Laura Fichtner

FIfF-Studienpreis 2015
3. Preis

Techno-Politics as Network(ed) Struggles

The Politics of Internet Surveillance

An dieser Stelle möchte ich mich gerne ganz herzlich beim FIfF für die Verleihung des Studienpreises bedanken, und ebenso für die Einladung zur Preisverleihung im Rahmen der FIfF-Konferenz, die im November 2015 in Erlangen stattfand. Mein besonderer Dank gilt Sylvia Johnigk und Kai Nothdurft, die mich auf die Bewerbung zum Preis aufmerksam gemacht haben, sowie Professorin Britta Schinzel für ihre Laudatio meiner Arbeit. Des Weiteren bedanke ich mich sehr herzlich bei meinen Professoren Michael Nagenborg und Peter-Paul Verbeek von der Universität Twente, ohne deren intensive Betreuung und Input diese Masterarbeit nicht möglich gewesen wäre!

Einleitung

Wie kann staatliche Überwachung im Sinne der von Edward Snowden enthüllten Dokumente als politisches Mittel verstanden werden? In diesem Artikel möchte ich gerne einen Ansatz zur Beantwortung dieser Frage vorstellen, an welchem ich im Rahmen meiner Masterarbeit in *Philosophy of Science, Technology and Society* an der Universität Twente in den Niederlanden gearbeitet habe. Während dieses Essay die wesentlichen Punkte der Arbeit herausstellt und in den größeren Kontext setzt, kann die Vollversion der Arbeit unter *http://essay.utwente.nl/66530/* heruntergeladen werden.

Im Folgenden setze ich die Arbeit zuerst in Bezug zu den den FIfF-Leser.innen vermutlich durchaus schon bekannten Snowden-Enthüllungen, durch welche wir tieferen Einblick in das System staatlicher (Internet-)Überwachung gewinnen konnten. Anschließend diskutiere ich die Frage, was Infrastruktur mit Politik zu tun hat und stelle die techno-politischen Dimensionen der Internet-Infrastruktur dar. Innerhalb dieses Rahmens fasse ich anschließend meine Analyse der NSA-Überwachungsmethoden und deren Implikationen zusammen. Abschließend gebe ich meine kurze Antwort auf die Frage, ob staatliche Überwachung tatsächlich nur eine Frage von Privatsphäre und Sicherheit ist.

Die Snowden-Enthüllungen und deren Konsequenzen

Im Juni 2013 trat Edward Snowden in Hongkong zum ersten Mal vor die Kamera von Laura Poitras und stellte sich den Fragen der Journalisten Glenn Greenwald und Ewen MacAskill.[1] Was daraufhin folgte, war wohl eines der größten Medienereignisse in der Geschichte des Whistleblowings. Die detaillierten Einsichten in die Methoden eines internationalen Netzwerkes staatlicher Überwachungsorgane, die wir dank Edward Snowden gewinnen konnten, haben wohl unser Verhältnis zum Internet und unser Verständnis von Online-Privatsphäre entscheidend mitgeprägt. Obwohl bereits seit längerer Zeit bekannt war, dass die NSA in großem Stile überwacht, schlugen die Veröffentlichungen weitreichende Wellen und prägten gar eine ganze Epoche der „Post-Snowden-Ära", gaben Anlass zu Büchern und zahlreichen Panels sowie Talkrunden in Politik, Fernsehen, Universitäten und in der Technikbranche selbst. Insbesondere in Amerika führten die „Snowden disclosures" zu Unmut, da klar wurde, dass die amerikanischen Überwachungsorgane in ihrem präventiven Generalverdacht durchaus keinen großen Unterschied zwischen amerikanischen und nicht-amerikanischen Staatsbürger.

Laura Fichtner, Foto: Kai Nothdurft

innen machen, was letztendlich nur noch die knallharten Verfechter.innen der „Nothing-to-Hide, Nothing-to-Fear"-Doktrin kalt lassen konnte.

