Eine Unterhaltung über Privatsphäre – Teil 5

Notiz: Diese Abschrift ist möglicherweise nicht 100% übertragbar

Nuala O'Connor: Lassen Sie uns das Gespräch über Terrorismus und die nationale Sicherheit wieder auf jeden von uns auf individueller und örtlicher Ebene zurückführen: Ein offensichtlich kritischer Fall, der gerade verhandelt wird, ist der Fall Apple vs. FBI. Ich bin übrigens unglaublich stolz, dass CDT als sachverständiger Berater hinzugezogen wurde, und ich nehme schon einmal vorweg, dass wir uns in diesem Fall klar auf der Seite der Verschlüsselungsbefürworter positionieren. Ich möchte die Runde zu ihren Gedanken dazu befragen und was dieser Fall für die individuellen Freiheiten und für die Privatsphäre des ständig online lebenden Einzelnen in der digitalen Welt bedeutet. Um die Frage zu verdeutlichen, zitiere ich den Chef-Technologen des CDT, Joe Lorenzo Hall: *Noch nie zuvor haben wir so viel von unserer Umwelt vernetzt und digitalisiert und noch nie zuvor hatten Durchschnittsbürger die Möglichkeit, ihre größten Geheimnisse dank immer sicherer werdender Smartphones so zu hüten, dass sogar den mächtigsten Regierungen der Zugriff darauf verwehrt bleibt. Müssen sich Gesellschaften, ja die Zivilisation im Allgemeinen, mit der Möglichkeit arrangieren, dass die einfachen Leute große Geheimnisse verbergen dürfen?*

Glenn Greewald: Also, ich beginne einfach mal mit ein paar Beobachtungen darüber, was bei dem FBI-Apple-Konflikt auf dem Spiel steht: Bevor ich Journalist wurde, war ich Anwalt, wie Sie zuvor anmerkten, und ich habe viele Fälle bearbeitet, in denen es um Redefreiheit ging. Und die Taktik der Regierung, wenn sie Redefreiheit untergraben wollte, war es, sich die unsympathischste Person zu holen und deren Recht auf freie Meinungsäußerung einzuschränken, damit ein Präzedenzfall geschaffen wird, der demonstriert, dass sie über diese Macht verfügt. Danach nehmen sie sich die sympathischeren Fälle vor. Aber dann ist es schon zu spät, weil die Person, mit der sie begonnen haben, so verhasst war, dass man ein solches Handeln durchgehen ließ. Und so kommt es dazu, dass Verteidiger der Redefreiheit wie die Amerikanische Bürgerrechtsvereinigung den Ku-Klux-Klan, Neonazis oder Fred Phelps verteidigen, also die am meisten verhassten Menschen der Gesellschaft, weil dies diejenigen sind, die am stärksten davon gefährdet sind, dass ihre Rechte in einer Weise eingeschränkt werden, in der später auch Ihre Rechte eingeschränkt werden. Genau das hat das FBI in diesem Fall getan: Sie fanden den unsympathischsten Fall. Wer würde jemals argumentieren, dass dem FBI der Zugriff auf das Telefon der Person verwehrt werden sollte, die die San-Bernadino-Morde beging? Natürlich niemand.

Und dennoch war das, was das FBI hier getan hat, reine Irreführung. Sie wollten einen Präzedenzfall schaffen, wodurch Apple und andere Unternehmen im Grunde genommen zur unfreiwilligen Arbeit für die Regierung gezwungen wären. Gezwungen, ihre eigenen Entwickler Hintertüren einbauen zu lassen, über die das FBI nicht nur auf das eine iPhone, sondern alle iPhones zugreifen könnte. Diese Hintertür könnte dann auch von vielen anderen Menschen genutzt werden. Und die größere philosophische Frage, die dadurch aufkam – und was Ihre Frage suggerierte – war die folgende: Sollte es überhaupt möglich sein, dass Bürger

in einer Art und Weise kommunizieren, die die Regierung physisch nicht einsehen kann? Genau das versucht die Regierung hier nämlich. Etwa so wie Football-Mannschaften oder Autovermietungen Mottos haben, hat auch die NSA ein Motto. Und ihr Motto, wie Ed vorhin gesagt hat, lautet *Wir sammeln alles*. Also nicht *Wir sammeln viel* oder *Wir sammeln die Gespräche von Terroristen*, nein sie wollen alles sammeln. Dies ist eine andere Art zu sagen, dass sie in der Lage sein möchten, die gesamte Kommunikation zwischen den Menschen auf diesem Planeten zu sammeln und zu speichern, was wiederum bedeutet, dass sie die Privatsphäre im digitalen Zeitalter beseitigen möchten. Und genau das steht im Fall Apple vs. FBI auf dem Spiel.

