Forkefeld, Nina

Working Paper

The invisible hand of social network: Wie viel Transparenz in Sozialen Netzwerken ist ökonomisch?

Discussion Papers, No. 24/2012

Provided in Cooperation with:
Witten/Herdecke University, Faculty of Management and Economics

Suggested Citation: Forkefeld, Nina (2012) : The invisible hand of social network: Wie viel Transparenz in Sozialen Netzwerken ist ökonomisch?, Discussion Papers, No. 24/2012, Universität Witten/Herdecke, Fakultät für Wirtschaftswissenschaft, Witten

This Version is available at:
https://hdl.handle.net/10419/66134

discussion papers

Fakultät für Wirtschaftswissenschaft Universität Witten/Herdecke

Neue Serie 2010 ff. Nr. 24 / 2012

The invisible hand of social network
Wie viel Transparenz in Sozialen Netzwerken ist ökonomisch?

Nina Forkefeld

discussion papers

Fakultät für Wirtschaftswissenschaft Universität Witten/Herdecke www.uni-wh.de/wirtschaft/discussion-papers

Adresse der Verfasser: Nina Forkefeld Nina Forkefeld
nina.forkefeld@gmx.de

1 Einleitung

1.1 Zum Titel

Im Rahmen der Wirtschaftsethik werden Annahmen und Modelle der Ökonomie durch eine anthropologische Perspektive ergänzt. In Anbetracht der aktuellen Finanzmarkt- und Euro- Krisen besteht ein enormer ethischer Anspruch an wirtschaftliches Handeln und die Folgen wirtschaftlichen Handelns. Ein ebensolcher Anspruch ist auch gegenüber Internetkonzernen und Neuen Medien spürbar.
Soziale Netzwerke wie Facebook nötigen ihre Nutzer zur Preisgabe privater Daten und zur Übertragung von Urheberrechten. Gerade Facebook und Google gelten gemeinhin als notorische Datensammler und stehen dafür nicht selten am Pranger. Missfallens-Stürme von Nutzern führen aber regelmäßig zur Anpassung von Datenschutzbestimmung. Ob diese Änderungen immer im Sinne der Nutzer sind bleibt dabei offen. Wie aber kann eine wohlfahrtsökonomisch effiziente Bestimmung des Transparenzgrades bezüglich persönlicher Daten und Urheberrechte gefunden werden? Dies soll die vorliegende Untersuchung zeigen.

Die Eingangshypothese dabei ist, dass ein staatlicher Regelungsbedarf im wohlfahrtsökonomischen Sinne nicht gegeben ist, da netzwerkökonomische Anreize die Betreiber der sozialen Netzwerke dazu bringen, einen Grad der Nutzerdatentransparenz zu wählen, der sowohl für sie als auch für den Nutzer als optimal zu bezeichnen ist. Am Beispiel von Facebook entsteht eine kritische Analyse weiterer wirtschaftsethischer Themenfelder, welche von netzwerkökonomischen Anreiz-Strukturen betroffen sind.

Zudem wird die Eingangshypothese einer eingehenden Prüfung unterzogen, die zeigen wird ob die Datenschutzmaßnahmen seitens der Nutzer und Betreiber ausreichend sind oder ob ein weiteres Eingreifen dritter Instanzen erforderlich ist.

1.2 Agenda

Diese Untersuchung stellt den Datenschutzdiskurs und das Problem des strukturellen Ungleichgewichts des Datenmarktes dar. Nach einer Definition des Datenschutzbegriffs und der Betrachtung der rechtlichen Determinanten, entsteht eine eigene Struktur-Definition des Datenschutzbegriffs. Diese ermöglicht es die Eingangshypothese zu überprüfen. Netzwerkökonomische Anreize der beteiligten Stakeholder-Gruppen werden untersucht. Experteninterviews belegen die einzelnen

Perspektiven der Datenschutz-Debatte in Deutschland. Zu den interviewten Experten dieser Arbeit zählen in alphabetischer Reihenfolge: Dr. Gunnar Bender (Director of Politics Facebook Germany), Axel E. Fischer (Vorsitzender der Enquete-Kommission Internet und Digitale Gesellschaft), Stefan Lorenz (IT-Spezialist und Entwickler der X-Pire!-Software, Backes SRT-GmbH), Peter Schaar (Bundesdatenschutzbeauftragter Deutschland), Rena Tangens (Vorsitzende der Datenschutzvereinigung FoeBuD e.V.) und Harvard-Hirnforscherin Diana Tamir, die ihre aktuelle Studie *„Disclosing information about the self is intrinsically rewarding“* zur Verfügung stellte. Außerdem war Bundestagspräsident Norbert Lammert am 18. Juni 2012 auf einer Bochumer Veranstaltung der Konrad-Adenauer-Stiftung zu einem kurzen Statement zur Thematik bereit. Seine Stellungnahme findet sich auf S.65 dieser Arbeit. Die Experten-Interviews, sowie die Studie befinden sich im Anhang ab S. 98.