Aber was der internationalen Internetcommunity, die sich ja schon lange mit den technischen und gesellschaftlichen Fragen des Datenschutzes, der IT-Sicherheit, Privatsphäre und, zumindest in jüngerer Vergangenheit, der *Big Data* beschäftigt, einen besonderen Dienst erwies, war der Umfang der gewonnenen Einsichten sowie die Details, die aus den klassifizierten schriftlichen Dokumenten entnommen werden können und somit etwaigen politischen, ethischen oder technischen Forderungen Nachdruck verleihen konnten. Die gewonnenen Einblicke ermöglichten dann letztendlich auch für mich das Verfassen einer technisch und empirisch wohlinformierten *Techno-Politics as Network(ed) Struggles*[2]. In der Arbeit konzeptualisierte ich den Begriff der *techno-politics*, welcher eine Form der Politik beschreibt, die durch technische Kanäle ausgeführt wird. In diesen techno-politics verschmelzen das Technische und das Politische miteinander – sie beschreiben die Technisierung des Politischen und die Politisierung des Technischen: technische Herausforderungen werden zum Gegenstand politischer Ambitionen, und politische Ambitionen werden durch technische Mittel verfolgt.

Was hat Infrastruktur mit Politik zu tun?

Die Frage, die ich mir in meiner Arbeit stellte, war nicht die Frage, inwiefern die NSA-Überwachung rechtliche Grenzen überschreitet oder gegen Verfassungen verstößt, oder etwa inwieweit die Gewährung innerer Sicherheit gegen die Bewahrung der Privat-

sphäre abzuwägen sei. Vielmehr konzentrierte ich mich darauf, zu verstehen, wie sich die ausgeprägte Form der NSA-Überwachung, oder allgemeiner jedwede Form der zentralisierten Internet-Überwachung, durch ein Macht- und/oder Marktmonopol, auswirkt auf die politischen Strukturen der globalen Öffentlichkeit, die durch das Internet und seine Infrastruktur entstanden ist.

In meiner Arbeit baute ich auf einen Begriff des Politischen und Demokratischen auf, der vom Amerikaner und Demokratie-Idealisten John Dewey bereits in den 20er-Jahren des letzten Jahrhunderts entwickelt worden ist.[3] Für Dewey besteht die Aufgabe der Politik vor allem darin, die Interaktionen und den Austausch innerhalb einer Gesellschaft im Sinne aller Beteiligten verlässlich und vernünftig zu regulieren. Er sieht diese Aufgabe dann in einer Demokratie erfüllt von den demokratisch gewählten Repräsentanten der *public*, der politischen Gemeinschaft oder Öffentlichkeit.[4] Diese sollen gemäß ihrer Aufgabe im Interesse dieser Öffentlichkeit handeln und ihre Entscheidungen auf Grundlage eines Austausches mit den Bürgern im öffentlichen und rationalen Diskurs fällen. Für Dewey ist eine solche politische Gemeinschaft oder Öffentlichkeit allerdings kein statisches Gebilde, und sie ist schon gar nicht festgelegt durch die Grenzen unserer heutigen Staatenlandschaft. Stattdessen wird sie vielmehr bestimmt durch eben jenen gesellschaftlichen Austausch, den Politik zu regulieren sucht.[5]

Auf Grundlage dieses Politikverständnisses werden technische Infrastrukturen dann zum zentralen Bestandteil der Politik und politischer Bestrebungen, da sie neue Kanäle eröffnen, über welche der gesellschaftliche Austausch verschiedener Güter oder Informationen erfolgen kann. Das Internet zum Bespiel schafft solche neuen Kanäle, und konsequenterweise entsteht dann eine neue politische Öffentlichkeit, die aus all jenen besteht, welche über diese Kanäle interagieren und so ein Interesse an deren Regulierung haben. So wird die Infrastruktur dann zum Gegenstand politischer Bestrebungen.

