

# Ich ist ein anderer

*Im Ausspionieren ihrer Bürger sind die USA weit vorn. Unterwegs mit der »Electronic Frontier Foundation«, die gegen die Auflösung der Privatsphäre kämpft*

Text: Peter Kreysler

Illustration: Thomas Armbrorst

Es ist eine seltsame Gruppe, die da zum Sightseeing durch San Francisco aufbricht und die sich weniger für die Golden Gate Bridge oder das pyramidenförmige Transamerica-Building interessiert, sondern nach dem Unsichtbaren Ausschau hält – nach Sensoren, die versteckt im Alltag vor sich hinarbeiten und Daten sammeln. Wahrscheinlich seien in diesem Moment bereits drei Videokameras auf uns gerichtet, sagt Seth Schoen, der wie die anderen zur Electronic Frontier Foundation (EFF) gehört, einer kleinen, aber einflussreichen Organisation, die den Schutz der Privatsphäre von US-Bürgern verbessern will. Denn im kommerziellen Bereich kennen die USA nur einen kümmerlichen Datenschutzzustand: Computer und Telefone werden kontrolliert, der Einkaufsbummel durch die Stadt aufgezeichnet. Daher hat Seth Schoen nicht mal mehr ein Handy.

Moderne Kommunikationsgeräte wie Handys, Laptops und Navigationssysteme senden ständig Informationen aus. So kann jeder US-Bürger mit der entsprechenden Software im Internet den Standort eines mit GPS ausgestatteten Handys herausfinden und dessen Bewegungen kontrollieren. Schön für besorgte Eltern, die ihre Kids so in der Diskothek orten.

Unten in der U-Bahn weist Seth Schoen auf die neuen Fahrscheinautomaten hin,

bei denen man ausschließlich mit Kreditkarte bezahlen kann. Dafür erhält man eine persönliche Plastikkarte, die mit einem Chip ausgestattet ist, der von einfachen Scannern gelesen werden kann und der bereits in vielen Pässen und Waren integriert ist. Bei jeder Fahrt erkennt der neue Automat, wer, wann, wo und wie lange die U-Bahn benutzt hat. So entstehen Bewegungsprofile, die im Datenzentrum gespeichert und eventuell auch an andere Firmen und staatliche Behörden weitergegeben werden können.

Schleichend ist die elektronische Beobachtung dank vieler kleiner Hilfsmittel in den US-Alltag getreten. Handys geben im angeschalteten Zustand ihren Standort permanent an die Telefongesellschaften weiter, die nicht gerade umsichtig mit den anvertrauten Daten ihrer Kunden umgehen. Seth Schoen und seine Kollegen von der EFF haben AT&T, den mit über 110 Milliarden Dollar Jahresumsatz größten Telefonkonzern der Welt, verklagt, weil das Unternehmen zugelassen hatte, dass die US-Regierung mithilfe des Geheimdienstes National Security Agency (NSA) die Telefonleitungen anzapft. Ein AT&T-Mitarbeiter berichtete der EFF sogar, dass die NSA eigens einen geheimen Raum eingerichtet habe, durch den der gesamte Telefon- und E-Mail-Verkehr von San Francisco laufe.

## *Ein Dutzend geheimer Datenräume im ganzen Land*

San Francisco ist kein Einzelfall: Ein Dutzend dieser geheimen Datenräume soll es im ganzen Land geben, um Millionen von Telefonaten und E-Mails elektronisch zu speichern und abzuhören. Vor ein paar Jahren war das noch illegal, ein Gesetz schrieb für jede Maßnahme einen Gerichtsbeschluss vor. Nach den Terroranschlägen vom 11. September 2001 wurden die Datenschutzgesetze Zug um Zug abgeschafft, bis schließlich im Juli 2008 selbst die massenhafte Speicherung privater Mails und Anrufe durch einen Zusatz zum »Protect America Act« legalisiert wurde. So ist der Schutz vor möglichen Attentätern nun vor den Schutz der Privatsphäre getreten. Die großen Telefongesellschaften wurden sogar



rückwirkend von jeglichem Fehlverhalten freigesprochen und die Klage der EFF abgewiesen. »In Zukunft« so fürchtet Kevin Bankstone, der Rechtsanwalt der Gruppe, »werden die Telefongesellschaften noch unbedachter mit der Regierung und den Behörden zusammenarbeiten.«

Nicht nur die Regierung, auch Privatfirmen haben zunehmend Interesse an elektronischen Daten, um zu erfahren, was die Menschen kaufen und wie sie leben. Der Handel mit der Identität der Verbraucher ist eine Boom-Branche. Einer der größten kommerziellen Datenhändler der Welt ist LexisNexis in Dayton, Ohio, dessen Kunden Informationen blitzschnell abfragen können – vor allem Rechtswissen und Daten aus der Wirtschaft, aber auch Angaben über Privatpersonen. Folgt man dem technischen Direktor, Allan D. McLaughlin, durch etliche Sicherheits-schleusen, gelangt man in das Allerheiligste des Konzerns: das Datenzentrum.



zu einem gigantischen Wissensschatz: 1,5 Petabyte (also 1,5 Millionen Gigabyte) stünden zur Verfügung, erzählt McLaughlin stolz. Aus dieser digitalen Weltbücherei ließe sich vieles erfahren, es sei nur eine Frage des Geldes.

