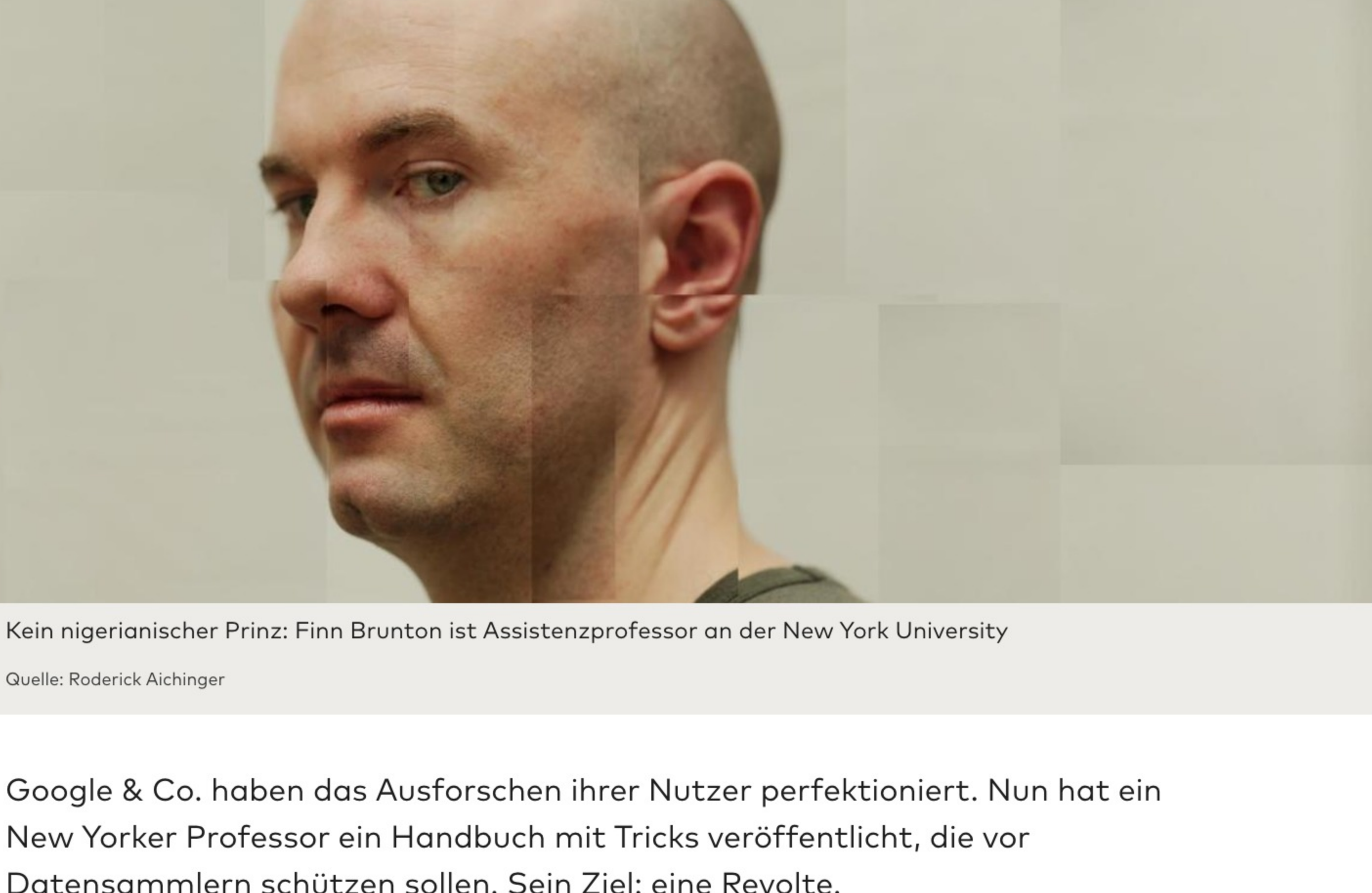


MEDIEN & TV AUSGEFORSCHTE NUTZER

So schlägt man Datensammler mit ihren eigenen Mitteln

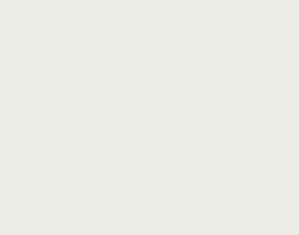
Von Hannes Stein | Veröffentlicht am 23.10.2015 | Lesedauer: 8 Minuten



Kein nigerianischer Prinz: Finn Brunton ist Assistenzprofessor an der New York University
Quelle: Roderick Aichinger

Google & Co. haben das Ausforschen ihrer Nutzer perfektioniert. Nun hat ein New Yorker Professor ein Handbuch mit Tricks veröffentlicht, die vor Datensammlern schützen sollen. Sein Ziel: eine Revolte.