Die eine Sache, die mich immer fasziniert, ist, dass wir *1984* in der High School gelesen haben und es irgendwie fast ein Klischee geworden ist, es in Debatten über Privatsphäre zu nennen. Nun liegt meine High-School-Zeit, als ich *1984* gelesen habe, leider schon etwas zurück, und ich hatte mich übrigens falsch daran erinnert. Meiner Erinnerung zufolge war Orwells Warnung, dass wir unsere Freiheit dann verloren haben, wenn wir in einer Gesellschaft leben, in der wir ständig beobachtet werden. Wenn man also *1984* anspricht, sagen die Leute *Nein, unsere Gesellschaft ist anders. Es werden gar nicht alle überwacht*. *Es werden gar nicht alle Emails von allen Leuten gelesen und alle Gespräche abgehört.* Ich habe mir tatsächlich noch einmal *1984* besorgt und gelesen, als ich mit dieser Arbeit begann. Und die Welt, vor der Orwell warnte, war nicht eine, in der wir alle überwacht werden, sondern es war eine Welt, in der wir jederzeit beobachtet werden *könnten*.

Und Winston Smith, die Hauptfigur, erzählte von dem Monitor, der in der Wohnung stand und von dem man nie wusste, ob er eingeschaltet war und ob man überhaupt von jemandem beobachtet wurde oder nicht. Was man wusste, war, dass man zu jeder Zeit beobachtet werden könnte, weshalb man sich so verhalten musste, als würde man beobachtet. Das führte dazu, dass Menschen, die wussten, dass sie beobachtet wurden, sich gehorsam, gefällig und unterwürfig verhielten und ohne Widerspruch handelten. Das ist der Präzedenzfall, den die Regierung im Fall FBI-Apple zu schaffen versucht, und zwar, dass es nie einen Moment geben kann, in der Sie in der Lage sind, unterhalb des Überwachungsradars der Regierung der Vereinigten Staaten zu kommunizieren.

Noam Chomsky: Ich stimme den Ausführungen voll und ganz zu.

NO: Ed, wie sehen Sie das?

Edward Snowden: Nun, wenn wir darüber nachdenken, lautet die Kernfrage meiner Meinung nach *Wer benötigt Privatsphäre*? Weder sprechen wir von den Mächtigen, wenn es um die Frage geht, wer Geheimnisse haben darf und ob die Öffentlichkeit Geheimnisse haben darf. Noch ist Privatsphäre etwas Neues. Wie gesagt, die Flüchtigkeit menschlicher Kommunikation ist der Status Quo. Das war in der Geschichte der Menschheit schon immer der Fall. Denken Sie kurz nach: Wenn Sie Polizeibeamter wären, der einer Straftat nachgeht, würden Sie dann lieber über die heutigen Möglichkeiten der Kommunikationstechnologie verfügen, oder über die von vor über 200 Jahren, als es noch nicht einmal Telefonleitungen gab? Als es noch keine Aufzeichnungen zu Reisen gab, keine automatisierten Grenzkontrollen, keine Einkaufsdaten über Kreditkarten. Es ist sehr wichtig, zu verstehen, dass sich die Kontroverse in diesen Fällen nicht darum dreht, mit wem die Person gesprochen oder mit wem sie sich getroffen hat, weil alle diese Informationen in den Metadaten stecken.

Metadaten existieren nicht einfach im Telefon. Metadaten sind die tatsächlichen Aktivitätsaufzeichnungen. Sie wissen, wie das Telefonsystem funktioniert: Sie haben ein Gerät hier und Ihr Gesprächspartner in einiger Entfernung hat auch eins. Die Geräte kommunizieren nicht auf magische Art und Weise miteinander. Die Signale müssen über die Leitungen der Netzanbieter wandern, die nicht den Kunden gehören. All diese Aktivitäten werden aus nachvollziehbaren Gründen von den Unternehmen aufgezeichnet, allein schon aus Gründen der Abrechnung, Wartung, Messung und so weiter, im Sinne des Kundendienstes. Und um sicherzustellen, dass die Anrufe bezahlt werden. Diese Aufzeichnungen wurden dem FBI bereits zuvor ausgehändigt und standen ihm schon kurz nach Untersuchungsbeginn zur Verfügung. Also wissen sie schon, dass von den Telefonen keine Gespräche mit Terroristen im Ausland getätigt wurden und so weiter. Wäre das der Fall, wäre Magie im Spiel. Und wären Terroristen auch noch Magier, hätten wir noch größere Probleme.