1.3 Der Datenschutz- und Informationssicherheits- Begriff

Der Datenschutz-Begriff ist einem stetigen Wandel unterworfen. Sein Begriffsinhalt ist daher diffus, nicht eindeutig und entzieht sich der Zuordnung zu einem einzigen semantischen Feld oder einem einzigen geographischen Rechtsraum. Dieses Kapitel wird die verschiedenen Bedeutungszusammenhänge des Datenschutz-Begriffs anhand der sich wandelnden Internetnutzung näher betrachten und so eine engere Begriffskonstruktion entwerfen. Diese fungiert als zweckdienliches begriffliches Instrument für die anschließende Analyse der netzwerkökonomischen Anreizstrukturen.

Die erstmalige Verwendung des Deutschen „Datenschutz“-Begriffs wurde 1972 durch das hessische Datenschutzgesetz geläufig. Das hessische Datenschutzgesetz war das weltweit erste überhaupt (Schaar, 2007, S. 25). 1977 wurde dieses Datenschutzgesetz in das Bundesdatenschutzgesetz übernommen und somit im Deutschen Rechtssystem implementiert. Schaar warnt vor einer Verwechslung des Datenschutz-Begriffs (meint hier: Schutz der Würde, Handlungsfreiheit und Privatsphäre von Individuen) mit dem Begriff der Datensicherheit (meint hier: Zugriffs- und Verfälschungsmöglichkeiten durch technologische Voraussetzungen) und eröffnet somit die Dualität des Begriffsverständnisses und den Spannungsdiskurs der Datenschutz-Definition (Schaar, 2007, S. 23 ff.).

Zunächst einmal stehen zwei Grunddefinitionen des Datenschutzbegriffs im

Vordergrund siehe (1) und (2): Die Schutz- und Sicherheitsmetaphorik entstammt der juristischen Einteilung in Besitztümer und Güter und bezieht sich vor allem auf die **schützenswerte Ressource geistigen Eigentums (1)**. Jedoch hat sich im Zuge der zunehmenden Globalisierung und Digitalisierung eine weitere Begriffs-Bedeutung heraus gebildet. Datenschutz ist heute vor allem der **Versuch Identitäten realer Personen zu schützen (2)**, im Sinne der Wahrung des individuellen Persönlichkeitsrechts. Die Internetnutzung hat sich dahingehend verändert, dass im Internet nicht mehr länger nur Informationen verbreitet und gesucht werden können. Die **eindeutige Identitätszuweisung zu einem Internet-Nutzer (3)** gerät mit der Diversität und Anzahl der Internetnutzungsaktivitäten zu einem komplexen Unterfangen.

Von der ursprünglichen Nutzung des Internets als Informations-Archiv beginnend, fanden bald auch schon Märkte ihren Platz im World Wide Web. Frühzeitige Anwender des Internets, die man als Nerds oder Geeks[1] bezeichnete, nutzten so genannte Managed Broad Band Services (meint verwaltete Breitbanddienste) und beteiligten sich z.B. an Foren (Brill / de Vries, 1998). Was anfänglich mit Partnerbörsen und Job-Portalen begann, entwickelte sich allmählich weiter zu umfassenden Einkaufsmöglichkeiten wie Shopping-Portalen, Internet-Auktionen oder schlichten Unterhaltungsportalen für Videos und Musik. Anfangs nur zögerlich wurden im Netz klassische Werbe-Anzeigen platziert, die beispielsweise alltägliche Konsumgüter anboten. Das Internet jedoch brachte viele neue Möglichkeiten und Geschäftsmodelle für das Angebots-Nachfrage-Prinzip. Mit den Repräsentanzen der Unternehmen im Netz stieg auch die Anzahl der Repräsentanzen von Privatpersonen in sogenannten Sozialen Netzwerken, Foren und sogenannten Social Communities.