Im Zusammenhang hierzu steht die Arbeit des Medientheoretikers Alexander Galloway, der es sich in *Protocol* einmal zur Aufgabe gemacht hat, die Kontrollstrukturen, die sich in der ansonsten transparenten Internet-Infrastruktur verbergen, sichtbar zu machen.[6] Er unterscheidet hier zentralisierte, dezentralisierte und verteilte Netzwerkstrukturen, die sich vor allem darin unterscheiden, wie sie 1. die Flüsse, die durch das Netzwerk und seine Infrastruktur ermöglicht werden, gestalten, 2. auf welche Weise Kontrollmechanismen und -instanzen implementiert werden und 3. wie sie die Machtverhältnisse zwischen den verschiedenen Netzwerkteilnehmer.innen gestalten.[7]

In einem zentralisierten Netzwerk, so Galloway, gibt es eine kontrollierende Instanz, einen Mittelpunkt, an den alle anderen anknüpfen. Dieser, als einziger Hauptknotenpunkt, hat das Recht, anderen den Zugang zum Netzwerk zu verwehren, und muss immer um Erlaubnis gefragt werden: dieser Mittelpunkt übersieht alle Flüsse im Netzwerk und kann Kommunikation zwischen anderen Netzwerkteilnehmern herbeiführen oder unterbinden.

Ein dezentralisiertes Netzwerk ist dann die Verbindung mehrerer zentralisierter Netzwerke: hier gibt es einige Hauptknotenpunkte, die sich auf einer hierarchischen Ebene befinden und miteinander gleichberechtigt agieren können. Diese haben allerdings ihre eigenen untergeordneten Instanzen, über welche sie wie im zentralisierten Netzwerk verfügen können. Als anschauliches Beispiel könnte man hier ans internationale Flugsystem denken. Auch dort gibt es einige Hauptknotenpunkte, beispielsweise New York, Frankfurt oder Amsterdam, die alle gleichberechtigte Verbindungen zueinander pflegen, allerdings die Kontrolle über provinziale Ziele haben – wer in eine kleine Stadt in der Provinz in den USA möchte, ist immer darauf angewiesen, erst einen großen Knotenpunkt anzusteuern.

Und dann gibt es letztendlich noch das anarchistische, das verteilte, Netzwerk, in dem man keinerlei Hierarchien zwischen verschiedenen Netzwerkteilnehmern entdecken kann. Stattdessen befinden sich alle auf gleicher Ebene und jeder Knoten kann beliebig mit jedem anderen Knoten im Netzwerk interagieren. In einem solchen Netzwerk gewinnen die Protokolle, also die allgemein gültigen Regeln, nach welchen man am Netzwerk teilnehmen und mit anderen interagieren kann, größte Bedeutung, da sie als allgemein verbindliche Standards die Funktionsfähigkeit der Netzwerkstruktur garantieren.

Was können uns nun aber die konzeptionellen Arbeiten von Dewey und Galloway über den NSA-Skandal und die politischen und sozialen Implikationen von Massenüberwachung durch staatliche Geheimdienste sagen? Meiner Meinung nach liegt hier eine große Bereicherung vor allem auf der strukturellen Ebene. Wenn wir diese konzeptuellen Arbeiten in Verbindung setzen mit einer konkreten empirischen Analyse, wie Überwachungstechnologien auf infrastruktureller Ebene operieren und technische Realitäten schaffen, können wir den NSA-Skandal nicht nur als Bestrebung, Individuen und deren Gedanken und Taten so detailliert wie möglich zu überwachen, verstehen, sondern als politisches Mittel, das durch Technik sozio-politische Strukturen zu schaffen und Machtpositionen zu erschaffen versucht.

Wenn wir uns nun weiter unten anschauen, wie die NSA-Überwachung tatsächlich funktioniert, sehen wir, dass sie erstens auf

Laura Fichtner

Laura Fichtner hat Elektro- und Informationstechnik in Karlsruhe und Philosophy of Science, Technology and Society in den Niederlanden studiert. Die hier vorgestellte Arbeit ist im Rahmen ihres Masters entstanden. Zurzeit forscht Laura zum Thema Überwachung und Cybersecurity im Internet der Dinge.
Das nebenstehende Logo der Arbeit stammt von Eva Müller.

der Grundlage eines geopolitischen Machtvorteils operiert und diesen zweitens durch das von ihr angelegte Schattennetzwerk und zum Trotz anderweitiger Bestrebungen der *Open Source Community* weiter auszubauen versucht.