Aber lassen Sie mich noch einmal auf die ursprüngliche Kernfrage zurückkommen: *Verdienen wir Privatsphäre? Ist die Welt bereit für eine Öffentlichkeit mit Privatsphäre?* Nochmal, es steckt bereits in unserer Sprache: Wir sprechen deswegen von *Privatleuten* und *öffentlichen Beamten*, weil die Regierung in fast allen Fällen so gut wie nichts über uns einfache Leute wissen sollte, wohingegen wir eigentlich fast alles über ihre Aktivitäten wissen sollten. Bedingt durch die steigende Zahl von Staatsgeheimnissen und die zunehmende Geheimhaltung in verschiedenen Bereichen erfahren wir jedoch immer weniger über die Regierung als dies früher der Fall war. Und dies entwickelt sich immer mehr zu einer Regierungskultur. Viele hohe Regierungsbeamte verwenden eigene Emailserver, um ihre Nachrichten vor öffentlichen Anfragen zu verbergen, die, wie Professor Chomsky es ausdrückte, das Gegengift dazu sind. OK, sie können kommunizieren wie sie wollen, solange wir Anfragen gemäß dem Freedom of Information Act einreichen können, solange diese Kommunikationen verlangt und letztendlich freigegeben werden können. Aber was passiert, wenn eine Kultur, in der niemand belangt werden kann, anfängt aufzublühen und innerhalb der Regierung Wurzeln schlägt? Und wir nichts darüber wissen, was sie tun? Wären sie in illegale oder unangemessene Handlungen verwickelt, würden wir es niemals erfahren, da sie ein System geschaffen haben, in dem sie das vor uns verbergen können. Gleichzeitig werden die Systeme zur ständigen globalen Überwachung weiter ausgebaut, nicht nur in den Vereinigten Staaten, sondern überall auf der Welt. So wird alles, was wir machen, gläsern, während die Aktivitäten der mächtigen, privilegierten Mitglieder der Gesellschaft immer undurchsichtiger werden.

NO: Um hier nochmal anzuknüpfen, Ed; viele von uns arbeiten in der Tech-Branche und dieser Fall dreht sich um die Fähigkeit jedes Einzelnen von uns, Technologie zum Schutze und zum Wohle einzusetzen. Können Sie den vielen Fragestellern eine Antwort darauf geben, welche Werkzeuge es gibt, die man nutzen könnte und sollte, bzw. was wir durch den Gebrauch von Technologie anstreben sollten? Die Frage richtet sich auch an die anderen.

ES: Das ist tatsächlich eine herausfordernde Fragestellung, die nicht so leicht beantwortet werden kann. Man kann nicht gänzlich unsichtbar durch das Web surfen. Es gibt keinen Unsichtbarkeitsumhang, keinen Zauberstab, der einen vor allem beschützen könnten. Insbesondere wenn man Sicherheitssoftware benutzt, die man nicht versteht, besteht die Möglichkeit, Fehler zu machen und Spuren zu hinterlassen. Dies ist einer der Gründe, weshalb die Behauptungen des FBI, sie würden völlig im Dunkeln tappen, lächerlich sind. Selbst wenn man ein verschlüsseltes Telefon und Verschlüsselungssoftware verwendet, gibt es immer noch die Metadaten und die privaten Aktivitätsaufzeichnungen, also Informationen, die als Nebenprodukt allein dadurch entstehen, dass man kommuniziert. Und auch wenn sie die Inhalte nicht lesen können, so sehen sie doch, dass etwas passiert ist. Und wenn ein US-Bürger oder irgendjemand unter Verdacht steht, etwas mit Terrorismus zu tun zu haben oder die Al-Qaeda-Hotline in Pakistan anzurufen; selbst wenn sie nicht wissen, worüber gesprochen wird, so wissen sie, dass es sich wahrscheinlich um eine Person von besonderem Interesse handelt. In Sachen Software sollten diejenigen, die interessiert und motiviert sind, das *Tor*-Projekt verwenden, etwa den *Tor* Browser, der als Sicherheitspaket heruntergeladen werden kann und normale Internetuser davor schützt, dass ihre Online-Aktivitäten von Wirtschaftsspionen, von Internetprovidern, von AT&T, Verizon, Comcast usw. ausgespäht werden. Dadurch erhalten sie keine Daten über Ihre Aktivitäten, die nicht zwingend erforderlich sind.