Somit ergibt sich eine **duale Datenschutz-Kultur**, denn sowohl Internetseiten-Betreiber wie auch Internetseiten-Nutzer benötigen Datenschutz. Aus diesem Grund operiert die IT-Sprache mit zwei Datenschutzbegriffen der **„data security" (Sicherheit)** und der **„data privacy" (Privatsphäre)**. **Der Privatsphäre-Begriff** entstammt einem 1890 in den USA veröffentlichten Aufsatz mit dem Titel „The Right to Privacy". Die Juristen Louis D. Brandeis und Samuel Warren leiteten aus den Grundsätzen zum Personen- und Eigentumsschutz das „right to be let alone" ab

[1] umgangssprachlich für Streber, meint aber eine Person, die sich durch großes Interesse an informationswissenschaftlichen, technologischen oder fiktionalen Themen auszeichnet

(Brandeis/Warren, 1890 und Schaar, 2007, S. 23), ein Vorgänger des „Rechts auf informationelle Selbstbestimmung“, welches einen privaten Rückzugsort für Meinungsbildungs- und Entscheidungsprozesse für private wie auch in der Öffentlichkeit stehende Individuen bedeutet: *„Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone" Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."* (Brandeis/Warren, 1890).

Der Sicherheits-Begriff bezieht sich seit dem Erlass des Bundesverfassungsgerichtes im so genannten Volkszählungsurteil im Jahre 2003 sowohl auf den **Schutz vor Datenmissbrauch** als auch auf die **informationelle Selbstbestimmung** (Wikipedia, 2012 A). Das Deutsche Bundesdatenschutzgesetz aus dem Jahr 1977 hingegen legte den Schwerpunkt einzig auf die Sicherheit der personenbezogenen Daten Betroffener, nicht aber auf deren geistiges Eigentum. Aufgabe des Datenschutzes war 1977 *„durch den Schutz personenbezogener Daten vor Missbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken“* (§ 1 Abs. 1 BDSG 1977). Heute wird die Wahrung der personenbezogenen Daten vor allem durch technische Errungenschaften, wie z.B. Cloud Computing [2] massiv erschwert. Obwohl bereits seit 2001 im Bundesdatenschutzgesetz der Grundsatz der **„Datensparsamkeit“** existiert (Schaar, 2007, S. 55) werden durch technologische Veränderungen wie Cloud-Computing immer mehr Daten auf zentralen Servern gespeichert, anstatt auf persönlichen Computern und Endgeräten (European Commission, 2012 A). Der Sicherheitsbegriff des Datenschutzes wurde daher 2003 in den einzelnen Bundesländern erweitert. Er umfasst aktuell eine Zugriffsbeschränkung für Dritte, auf gespeicherte und auch veröffentlichte Daten (Schaar, 2007). Geistiges Eigentum ist somit ebenso geschützt, wie die Persönlichkeitsrechte. Dies ist aber erst der Fall seit aus den allgemeinen

[2] Cloud Computing beschreibt die Möglichkeit Computerprogramme, Anwendungen und Daten nicht mehr länger auf dem eigenen Rechner zu speichern, sondern diese an zentrale Rechenzentren auszulagern. Nutzer können auf virtuelle Programme und Speicherplatz im Netz flexibel zugreifen.

Persönlichkeitsrechten ein „Recht auf informationelle Selbstbestimmung“ abgeleitet wurde. Diese Veränderung belegt beispielsweise das aktuelle Landesdatenschutzgesetz des Landes Nordrhein-Westfalen: *„Aufgabe dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).“* (Landesdatenschutzgesetz Nordrhein-Westfalen, § 1, 2003).

Die seit 2003 bestehende Datenschutz-Mischform aus „data protection“ und „data privacy“ ist bis jetzt allerdings noch kein vollständiger Bestandteil der Definition. Der Deutsche Duden definiert Datenschutz beispielsweise wie folgt *„Schutz des Bürgers vor Beeinträchtigungen seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen“* (Duden, 2012). Auch die Europäische Union hält es noch mit der älteren Definition von 2003, laut der EU bedeutet Datenschutz *„insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“* (Art. 1 Abs. 1 Richtlinie 95/46/EG, 1995). Diese europäische Datenschutzrichtlinie und die Datenschutzgesetze der Europäischen Staaten verankerten eine **verbindliche und unabhängige Datenschutzkontrolle** für Unternehmen, sowie für private wie öffentliche Institutionen. Dies bedeutete einen **signifikanten Unterschied zu den Entscheidungen des US-Kongresses**, der 1974 zwar einen „Privacy Act“ verabschiedete, dabei jedoch die Wirtschaft ausklammerte. Auch der US-Senat entschied sich für einen Marktmechanismus in Sachen Datenschutz und traf die Entscheidung kein unabhängiges Datenschutzkontroll-Organ einzusetzen (Schaar, 2007, S. 24ff.).