0 Kommentare



Sieht so ein Rebell, ein Guerillakämpfer aus? Finn Brunton ist ein hochgewachsener, schlanker Mann mit militärisch kurzem Haarschnitt. Er trägt ein verwaschenes T-Shirt, dazu Trainingshosen und knallrote Turnschuhe, und wenn er lacht, könnte man denken, er sei gerade eben fünf Jahre alt geworden. Er lehrt als Professor an der New York University, sein Büro ist eng – es hat gerade genug Platz für ein Stehpult und Bücherregale. Die Aussicht geht auf eine rote Brandmauer aus Ziegeln. „Wie das Bühnenbild für ein Sartre-Stück, nicht wahr?“, sagt der junge Professor und grinst.

Finn Brunton kann sich noch genau an den Tag, an die Stunde erinnern, als die Rebellion begann. Er stand im Büro seiner Kollegin Helen Nissenbaum, die an der New York University Philosophie unterrichtet. Nissenbaum hatte gerade mit ein paar anderen Leuten zusammen eine App entwickelt, die „TrackMeNot“ heißt. Diese App soll es Google und Co. schwerer machen, das Suchverhalten von einzelnen Internetnutzern zu verfolgen, indem für jede Internetsuche Dutzende Phantomsuchen generiert werden: Das elektronische Rauschen, das auf diese Weise entsteht, soll die Stimme des Individuums übertönen.

Helen Nissenbaum ist – als Philosophin – die Fachfrau fürs Abstrakte, fürs große Ganze, für das Prinzip; sie interessiert sich schon seit vielen Jahren für die Frage, wie man seine Privatsphäre schützen kann. Finn Brunton ist kein Philosoph, sondern Historiker. Spezialgebiet: Geschichte der Wissenschaft und der Technologie. „Und als Helen von ihrer App erzählte, fiel mir sofort der Luftangriff der Royal Air Force auf Hamburg im Sommer 1943 ein.“

Von britischen Bomben lernen

Damals warfen die britischen Bomber pfundweise Stanniolpapierstreifen ab, die genau halb so breit waren wie die Wellenlänge des deutschen Radars. Plötzlich wurden die Radarschirme von Signalen überflutet. Die britischen Flugzeuge verschwanden hinter Millionen leuchtender Pünktchen. „Chaff“ nannte das britische Militär die Stanniolstreifen: Spreu. Die Spreu verbarg den Weizen, indem sie ihn unter sich begrub.

Dem System wurden keine Informationen vorenthalten, im Gegenteil: Es wurde mit Informationen förmlich zugeschüttet. Just diese Taktik, so meinen Finn Brunton und Helen Nissenbaum, sollten wir heute anwenden, um uns gegen schnüffelnde staatliche Behörden, aber auch gegen riesige Konzerne zu wehren, die unsere Daten sammeln und missbrauchen; wir sollten sie geschickt an ihren virtuellen Nasen herumführen.

Facebook darf User-Daten nicht in den USA speichern



Facebook darf künftig keine User-Daten mehr von seiner Zentrale in Dublin in die USA übermitteln – das urteilt der Europäische Gerichtshof. In den USA seien sie nicht angemessen geschützt. Geklagt hatte ein Student.
Quelle: Die Welt

„Obfuscation“ heißt diese alte und neue Taktik – ein Wort, das sich nur schwer ins Deutsche übersetzen lässt. Vernebelung, Trübung, Verdunkelung, Verschleierung. Nun haben Brunton und Nissenbaum ein Handbuch vorgelegt, das diese alt-neue Guerillataktik lehren soll: „Obfuscation. A User's Guide for Privacy and Protest“. Es ist schwarz eingebunden – also in der Farbe des politischen Anarchismus – und beginnt mit dem bescheidenen Satz: „Wir wollen mit diesem Buch eine Revolution auslösen.“