Vor drei Jahren gelang es einigen Hackern, die LexisNexis-Rechner mit gestohlenen Passwörtern zu knacken und über 30 000 Adressen und personenbezogene Daten zu stehlen, die den Betrügern Zugang zu Bankkonten und Kreditkarten ermöglichten. Ein ungeheurer Datendiebstahl, der selbst den US-amerikanischen Kongress alarmierte. Verbessert hat sich dadurch kaum etwas: Auch andere großen Datenkonzerne wie Axiom oder Choicepoint geraten immer wieder negativ in die Schlagzeilen, weil der Zugang zu sensiblen Privatinformationen fast jedem offensteht. Um an die Datenbank von Choicepoint zu kommen, reicht es, einen Fragebogen auszufüllen und ein sogenanntes »legitimiertes Geschäftsinteresse« nachzuweisen. Für ein paar Betrüger aus Los Angeles ein Kinderspiel: Sie füllten den Fragebogen aus, gaben »Schuldeneintreibung« als Gewerbe an und erhielten ohne Probleme freien Zugang zum Rechenzentrum. Mithilfe einer Internetverbindung luden sie die Daten von rund 150 000 Bürgern herunter und bestellten u. a. Kreditkarten.

Die Automatisierung hat die Gänge leer gefegt, man sieht nur Computer, soweit das Auge reicht. Die Daten, die Lexis Nexis aus der ganzen Welt empfängt, werden vollautomatisch von Maschinen bearbeitet. Automatisierte Analysewerkzeuge, die mit elektronischen Analogien und Wörterbüchern arbeiten, versorgen die computerisierten Datenspeicher und Suchmaschinen mit den aufbereiteten Informationen. Innerhalb von fünf Sekunden haben die Kunden so Zugang

Nicht nur Musik oder Computerprogramme – auch Menschen werden heute raubkopiert, wenn sie nicht geschützt sind. Laut einer Studie des FBI ist Identitätsdiebstahl in den USA das Verbrechen mit einer großen Wachstumsrate – und es gibt sogar noch eine Steigerung: das sogenannte Identitäts-Klonen: Dabei übernimmt jemand komplett die Identität einer Person und begeht unter deren Namen Straftaten. Bronty Kelly ist genau

das passiert: Vor über zehn Jahren wurde seine Brieftasche gestohlen, mit Führerschein und Militärausweis, auf dem seine Sozialversicherungsnummer stand. Von den weitreichenden Konsequenzen merkte er erst einmal nichts – bis er erfolglos einen Job suchte, nachdem er seinen Militärdienst in San Diego geleistet hatte.

*Er fiel bei jeder Bewerbung durch – kein Wunder*

In den USA führen alle Arbeitgeber elektronische Backgroundchecks mithilfe der großen Datenbanken durch. Mit einem Mausklick und einer Internetverbindung zu einem der großen Datenhändler liegt den Unternehmen so die gesamte Lebens- und Arbeitsbiografie offen. Da die Arbeitgeber nicht verpflichtet sind, den Bewerbern mitzuteilen, warum sie jemanden ablehnen, hatte Bronty Kelly lange Zeit keine Ahnung, warum er ständig abgelehnt wurde. Erst die Recherchen eines TV-Reporters brachten Klarheit. »Auf meinen Namen waren etliche Haftbefehle ausgestellt. Kellys Datenklon hatte sich kurzerhand bei jeder Verhaftung mit einem Führerschein und einer Sozialversicherungskarte ausgewiesen, die auf Kellys Namen ausgestellt waren.

Aber auch mit einer neuen Sozialversicherungsnummer fiel Kelly seltsamerweise bei jeder Bewerbung durch. Diesmal stolperten die Computer darüber, dass Kelly keine Eintragungen über Arbeit und Kreditkartennutzung hatte. Dass ein 40-jähriger kaum Datenspuren hinterlassen hatte, seine Konsumgewohnheiten nicht erfasst waren. Von dieser Spezies gibt es in den USA nur noch wenige Exemplare: Die meisten davon sind Exmafiosi, die sich im Zeugnenschutzprogramm befinden.

----- Amarillo, Texas, 1 p.m. -----

## ON THE ROAD, TAG 4



Mein Rucksack ist weg. Ein Gepäckjunge sagte mir, er sei auf dem Weg versehentlich ausgeladen worden und werde jetzt für ein paar Dollar auf

einer Auktion im Hinterland verscherbelt. (Lies auf Seite 42: Wie blöd Las Vegas ist)

Distanz bis zum Ziel: 1814 Kilometer

Letzte Nacht geschlafen: 2 Stunden

Gegessen: Steak beim Mexikaner

Andere Deutsche: 0

Besondere Vorkommnisse: 30 Dollar von einer betrunkenen

Frau geschenkt bekommen, die ich an Obdachlose

verschenken soll