Der Europarat versteht Datenschutz als Schutz des *„Recht[s] auf einen Persönlichkeitsbereich […] bei der automatischen Verarbeitung personenbezogener Daten“* (Art. 1 Europäische Datenschutzkonvention, 1995). Trotz eingeführter Kontrollinstanz arbeitet die Europäische Union derzeit an der Erweiterung des Datenschutzbegriffs, um auf aktuelle technologische Entwicklungen zu reagieren. Am 25. Januar 2012 kündigte man in Brüssel eine übergreifende Online-Datenschutz-Reform an, mit dem Ziel, die Datenspeicherrechte im Sinne der Persönlichkeitsrechte, ebenso wie die europäische Digitalökonomie, zu stärken.

Grund hierfür sei das mangelnde Sicherheitsempfinden von Internet-Nutzern bezogen auf die Autonomie ihrer Datenpreisgabe (European Commission, 2012 B). Bislang ist der „data privacy"- Begriff und der Schutz der Privatsphäre des beruflichen, öffentlichen und privaten Lebens von Personen im **europäischen Rechtsraum** jedenfalls noch nicht gebräuchlich. In der Gesetzgebung wird überwiegend der Begriff "data protection" verwendet, der sowohl als Datensicherheit wie auch als Informationssicherheit übersetzt wird. Im Fokus dieser Begrifflichkeit steht **die Datensicherheit im Sinne der Vermeidung von Datendiebstahl, Datenveränderung und -Missbrauch, sowie der Schutz vor Datenverlust.**

Doch auch die fortschrittlichere Datenschutzdefinition war vor 2003 in der Literatur zu entdecken. Bereits im Jahre 2001, vor dem Erlass 2003, betonten die Autoren des Buches „Sicherheitskonzepte für das Internet" die Wichtigkeit der Autonomie der Internetnutzer in Bezug auf ihre privaten wie öffentlichen Daten: *„Zum klassischen Schutz der individuellen Privatsphäre im Sinne der Verwirklichung der informationellen Selbstbestimmung tritt untrennbar sowohl die notwendige Berücksichtigung der kommunikativen Autonomie aller an der elektronischen Kommunikation Beteiligten, als auch die notwendige Gewährleistung einer hinreichenden technischen Datensicherheit als Grundvoraussetzung hinzu [...] Die erfolgreiche Erfüllung aller Aufgaben hängt dabei zunehmend von der Realisierung der vier wichtigsten informationstechnischen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit ab, d.h. der technologisch auszuschließenden unbefugten Kenntnisnahme Dritter sowie der [...] im – autorisierten – Bedarfsfall möglichen Identifikation der kommunizierenden Nutzer."* (Müller/Reichenbach, 2001, S. 193).

Die von Müller und Reichenbach formulierten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit sind Richtziele, wie sie heute u.a. auch in den Nutzungsbedingungen eines Sozialen Netzwerks wie Facebook wiederzufinden sind. Die Autoren jedoch schreiben bereits in ihrem Werk 2001, drei Jahre vor der Gründung Facebooks, dass lückenloser Datenschutz in dezentralen Netzwerken eine auf Dauer nur schwierig zu bewältigende Herausforderung darstellt: *„[...] die Dezentralisierung der Datenverarbeitung in komplexen Netzwerken macht allein die Feststellung sämtlicher potentiell sensibler Verarbeitungsprozesse unmöglich [...]"*

(Müller/Reichenbach, 2001, S. 191).

Das Gabler-Wirtschaftslexikon versteht unter dem Datenschutz-Begriff einen: „*Sammelbegriff über die in verschiedenen Gesetzen zum Schutz des Individuums angeordneten Rechtsnormen, die verhindern sollen, dass seine Privatsphäre in einer zunehmend automatisierten und computerisierten Welt („Der gläserne Mensch“) vor unberechtigten Zugriffen von außen (Staat, andere Private) geschützt wird*“ (Gabler, 2012). Mit dieser Auslegung wird zwar das im Datenschutz-Begriff enthaltene Spannungsverhältnis zwischen Freiheitsanspruch und Wahrung der Menschenwürde nicht besonders exponiert, jedoch wird deutlich, dass der Schutz der Privatsphäre des Individuums nach heutiger Definition im Vordergrund steht.