Der Craigslist-Räuber

Was vom ersten Augenblick an für Finn Brunton einnimmt, ist freilich gerade der Mangel an revolutionärer Verbissenheit. Er muss selbst lachen, wenn er weitere historische Beispiele für „obfuscation“ aufzählt. Da war etwa der „Craigslist-Räuber“, dem es bei einem Bankraub mithilfe von Pfefferspray gelang, 400.000 Dollar zu ergattern; dabei trug er Jeans, ein blaues Hemd, klobige Arbeitsschuhe und eine gelbe Sicherheitsweste. Sein Gesicht war hinter einer Schutzbrille und einer Mundmaske für Maler versteckt.

Naturgemäß suchte die Polizei also nach einem Mann, auf den diese Beschreibung passte. Allerdings trieben sich zur selben Zeit an die zwanzig Männer in Jeans mit blauen Hemden, mit gelben Sicherheitswesten, Schutzbrillen und Masken am Tatort herum. Sie meldeten sich auf eine – selbstverständlich fiktive – Stellenanzeige, die der Räuber vorsorglich auf der Online-Plattform Craigslist aufgegeben hatte, ehe er sich auf den Weg machte. Dann ist da die – leider erfundene, aber doch sehr schöne – Geschichte von den Dänen, die sich, angestiftet von ihrem König, allesamt gelbe Sterne angeheftet haben sollen, um die Juden zu verstecken. „Die Vernebelungstaktik, die wir lehren, erinnert sehr an Streiche, die Kinder den Erwachsenen spielen, an Schabernack, an Unfug aller Art“, sagt Finn Brunton. „Genau das gefällt mir.“

Zu den Ersten, die im Internet in großem Maßstab ihre Kunden ausforschten, gehörten zum Beispiel Supermärkte. Sie taten es mithilfe der Kundenkarten, die sie ausgaben. Sie ermittelten, wer bei ihnen wann was einkaufte, um besser auf die Wünsche der Kunden einzugehen. Dass das nicht immer ganz unschuldig war, zeigte sich 1999 bei einem Rechtsstreit in Los Angeles.

Werbebanner? Anklicken!

Nachdem ein Kunde in einem Supermarkt ausgerutscht und hingefallen war, drohten die Anwälte der Supermarktkette zu enthüllen, dass der Kunde früher Alkoholiker gewesen war. Nach einer Serie von ähnlichen Fällen begannen manche Einkäufer also, ihre Kundenkarten untereinander auszutauschen. Zuerst trafen sie sich noch persönlich, dann funktionierte der Tausch per Post, mittlerweile gibt es natürlich längst Internetbörsen, um Kundenkarten auszutauschen und die Supermarktketten mit virtueller Spreu einzudecken.

Weitere Guerillatricks: „FaceCloak“ ist eine Internet-App, die alle persönlichen Daten, die normalerweise auf Facebook gespeichert werden, an anderer Stelle lagert, wo sie nur von ausgesuchten Freunden eingesehen werden können. „AdNauseam“ ist ein Programm, das heimlich und im Hintergrund auf alle Werbebanner klickt, die sich beim Browsen auftun – wirklich auf alle, sodass die gesammelten Daten dann in der Summe rein gar nichts mehr ergeben.

Finn Brunton ist kein Wahnsinniger. Er verwechselt das FBI nicht mit der Stasi, und er weiß auch ohne Nachhilfe ganz gut, dass es sich bei den Vereinigten Staaten nicht um eine faschistische Diktatur handelt. „Die Diskussionen bei meinen Freunden aus dem Milieu der libertären Hacker, für das ich übrigens sehr viel Respekt habe, drehen sich um etwas anderes“, sagt er. „Es geht ihnen um Minderheiten, um Leute, die verletzlich sind. Da hat dieses Land leider eine fürchterliche Vergangenheit.“