Es geht nicht nur um die Regierung. Es geht auch darum, etwas googeln zu können, ohne nach Hause zurückverfolgt zu werden. Wenn es um die Kommunikation zwischen Handygeräten geht, etwa SMS zu versenden, benutzen Sie die App *Signal*, die es für Android und iOS gibt. Sie schützt die Kommunikation über das Telefon, so dass zum Beispiel der Inhalt von SMS-Nachrichten oder möglicherweise intime oder private Fotos nicht von Ihrem Netzbetreiber eingesehen werden können. Und sie können dann auch nicht von NSA-Mitarbeitern herumgereicht werden, wie dies mit Nacktfotos üblich war, als ich dort gearbeitet habe. Es entsteht dieses Gegengewicht, in dem man dann hinterfragt *Nun, wenn es solche Tools gibt, bedeutet das, dass Terroristen ungeschoren davonkommen, weil wir nicht wissen, was sie vorhaben?* Das ist eben nicht der Fall. Wenn wir uns perfekte software-basierte Verschlüsselung in der Theorie ansehen, muss man zunächst das technologische Prinzip dahinter verstehen. Jedes Mal, wenn Sie Information chiffrieren, also wenn Sie etwas verschlüsseln, damit Ihre Gegner es nicht sehen können, bedeutet das nämlich, dass auch Sie selbst es nicht mehr sehen, bis Sie es wieder entschlüsseln und sichtbar machen. Normalerweise erfolgt dies durch die

Nutzung eines Passworts oder eines Schlüssels. Man kann sich dies folgendermaßen begreifbar machen: Wenn Sie Ihr Telefon ausschalten, auf den Tisch legen, irgendwo liegen lassen, egal, dann ist es verschlüsselt, nur noch Hintergrundrauschen, aber Sie können nichts mehr damit machen. Es ist dann nur noch ein Klotz im Regal.

Wenn Sie also wieder SMS lesen, jemanden anrufen, Fotos ansehen möchten, müssen Sie das Telefon wieder entsperren können. Wenn Sie das tun, gelangen Sie an den wunden Punkt, den Regierungen ausnutzen können und auch werden. Genauso wie kriminelle Gruppierungen und andere Organisationen es tun, indem sie einfach Ihr Gerät hacken können, so lange es eingeschaltet und unverschlüsselt ist, und den Schlüssel stehlen, der das Gerät entsperrt. Wenn Sie zum Beispiel an den Drogenmarkt auf der Silk Road denken, da gab es diese Person, die im Verdacht stand, ein krimineller Drahtzieher zu sein, der verschlüsselt kommunizierte. Man befürchtete, dass man nicht an die Beweise für seine Überführung kommen könnte – obwohl das in dem Fall nicht einmal notwendig war. Was soll man also machen, wenn es einem selbst nicht möglich ist, die Verschlüsselung zu knacken, und auch Apple nicht in der Lage oder willens ist, das Gerät für das FBI zu entsperren? Bedeutet das, dass die Regierung die Hände über dem Kopf zusammenschlägt und sagt *Das war's. Wir müssen dicht machen. Es gibt keine weiteren Untersuchungen zur Strafverfolgung*? Nun, im Falle dieser verdächtigen Person, die verschlüsselt kommunizierte, ihre Festplatten verschlüsselte und so weiter, wurde ein ganz einfacher Trick angewandt: Man wusste, dass die Person von öffentlichen Bibliotheken aus operierte. Nachdem sie also ihren Laptop geöffnet, das Gerät entschlüsselt und mit den vermeintlichen kriminellen Aktivitäten begonnen hatte, stellten sich zwei als Ehepaar getarnte FBI-Agenten zur Linken des Verdächtigen und machten eine Szene. Sie taten so, als hätten sie einen riesigen Streit. Als sich der Verdächtige nach links zu ihnen hindrehte, schnappte sich ein anderer FBI-Agent von rechts seinen Laptop, der ja nun entschlüsselt war, und rannte damit davon.

Verschlüsselung zu umgehen gehört für die NSA zum Tagesgeschäft. Ich habe das selbst miterlebt. Verschlüsselung ist eine Hürde, ja, aber die Öffentlichkeit will ihre Rechte geschützt sehen; nicht nur in den Vereinigten Staaten, sondern auch in Ländern, in denen man sich nicht immer auf seine Rechte stützen kann, wo es örtliche Polizeistellen gibt, die möglicherweise Journalisten ausspähen; es entsteht ein Weg, Menschenrechte dank neuer Mittel durchsetzen zu können, die verlässlich und international anwendbar sind. Wir dürfen das nicht für einen Anspruch opfern, effizienter an Informationen zu gelangen, den es so vor wenigen Jahren noch gar nicht gegeben hat.