Der Identitätsschutz und der Schutz der Privatsphäre ist allerdings nicht erst seit kurzem ein Anliegen der Deutschen Politik, wie die Begriffsentstehung vermuten lassen könnte. Bereits 1997 wurde in Deutschland gesetzlich vorgeschrieben, dass anonyme Äußerungen und das Verwenden von Synonymen und Nicknames zulässig sind. Betreiber müssen ihren Nutzern die Inanspruchnahme auch anonym oder pseudonym ermöglichen. Die gesetzliche Vorgabe findet sich in § 13 Abs. 6 des Telemediengesetzes (TMG):
„Der Dienstanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“ (Schaar, 2012 A).

Generell bezieht sich der **Datenschutzbegriff** auf die **rechtlichen Grundlagen zum Schutze von Menschenwürde und informationeller Freiheit**. Der Begriff der **Informationssicherheit** hingegen befasst sich eher mit **technischen Bedingungen von personenbezogenen Daten**. Der optimale Datenschutz-Begriff müsste daher folgende Kriterien erfüllen:

1.4 Eine eigene Datenschutz-Strukturdefinition

Schutz der **Menschenwürde (A)** gemäß der Persönlichkeitsrechte des Grundgesetzes, sowie der daraus abgeleiteten **informationellen Selbstbestimmung (B)**. Außerdem Schutz **geistigen Eigentums (C)** gemäß dem Urheberrecht. **Nutzer-Autonomie (D)** bezüglich Datenpreisgabe, Speicherung und Löschung, sowie Freigabe von Daten und Informationen nur nach vorheriger Zustimmung des

Nutzers, kann durch **Transparenz (E)** bezüglich der Datenverwendung seitens der Betreiber erreicht werden. **Schutz von Nutzer-Identitäten (F)** durch eindeutige Identifizierung von Internet-Nutzern.

Während (A), (B), (C) und (F) diejenigen Determinanten sind, die durch einen **gesetzlichen Rahmen** implementiert werden, unterliegen die Definitions-Eckpunkte (D) und (E) nicht allein technischen Voraussetzungen, sondern einer **gegenseitigen Compliance-Vereinbarung von Betreibern und Nutzern**. **Insbesondere der Identitätsschutz (F) unterliegt sowohl gesetzlichen wie auch Compliance-Vereinbarungen,** Privatsphäre kann z.B. sowohl durch individuelle Nutzereistellungen wie auch durch einen Rechtsrahmen gewährleistet werden. Selbiges gilt für weitere Identität schützende Faktoren, wie Arbeitnehmerschutz, Mobbing-Immunität, Hacking- und Spionage-Immunität. All diese Bereiche können sowohl mit staatlichen Sanktionierungen belegt werden, wie auch durch Anreizstrukturen in Unternehmen und in öffentlichen wie privaten Institutionen verankert werden. Durch eine unternehmerische Selbstverpflichtung, z.B. zu einer „Datensparsamkeit“ mit der Anforderung nicht mehr persönliche Daten zu erheben als notwendig, kann eine Sensibilisierung geschehen und die derzeit vorherrschende Unverbindlichkeit abnehmen.

Auch Betreiber sollten über eine **selbst gewählte Limitierung der Datenvorratshaltung** nachdenken, um das Risiko für Missbrauch, Identitätsdiebstahl, Mobbing oder Erpressung zu begrenzen. **Selbstverpflichtung statt Sanktionierung** kann einen wertvollen Wissenstransfer unterstützen.

Betreiber sollten generell Nutzerorientiert agieren und ihre eigene **Anwendungs-Plausibilität,** sowie den **Zusatznutzen eines neuen Produktes** überdenken. Nach wie vor ist umstritten, ob der Betreiber eine Bringschuld oder der Nutzer eine Holschuld inne hat.

Aktuelle Überlegungen gehen zu einer Freigabe-Politik seitens der Nutzer, die Steiner wie folgt beschreibt: *„Personenbezogene Daten dürfen aber nur genutzt werden, wenn gesetzliche Vorschriften dies zulassen oder der Betroffene ausdrücklich eingewilligt hat, und zwar in schriftlicher Form. Im Internet wird häufig eine elektronische Einwilligung angefordert z.B. durch das Anklicken eines*

*Buttons. Personenbezogene Daten müssen nach ihrer Nutzung gelöscht werden [...]. Außerdem muss der Nutzer darüber informiert werden, welche Daten zu welchem Zweck gespeichert wurden. Wenn etwa Daten zur Erstellung eines Nutzerprofils oder im Rahmen einer Untersuchung gespeichert wurden, muss dem Nutzer dies mitgeteilt werden.“ (*Steiner, 2006, S. 47 ff)

Die Bringschuld des Betreibers hat laut dieser Definition einen hohen Stellenwert. Diese Arbeit wird weiterhin untersuchen in welcher Weise **Nutzer und Betreiber ein gemeinsames Datennutzungs-Optimum** erreichen können.