Doch die Idee, die Ursprung und Entstehung des Internets letztendlich geleitet hat, war eigentlich die Idee einer dezentralen Infrastruktur, die in ihrer Funktionsweise einem zentralisierten Angriff trotzen könnte. Diese Idee trieb *World-Wide-Web*-Begründer Berners-Lee dann weiter vorwärts.[8] Die Entwicklung der *Hypertext Markup Language* (HTML) und der Internetprotokolle transformierten das Netzwerk der Netzwerke dann vollends zu einem verteilten Netzwerk, das jedem Teilnehmer gleiche Rechte eingesteht und die gleichen Regeln auferlegt, und das es so jedem gleichermaßen ermöglicht, mit jedem anderen beliebigen Netzwerkteilnehmer privat und Ende-zu-Ende zu kommunizieren oder Informationen für jeden zugänglich zu veröffentlichen.

Wie gestaltet sich eigentlich die Internet-Infrastruktur?

Wie bereits erwähnt, ist diese verteilte Netzwerkstruktur vor allem in den Protokollen des Internets eingebettet, zum Beispiel in der TCP/IP-Protocol-Suite. Diese Protokoll-Ebene ist eine logische Ebene, die die Regeln beschreibt, nach welchen der Austausch von Informationen zwischen zwei Netzwerkteilnehmern über das Internet erfolgen kann. Zu diesem Zweck bekommt jeder Netzwerkteilnehmer, das heißt jedes am Internet angeschlossene Gerät, eine eindeutig identifizierbare Adresse zugeschrieben, die wohlbekannte IP. Wenn nun ein Gerät eine Nachricht an ein anderes Gerät schicken möchte, so muss es diese Nachricht mit der Adresse des Empfängers kennzeichnen, ähnlich der Adresse auf einem Briefumschlag.

Das TCP (*Transmission Control Protocol*)-Routing-Protokoll legt dann fest, wie die Nachricht zum Empfänger kommt, nämlich indem sie von Router zu Router hüpft – jeder Router, jeder Knotenpunkt schaut sich die Adresse der Nachricht an und leitet diese weiter in die richtige Richtung. Das können wir uns wieder so ähnlich vorstellen wie bei der Post: zuerst wird auf den Ländercode geschaut, dann auf das Bundesland, die Gemeinde, den Ortsteil und schließlich Straße und Hausnummer. Durch diese Routingprotokolle wird die Idee des verteilten Netzwerkes, in dem jeder mit jedem gleichermaßen und nach den gleichen Regeln kommunizieren kann, dann zur Realität.[9]

Damit dieses verteilte Netzwerk allerdings technisch wirklich funktionieren kann, braucht das Internet neben diesen logischen Protokollen eben auch noch eine physisch-materielle Infrastruktur, die Informationen in Form von elektrischen oder optischen Signalen übertragen kann, genauso wie unsere verteilte postalische Kommunikation die Infrastruktur der Post, ihre Außenstellen, Sammelstellen und Verteilungscenter, LKWs und deren Autobahnen benötigt. Das Beispiel mit der Post zeigt uns indes auch gleich noch einen weiteren wichtigen Punkt: obwohl sich die logische, die Protokoll-Ebene, die es jedem erlaubt, eine Adresse zu haben und frei mit jeder anderen Adresse zu kommunizieren, als verteiltes Netzwerk gestaltet, kann es auf einer anderen Ebene der kommunikationstechnischen Infrastruktur durchaus zur Bildung zentralisierender Netzwerkstrukturen kommen.

Genauso verhält es sich auch mit der Internet-Infrastruktur. Wenn wir uns anschauen, wie Daten nach den Protokoll-Regeln übertragen werden und als Signale durch eine globale Infrastruktur an ihr Ziel huschen, können wir durchaus andere, dezentralisierte Netzwerkstrukturen entdecken. Da sind zum Beispiel die großen Unterseekabel, die es ermöglichen, Daten über Kontinente hinweg zu übermitteln und auszutauschen.[10] Diese Kabel werden meist von einigen großen Firmen betrieben, und es gibt einige wenige dicke Kabel, die die meisten interkontinentalen Daten übertragen. Wenn diese das Festland erreichen, werden sie an großen Schaltstellen gebündelt und von dort aus weitergeleitet.