SIE MÜSSEN BEDENKEN, DASS DATEN, DIE EINMAL GESAMMELT WURDEN, DA SIND UND NICHT MEHR GELÖSCHT WERDEN KÖNNEN

FINN BRUNTON

Wenn man an die Behandlung der Schwarzen, der amerikanischen Ureinwohner oder der Amerikaner japanischer Abstammung denkt, die im Zweiten Weltkrieg unter Franklin D. Roosevelt in den Rocky Mountains in Barackenlager gepfercht wurden, muss man dem Historiker recht geben. „Sie müssen bedenken, dass Daten, die einmal gesammelt wurden, da sind und nicht mehr gelöscht werden können“, sagt Finn Brunton. „Wir wissen nicht, was in Zukunft mit ihnen angestellt werden wird.“ Die Kosten, um jemanden auszuspionieren, seien dramatisch gesunken, von mehreren Tausend Dollar auf ein paar lumpige Cent. In der guten, alten Zeit musste man noch extra einen Agenten losschicken, der das Geschäft des Spionierens besorgte. Heute stellen die meisten von uns ihre Daten freiwillig zur Verfügung. Die berufsmäßigen Sammler müssen nur ihre Netze auswerfen, das ist alles.

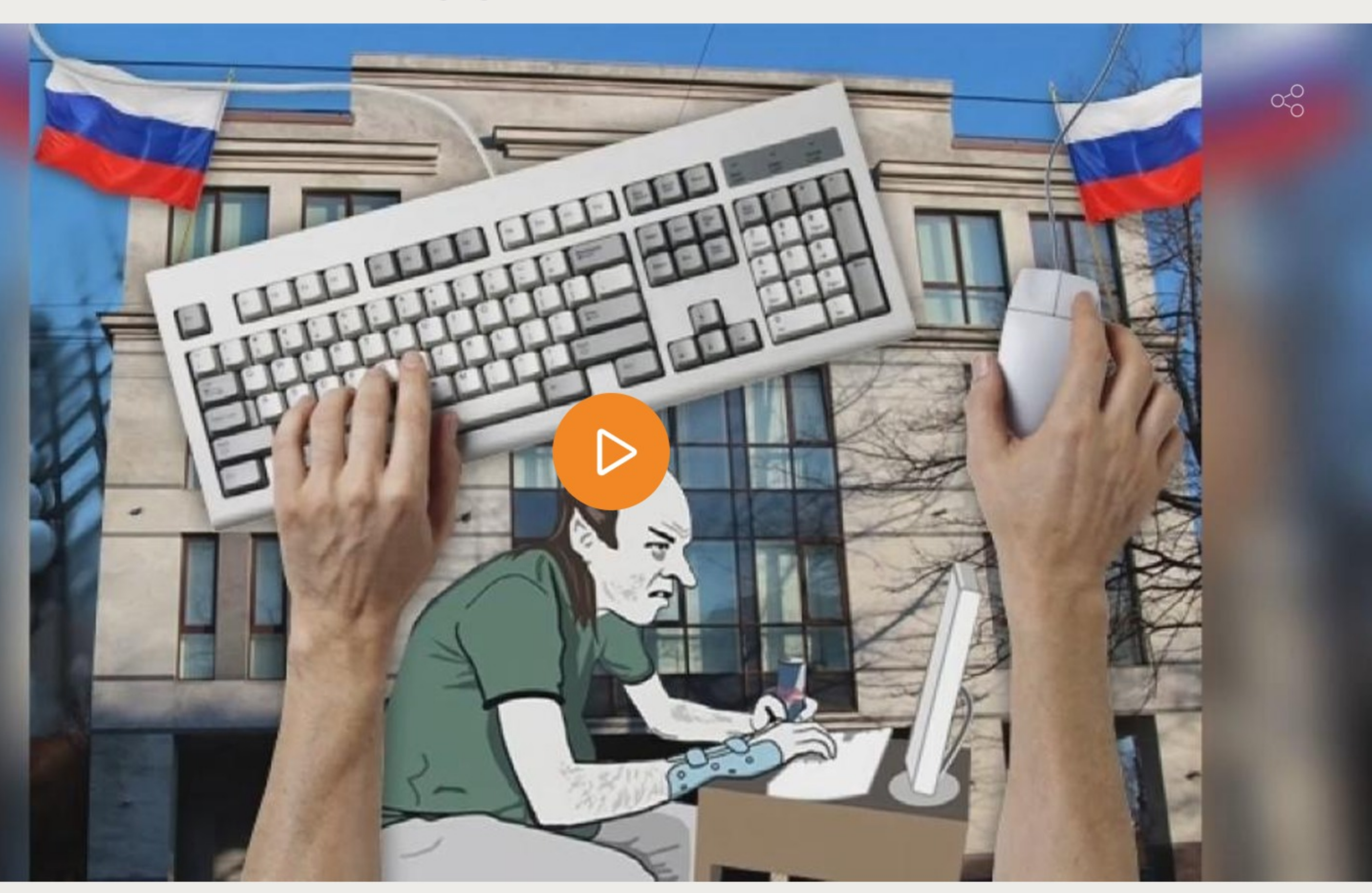
Naturgemäß war Finn Brunton als Kind das, was man einen „Nerd“ nennt – ein Sonderling, ein Außenseiter, ein Intelligenzbolzen mit abgelegenen Interessen. Später, als junger Mann, verdiente er Geld, indem er Kulissen für Hollywoodfilme anfertigte, vor allem Möbel – „es waren aber nur wirklich schlechte Filme darunter“. Dann wurde er Wissenschaftshistoriker und lehrte im fernen Schottland, in Aberdeen. Dabei fing er an, sich für die Geschichte des Spam zu interessieren.