1.5 Rechtliche Grundlagen des Datenschutzbegriffs in Deutschland

Die demokratische und gesetzliche Basis des Deutschen Datenschutzes sind die Grundrechte auf Datenschutz, das Telekommunikationsgeheimnis, und die Meinungsfreiheit (Art. 2 I iVm 1 I, 5, 10 GG, Art. 7, 8, 11 Europäische Grundrechte Charta). Weitere Grundlagen bilden das Bundesdatenschutzgesetz (BDSG), und das Telemedien Gesetz (TMG). Aktuell besteht zudem die Überlegung seitens der EU, die Europäische Datenschutzrichtlinie aus dem Jahre 1996 zu erweitern und künftig als Europäische Datenschutz-Grundverordnung zu erlassen. Die so genannte E-Privacy-Richtlinie ist eine EU- Datenschutzrichtlinie für elektronische Kommunikation aus dem Jahr 2002. Sie ist die Fortsetzung früherer Überlegungen zur Privatsphäre im digitalen Zeitalter und reguliert u.a. den Umgang mit Verkehrsdaten, Spam und Cookies (Weichert, 2012). Diese Richtlinie (2002/58) wurde durch die Richtlinie (2009/136) erweitert. Dies betraf vor allem die Verwendung der so genannten Cookies, die fortan nur mit der vorherigen Zustimmung der jeweiligen Nutzer eingesetzt werden sollen (E-Privacy-Directive u.a. Art. 5 Abs. 3 – Cookieregelung).

Die Ansammlung gesetzlicher Regulierungen ist komplex und intransparent und wird zudem ergänzt durch weitere europäische Regelungen und Gesetze, wie z. B. durch das Urheber- und Markenrecht, das Vertragsrecht, den Verbraucherschutz, die AGB’s , und Regelungen zum Fernabsatz. In Deutschland wichtige Grundregeln lassen sich in **sieben Prinzipien** akkumulieren: Das Prinzip der **Rechtmäßigkeit der Datenerhebung**, d.h. dass Daten nur aus triftigem Grund z.B. für einen Vertragsabschluss erhoben werden (§§ 4, 27ff. BDSG, TMG). Das Prinzip der

Einwilligung durch den Kunden oder Nutzer, welches bedeutet dass dieser der Datenerhebung aktiv zustimmen muss (§ 4a BDSG, § 13 Abs. 2 TMG). Der Grundsatz der **Zweckbindung der Datenerhebung**, der besagt dass die Daten z.B. beim Zustandekommen eines Kaufvertrags nur für dessen Erfüllung gespeichert werden, aber nicht unbedingt zu weiteren Zwecken wie z.B. Werbung eingesetzt werden. Die Maxime der **Erforderlichkeit und Datensparsamkeit** ist nicht gesetzlich fixiert, sondern vielmehr eine Norm, die dazu anhält, nicht mehr Daten als notwendig zu dokumentieren. Eine ebensolche Richtlinie ist die Beachtung von **Transparenz und Betroffenenrechten**, ein wünschenswertes Vorgehen, dessen Missachtung jedoch nicht rechtlich sanktioniert wird. Der Aspekt der **Datensicherheit** besagt, dass Daten vor Fremdzugriffen und Missbrauch geschützt sein sollen. Bei Nichtbefolgung gibt es jedoch keinen einheitlichen Maßnahmenkatalog, sondern vielfältige und unterschiedliche Verfahrensweisen (Weichert, 2012). Der Grundsatz der Möglichkeit der **Kontrolle** von Datenschutzpraktiken letztlich ist wieder gesetzlich gefordert (§ 38 BDSG).

Thilo Weichert, Datenschutzbeauftragter in Schleswig-Holstein, kritisiert die Deutsche Regelungsvielfalt, sowie die Tatsache, dass das Bundesministerium des Inneren (BMI) bis Ende 2010 nur rechtlich bereits festgelegte Sachverhalte weiter vertiefte, wie z.B das Verbot schwerer Eingriffe ins Persönlichkeitsrecht (StGB) und das Verbot der Bildung von Persönlichkeitsprofilen (BVerfGseit 1969, Mikrozensus). Andere wichtige Grundsatzfragen werden seiner Auffassung nach nicht ausreichend diskutiert, wie z.B. die Interessenabwägung zwischen Social Media Nutzern und Werbetreibenden oder die Frage der Erfassung internationaler Netzwerkbetreiber im europäischen Markt (Weichert, 2012).