Dann gibt es weiterhin die großen IXPs, die *Internet Exchange Points*, von denen sich viele der wichtigsten in den USA und in Europa, also auf Boden NSA-Verbündeter, befinden.[11] Diese Internet Exchange Points fungieren als Hubs, an denen die meisten Internetkommunikationen zusammen geführt werden und von dort aus wieder weiter Richtung Endstation verteilt werden (ähnlich den großen Verteilungszentren der Post). Und dann gibt es natürlich noch die großen Internetriesen, Konzerne wie Google, Facebook und Microsoft, die das Marktmonopol vieler Internetservices innehaben und die Daten stellvertretend für ihre Kunden speichern.

Überwachung als Mittel einer infrastrukturellen Politik

Wenn wir uns nun einmal anschauen wollen, wie genau die Internetüberwachung der Geheimdienste überhaupt funktioniert, und das können wir mit Hilfe der Snowden-Dokumente jetzt eben auch, dann entdecken wir, dass diese vor allem auf die physische Ebene der Infrastruktur angewiesen ist, eben jene Ebene, wo es innerhalb einer dezentralisierten Dateninfrastruktur verschiedene Hauptknotenpunkte gibt. Ein kurzer Exkurs zurück zu Galloways Netzwerkdiagrammen macht klar, warum: Überwachung gestaltet sich innerhalb verteilter Netzwerke als besonders schwierig und aufwändig, da Kommunikation über eine große Anzahl beliebiger Pfade erfolgen kann – im Netzwerk gibt es keine zentralen Kontrollstellen, wo Informationsströme zusammenkommen oder von wo aus sie kontrolliert, verarbeitet oder verteilt werden.

Da ein solches Netzwerk in der Realität technisch aber schwer umzusetzen wäre, ist die physische Infrastruktur des Internets zu einer dezentralisierten Dateninfrastruktur gewachsen, wo die Knotenpunkte der Kabel- und Servicenetzwerke sowie die IXPs wichtige Kontrollinstanzen darstellen. In solch einem dezentralisierten Netzwerk gestaltet sich Überwachung und zentralisierte Kontrolle wesentlich einfacher als in einem verteilten Netzwerk, da durch Anknüpfung an die Hauptknotenpunkte so gut wie alle Kommunikationen abgefangen werden können. Und genau hier setzt die NSA an, um ihr Schattennetzwerk der Überwachung zu errichten: da es für die NSA unmöglich wäre, alle einzelnen Internetteilnehmer an deren PC oder Server direkt anzuzapfen, abzuhören und zu überwachen, konnte sie sich die Knotenpunkte der materiellen Dateninfrastruktur des Internets zunutze machen.

So ist es kein Wunder, das die NSA auf ihren internen Folien vermerkt, dass die meisten Internetkommunikationen durch die

USA fließen werden.[12] Korrekterweise weist sie darauf hin, dass damit auch zu rechnen sei, wenn der geographisch direkteste Weg nicht durch die USA führt: da die besten Kabel von und zu den Knotenpunkten in den USA führen, ist es für Internetprovider häufig ökonomisch günstiger, ihren ganzen Verkehr durch die USA zu schicken. Und hier kann die NSA ansetzen: da sie auf amerikanischem Boden freie Verfügungsgewalt hat, kann sie dann ganz gemütlich ihre Überwachungsgeräte an diesen Knotenpunkten installieren.

Das hat sie zum Beispiel bei AT&T in San Francisco gemacht.[13] Wie wir vom ehemaligen Mitarbeiter Mark Klein bereits seit 2007 wissen, hatte sie dort ihren eigenen geheimen Raum beantragt, wo sie eine Kopie aller Internetkommunikationsflüsse mit einem Gerät namens Narus STA 6400 analysierte und von dort dann in ihr eigenes Überwachungsnetzwerk einspeiste. Um die geographische Bedeutung gewisser Knotenpunkte der Netzwerkinfrastruktur hervorzuheben, bildet die NSA auf einer anderen Folie als Hintergrund eine Landkarte des Verlaufes der Überseekabel ab.[14] Dort weist sie dann auch ihre Mitarbeiter an, die beiden Überwachungsprogramme *Upstream* und *PRISM* parallel zu verwenden. Während Upstream die Daten, die vorbeifließen, direkt von den Glasfaserkabeln und der Infrastruktur sammelt, greift PRISM auf die Server der großen Internetkonzerne zu, die die vertraulichen Daten ihrer Kunden dort speichern. So kann die NSA mit ihren Überwachungsmethoden die großen Knotenpunkte der Infrastruktur angreifen, von wo aus sie dann eine Verbindung zu ihrer übergeordneten Kontrollstelle schafft.