„Spam“ – das ist der Müll, der Abfall, der jeden Tag unsere elektronischen Briefkästen verstopft. Finn Brunton beschloss, die Sichtweise umzudrehen: Er begriff Spam nicht als Müll, sondern als das wichtigste Produkt, das im und vom Internet produziert wird. Dabei stellte er fest, dass Spam das Internet tatsächlich definiert und geprägt hat – als Wettlauf zwischen Spam-Herstellern und jenen, die versuchten, immer raffiniertere Spam-Filter zu entwerfen.

Nigerianische Prinzen im 18. Jahrhundert

Außerdem fand Brunton heraus, dass es manche Formen des Spam schon ziemlich lange gibt. Wir alle kennen die verzweifelt-poetischen E-Mails von vermeintlichen nigerianischen Prinzen, die uns in schlechter Rechtschreibung und mit schiefer Grammatik anflehen, ihnen unsere Kontonummern zu verraten, damit sie dort ihre Millionen parken können, die von irgendwelchen Finsterlingen bedroht seien; wir würden von dem Kuchen auch ein Stück abbekommen. Nach exakt diesem Schema funktionierte bereits eine Form des Betrugs, die im 18. Jahrhundert aufkam, im Gefolge der Französischen Revolution – nur waren es damals völlig fiktive Adelige, die um den Beistand der Leichtgläubigen baten.

Russische „Trolle“ hetzen gegen Kanzlerin Merkel



Sogenannte „Trolle“ müllen die Kommentarspalten von Internetseiten mit Propaganda oder Beschimpfungen zu. Selbst die sozialen Netzwerke von Kanzlerin Merkel sind nicht mehr sicher.
Quelle: N24

Es ist vor allem dieses historische Bewusstsein, das die Lektüre von „Obfuscation“ zu einem Vergnügen macht. Und natürlich ist Finn Brunton nicht naiv. Er weiß, dass die Guerilla-Taktik der Verschleierung eine Waffe nicht nur in den Händen der Wehrlosen, sondern auch der Mächtigen sein kann. Wladimir Putin etwa beschäftigt eine ganze Armee von Trollen, die ihre Kommentare in den Spalten westlicher Medien absondern. „Es war in den vergangenen Monaten hochinteressant, das zu studieren“, sagt Brunton. „Am interessantesten ist, dass es Putin überhaupt nicht mehr darum geht, eine bestimmte Version der Wahrheit durchzusetzen. Es geht nur darum, durch die bloße Masse von Kommentaren Verwirrung zu stiften.“ Als begeisteter Leser von Stanislaw Lems utopischen Romanen kann Finn Brunton sich übrigens sehr gut vorstellen, dass es zu einer Art kaltem Krieg kommen könnte, in dem sich Datensammler hier und Verwirrungstifter dort immer kompliziertere Apps ausdenken.

Trotzdem strahlt Brunton, wie er da in seinem verwaschenen T-Shirt mit seinen knallroten Turnschuhen am Pult steht, einen lausbüschigen Optimismus mit seinen praktiziert er denn auch selbst, was er predigt? Verwischt er im Internet seine Spuren? „Aber klar doch!“, sagt er. „Ich habe den Ehrgeiz, meinem Lebenslauf mit der Zeit immer mehr Lügen anzufügen. Versprochen!“