2 Theoretische Fundierung

Um den Diskurs der Datenschutzdebatte im Internetzeitalter besser zu verstehen wird in diesem Kapitel eine theoretische Grundlage geschaffen, die aktuelle Ansätze und Thesen zur Omnipräsenz von Medialität nachvollziehbar macht. Heutzutage ist es eine Selbstverständlichkeit allerorts und jederzeit erreichbar (Mobile Endgeräte) und sichtbar (Überwachungskameras) zu sein. Mit der Preisgabe von Informationen über das Selbst im Internet entsteht jedoch die Frage ob eine verstärkte Eigenkontrolle

oder doch äußerlicher Zwang zu einem tragbaren Umgang mit neuen Medien führt. Kapitelabschnitt 2.1 stellt zwei verschiedene Datenschutzansätze zu dieser Fragestellung vor. Die Problematiken der Allgegenwart des Internets werden in Kapitel 2.2 näher betrachtet. Grundlegendere Annahmen darüber. Mit der Frage warum Individuen in Sozialen Internet-Netzwerken agieren beschäftigt sich Kapitel 2.3

2.1 privacy-by-design vs. privacy-by-default

Der **privacy-by-design- Begriff** bezeichnet eine dem gesetzlichen Datenschutz vorgelagerte Variante technologischer Begrenzung. Bereits bei der Konzeption und Neuentwicklung von Internet-Produkten (z.B. Software oder Internetdienste), soll dabei Rücksicht auf Datenschutzgrundsätze und mögliche Konflikte bei der Produktnutzung genommen werden (Lüpken-Räder, 2012, S.96). Datenschutzproblemen soll präventiv vorgebeugt werden. Je früher ein Internet-Produkt auf Datenschutz-Kompatibilität abgestimmt wird (im Idealfall sogar gleich bei der Programmierung), desto weniger Kosten entstehen bei der Behebung von Rechtswidrigkeiten und Verstößen. Die technische Vorgabe einer programmierten Internet-Anwendung beschränkt das Produkt apriori auf Datenschutzkonforme Nutzung (Corchado et al., 2011, S.185). Der privacy-by-design-Ansatz entspricht den Überlegungen zur Informationssicherheit und „data security“ aus Kapitel 1.3.

Der **privacy-by-default- Begriff** meint die Möglichkeit einer nutzerdefinierten Voreinstellung. Jeder Nutzer sollte Internetprodukte mit datenschutzaffinen Einstellungen verwenden können und selbst das Maß seiner Datenpreisgabe durch eigene Einstellungen bestimmen können. Der Hersteller trägt die Verantwortung ein derartiges Voreinstellungssetting anzubieten, dass die Privatsphäre des Nutzers bestmöglich gewährleistet (Lüpken-Räder, 2012, S.96). Insbesondere Soziale Netzwerke könnten von einer derartigen individuellen Wahlmöglichkeit profitieren. Beispielsweise bei Einstellungen in denen das persönliche Nutzerprofil, nur von bereits verknüpften Freunden eingesehen, nicht aber von Suchmaschinen gefunden werden kann (Moore T. et al., 2010, S.141). Der privacy-by-default-Ansatz entspricht den Überlegungen zur Privatsphäre im Sinne des Rechts auf informationelle Selbstbestimmung und „data privacy“ aus Kapitel 1.3.

2.2 Ubiquitous Computing – Allgegenwärtige Datenverarbeitung

Der Ubiquitous Computing- Begriff wurde von dem US- Informatik und Kommunikationswissenschaftler Mark Weiser geprägt, der 1991 in seinem Werk „The Computer for the 21st Century“ die Entwicklung der Allgegenwärtigkeit des Internets voraus sagte: *„In the 21st century the technology revolution will move into the everyday, the small and the invisible“* (Weiser, 1991). Er skizzierte schon damals eine digitale Medienwelt, die sich weg vom persönlichen PC und hin zu intelligenter Technik und intelligenten Alltagsgegenstände bewegt. Dabei spricht er von kleinen und unsichtbaren Prozessoren und hatte dabei sowohl den Trend zur Microchip-Entwicklung als auch die Entstehung kabelloser Netzwerke vor Augen.