Mit diesen Techniken ist es der NSA dann scheinbar erfolgreich gelungen, ein zentralisiertes Schattennetzwerk zu erschaffen, das oberhalb der normalen Infrastruktur operiert und erst einmal nicht in Datenflüsse eingreift oder sie manipuliert, sondern eigentlich „nur" mithört. Dieses Netzwerk wird als Schattennetzwerk bezeichnet,[15] da es zunächst einmal für uns als Nutzer unsichtbar bleibt und nicht in den Alltag des Internets einzugreifen scheint. Für uns Nutzer ist ja die materielle infrastrukturelle Ebene, die Ebene, die Datensignale überträgt, normalerweise eigentlich nicht Teil der Erfahrung des Cyberraums.

Was wir erfahren, ist ein verteiltes Netzwerk, in dem wir uns frei bewegen können, und in dem wir uns mit jeder anderen Teilnehmerin (prinzipiell) austauschen können. Solange die materielle Ebene nach Plan funktioniert und unsere Daten verlässlich und nach den festgelegten Regeln überträgt, müssen wir uns um sie nicht kümmern. Genauso kennen wir uns ja bei der Post eigentlich auch nicht genau aus mit der Geographie der Verteilungscenter oder -routen, und das müssen wir ja auch nicht, wenn wir einen Brief an eine beliebige Bekannte oder Unbekannte verschicken wollen. Im Gegensatz zur Post allerdings gibt es in den Internetprotokollen wesentlich weniger Regeln, die genau bestimmen, wer welche Nachricht lesen oder anschauen kann. Des Weiteren sind die digitalen Datenpakete wesentlich einfacher heimlich mitzulesen, da man diese auch samt Inhalt kopieren kann, ohne Spuren am Briefumschlag zu hinterlassen.

Allerdings heißt diese Transparenz, die die NSA-Überwachung auszeichnet, nicht, dass diese keine Auswirkungen auf uns und das Internet selbst hat – im Gegenteil! Ohne unser Wissen werden wir Teil eines zentralisierten Netzwerkes, das außerhalb unserer demokratisch legitimierten Ordnung operiert. In diesem Schattennetzwerk positioniert sich die NSA selbst an höchster Stelle, von wo aus sie das gesamte, globale Netzwerk übersieht und letztendlich auch kontrolliert. Zumindest in der Theorie kann die NSA so nun Informationen über jede normale Internetteilnehmerin abrufen, die Kommunikation jeder mit jeder heimlich mitlesen oder sogar Kommunikationsströme einfach abbrechen oder unbemerkt manipulieren.

Das hat sie in ihrem Programm *Quantumtheory*, welches Malware in normale Internetkommunikationen einschleust, auch getan.[16] Die NSA selbst entzieht sich allerdings jeder Überwachung oder Kontrolle. Die Tatsache, dass ihr Schattennetzwerk unbemerkt und mit digitalen, also leicht und unbemerkbar kopierbaren Daten operiert, unterstützt diese Dynamik zusätzlich. So werden wir als gemeinsam Überwachte im Sinne Deweys Teil einer politischen Öffentlichkeit mit all denen, die mit uns durch das Netzwerk verbunden werden und unser Schicksal teilen.

