europa. Bevorstehende Gerichtsurteile werden, nach meiner Einschätzung, wahrscheinlich zusätzlichen Druck auf die Gesetzgeber ausüben, sinnvolle Reformen zu beschließen.

Wir müssen erkennen, dass Menschen ein individuelles Recht auf Privatsphäre haben, aber sie haben auch ein kollektives Recht auf Privatsphäre. Niemand sollte ihre Kommunikation beschlagnahmen und für unbestimmte Zeit speichern ohne jeden Verdacht oder Rechtfertigung, ohne jeden Verdacht, in irgendeine Art Kriminalität konkret verwickelt zu sein. Genauso, wie das bei jeder anderen Strafverfolgungsermittlung wäre.

Telekommunikationsanbieter müssen erkennen, dass die Rechte ihrer Kunden vor den Interessen irgendeines Staates kommen. Heute lautet ihre Standardantwort auf jede Kritik, die ihnen wegen der Mitwirkung an Abhörprogrammen entgegenschlägt, „wir halten uns an das Recht des Landes X, wenn wir in diesem Land tätig sind.“

Das mag stimmen, und mag auch rechtlich gesehen vernünftig sein, aber es heißt nicht, dass sie davon befreit sind, die Rechte ihrer Kunden zu verteidigen zu müssen. Wenn wir ihnen die intimsten Details unserer Leben anvertrauen, wenn wir ihnen unsere privaten Aufzeichnungen zur Verwahrung geben, müssen sie sicherstellen, dass sie ein angemessener Advokat für uns als Kunden sind, nicht nur gesetzlich, sondern sozial gesehen. Und das heißt, dass sie ihre Lobbymöglichkeiten einsetzen müssen, sie müssen ihre wirtschaftliche Schlagkraft nutzen, um die Regierungen zu zwingen, in welcher Rechtsprechung auch immer, verantwortlicher zu handeln was die Gewährleistung unserer öffentlichen Interessen angeht.