Wenn die NSA dann die Form dieses Netzwerkes bestimmt, und dort an höchster Instanz steht, dann hat sie de facto Politik im Deweyschen Sinne gemacht, denn sie hat eine gewisse Netzwerkstruktur geschaffen, die Austausch und Interaktionen innerhalb der Infrastruktur auf eine bestimmte Weise gestaltet, bestimmt und kontrolliert. Auf Grund der Geheimhaltung dieser globalen Überwachungskanäle allerdings geschieht diese Politik, diese Regulierung, nicht in einer Weise, die laut des hier beschriebenen Ansatzes als demokratisch verstanden werden kann. Zum einen findet hier keinerlei öffentlicher Diskurs statt, an welchem die betroffene Öffentlichkeit teilnehmen und somit mitentscheiden kann, oder durch welchen sie ihre Vertreter kontrollieren kann. Zweitens sehen wir hier einen nationalen Sicherheitsdienst, der im Interesse einer Nation die Gestaltung eines globalen Netzwerkes anstrebt: das heißt, dass die Politik, die die Interaktionen im Internet mitgestaltet und formt, nicht im Interesse aller Beteiligten, sondern im Interesse einer Minderheit handelt.

Die gängigen Anti-Überwachungsmaßnahmen wie Verschlüsselung und Onion-Routing versuchen diesen Tendenzen entgegenzusteuern. Indem sie Überwachung auf der infrastrukturellen Ebene durch ein unlesbar Machen der übertragenen Nachrichten erschweren, versuchen sie so dem zentralisierenden Moment der Überwachung entgegenzuwirken und ein verteiltes Netzwerk zu schaffen, in dem wir frei und ungestört kommunizieren können. Allerdings tun sie das auch nicht unbedingt immer auf eine demokratische Art und Weise, sondern schaffen, genauso wie die NSA, mit Hilfe von Applikationen technische Realitäten.

Staatliche Überwachung – nur eine Frage der IT-Sicherheit und Privatsphäre?

Solche Betrachtungen eröffnen die Möglichkeit, die NSA-Affäre nicht nur unter den Aspekten von Privatsphäre, innerer Sicherheit und Cybersecurity zu betrachten, sondern staatliche Überwachung als politisches Mittel zu begreifen, das gewisse Machtverhältnisse innerhalb einer globalen Online-Gesellschaft zu schaffen sucht. Die Analyse, die ich in meiner Arbeit gemacht habe, hat gezeigt, dass es möglich ist, in der NSA-

Affäre strukturelle Aspekte zu identifizieren, die zeigen, wie solche Überwachungsmethoden auf den strukturellen Aufbau des globalen Netzwerkes abzielen. Indem sie ein zentralisiertes Schattennetzwerk kreieren, suchen sie gewisse globale geopolitische Bestrebungen ins Internet zu übertragen und dort zu verfestigen.

Im Sinne der von mir bemühten politischen Philosophie John Deweys können diese Bestrebungen dann insofern als politische Aktivitäten verstanden werden, als sie die infrastrukturelle Form des Internets mitgestalten und somit abzielen auf eine großflächige Regulierung der Interaktionen der globalen Öffentlichkeit, welche durch das Internet erst so geschaffen wurde. Die von Galloway beschriebenen Netzwerk-Topologien helfen uns zu verstehen, wie dieses strukturelle Formen der Netzwerkcharakteristika geschehen kann. Hier nützten die Überwachungsorgane selbst die bereits vorhandenen Knotenpunkte der dezentralisierten materiellen Internet-Infrastruktur aus, um darauf ihr zentralisiertes Schattennetzwerk aufbauen zu können. Insofern geht es nicht nur um die Frage, wer auf welche Informationen über welche Individuen zugreifen oder wessen persönliche E-Mails mitlesen kann oder inwiefern Möglichkeiten zur privaten Kommunikation geschwächt werden. Vielmehr geht es auch darum, wer Kontrolle über ein Netzwerk und dessen Interaktionen ausüben kann und welche Machtstrukturen in der Internet-Infrastruktur implementiert werden.

Anmerkungen (➔ Links in der online-Ausgabe abrufbar)

1 *Frontline PBS (2014, 13. Mai). United States of Secrets. Video-Datei, ➔*
2 *Fichtner, L. (2014). Masterarbeit Philosophy of Science, Technology and Society. ➔*
3 *Dewey, J. (1927). The public and its problems: An essay in political inquiry. Athens, OH: Swallow Press/Ohio University Press*
4 *Dewey (1927), S. 82*
5 *Dewey (1927), S. 16, p. 27*
6 *Galloway, A. (2004). Protocol: How control exists after decentralization. Cambridge, MA: The MIT Press*
7 *Galloway (2004), S. 11–12, 30–31*
8 *Berners-Lee (1999). Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor. New York, NY: HarperCollins*
9 *Blum, A. (2012). Tubes: A journey to the center of the internet. New York, NY: HarperCollins*
10 *TeleGeography (2014). Submarine Cable Map 2014. ➔*
11 *TeleGeography (2012). Global Internet Map 2012. ➔*
12 *The Guardian (2013, 1. November). NSA Prism program slides. ➔*
13 *Klein, M. (2007, 15. Mai). Spying on the home front (Interviewer H. Smith). ➔*
14 *The Washington Post (2013, 6. Juni). NSA slides explain the PRISM data-collection program. ➔*
15 *Appelbaum, J.; Horchert, J.; Reißmann, O.; Rosenbach, M.; Schindler, J.; Stöcker, C. (2013, 30. Dezember). Neue Dokumente: Der geheime Werkzeugkasten der NSA. SPIEGEL ONLINE NETZWELT, ➔*
16 *SPIEGEL ONLINE (2013, 30. Dezember). NSA-Dokumente: So übernimmt der Geheimdienst fremde Rechner. ➔*

Angela Meindl

FIfF-Studienpreis 2015 3. Preis

Internet-Profiling – Umfang, Risiken und Schutzmaßnahmen am Beispiel Google

Einen weiteren dritten Preis des FIfF-Studienpreises hat die Autorin für ihre Bachelorarbeit erhalten. Es geht darin um das Thema Datensammeln. Am Beispiel von Google wird gezeigt, wie Daten von Internetnutzer.innen unbemerkt gesammelt werden und wie diese Daten genutzt werden können. Sie befasst sich mit der Frage, welche Risiken dadurch entstehen können und welche Möglichkeiten des Schutzes bestehen. Ausführlich hat die Autorin über ihre Arbeit bereits in FIfF-Kommunikation 2/2015 *berichtet.[1] Wir bringen deshalb an dieser Stelle einen von der Redaktion gekürzten zusammenfassenden Bericht über ihren Inhalt.*

erschienen in der FIfF-Kommunikation, herausgegeben von FIfF e.V. - ISSN 0938-3476 www.fiff.de

Internet-Profiling nennt man den [illegible] niken werden im Einzelnen besich im Internet bewegen, mög[illegible]en nicht nur Aktivitäten der Nutonen zu sammeln und diese in [illegible] gerufene Webseite, Referrer und sammenzuführen. Dafür werden nicht nur die Daten gesammelt benutzte Suchmaschine, sondern auch viele Informationen über und gespeichert, die beim Ausfüllen eines Formulars absichtlich das benutzte Computersystem eingesammelt. Diese Datentypen preisgegeben werden. Mit Hilfe verschiedener Techniken, die werden in der Arbeit zusammengestellt. Aus diesen Informatiobeim Besuch einer Webseite nicht unmittelbar bemerkt werden, nen lässt sich ein *Browserfingerprint* erstellen. Nach einer Stukann der Weg der Internetnutzer.innen durch das Internet ver- die von Henning Tillmann[2] sollen Browserfingerprints mit einer folgt und dokumentiert werden. Begründet wird dieses Verfah- Wahrscheinlichkeit von bis zu 92,57 % auf die zugehörige Perren mit gezielterem personenbezogenem Inhalt, mit einer Ver- son hinweisen.
besserung der Usability, mit der Erhöhung der Effektivität von Webseiten und mit der Analyse von Werbekampagnen.

Weiter geht die Arbeit auf das *Targeting* ein, das heißt, auf das Ziel der Auswertung der eingesammelten Daten. Mit *Mouse-Targeting* wird das Leseverhalten auf der Webseite analysiert. Mit *Geo-Targeting* wird der Standort des Nutzers ermittelt. Die wichtigste Rolle spielt das *Behavioural-Targeting*. Alle erDie Arbeit geht zunächst darauf ein, mit welchen Techniken hobenen Daten und die daraus gewonnenen Analyseergebdaten gesammelt werden. Sie beschränkt sich darauf, exemplarisch die bekanntesten Dienste von Google zu untersuchen. Dort werden Daten mittels Zählpixel, Logdateien, Skripten und