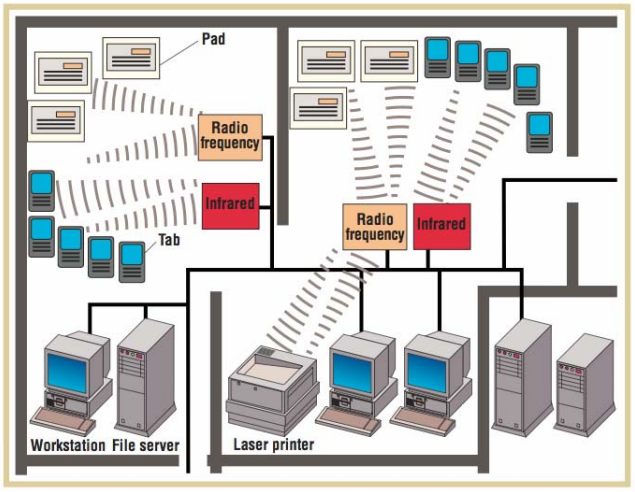


Abbildung 1 „Ubiquitous Computing“ Reprint aus dem Werk von Weiser, 1991

Erstaunlich daran ist, dass das Smartphone, also das erste Mobiltelefon, welches die Funktionalität eines Computers besaß erst 2005 für Endverbraucher erhältlich und technologisch erschwinglich war. Ende der achtziger Jahre war die Markteinführung des iPhones im Jahr 2007 ebenfalls noch nicht absehbar. Weiser unterschied bereits 1991 kabelgebundene und drahtlose Netzwerke, die es ihren Nutzern ermöglichen, Programme und Daten zu teilen. Er dachte an zukünftige Geräte im Taschenformat und verwendete dabei bereits den Begriff Tabs (Tablet-PCs), die heute auch als Pads (Touchpads) bekannt sind. Er schrieb, dass zukünftige Netze geeignet sein müssen, um hunderte von Geräten zu unterstützen, egal ob Taschengeräte, Laserdrucker oder Großbild-Displays, die Bewegung der Geräte von einem Ort zum anderen, werde das Modell der Zukunft sein. Dabei hatte Weiser bereits Funkfrequenz-basierte Netzwerke und Infrarot-Übertragung im Sinn und er sollte damit Recht behalten

(Weiser, 1991).

Genau diese Beweglichkeit, Allgegenwart und Möglichkeit des mobilen Datentransfers ist es, welche den Datenschutz vor neue Herausforderungen stellt. Ubiquitäre Internet-Nutzung basiert auf der möglichst exakten Abtastung der Umwelt durch IT-Systeme. Dies bedeutet Standortdaten wie Position, Geschwindigkeit, Wetter und die den Nutzer umgebende Infrastruktur, werden durch Sensoren erstellt und an Datenverarbeitungssysteme (Server) weitergeleitet. Ubiquitäre Datenverarbeitung bedeutet sensorische Datenverarbeitung, das technische Gerät erkennt die Umgebung des Nutzers anhand von Sensoren. Einzig der olfaktorische Sinn ist bislang nicht in Smartphones und PCs integriert. Jedoch existieren bereits heute Datenübertragungswege die den menschlichen Sinnen entsprechen. Akustische, optische, und Funk-Datenübertragungen aus der Nutzerumgebung, sowie weitere Übertragungsformen wie z.B. RFID (radio frequency identification = Identifizierung per Funk) sorgen für kontaktfreies Speichern und Auslesen von Daten (Taucis-Studie, 2006).

Es braucht nicht viel Phantasie, um hierin auch Überwachungs- und Kontrollmöglichkeiten (z.B. zwecks Personenerkennung und Verhaltensanalyse) zu erkennen. Problematisch ist vor allem die Möglichkeit des Taggings, Trackings und Profilings von Personen, da ihre Privatsphäre dadurch verletzt werden kann. Ein Beispiel hierfür sind so genannte RFID-Tags, sie ermöglichen die Identifikation eines Objekts mit einer eindeutigen Kennung. Die Kennung enthält Informationen zu dem Gegenstand, welche sich mit einer Datenbank abgleichen lassen. Der „Electronic Product Code“ (EPC) ist ein Nummerncode der die eindeutige Erkennung und Unterscheidung ermöglicht.

Für den Nutzer kann diese Erkennung einen erheblichen Eingriff in die Privatsphäre bedeuten, da kein Sichtkontakt für die Identifikation nötig ist. Der Nutzer merkt überhaupt nicht, dass er auf RFID-Tags gescannt wird. Ebenso wenig ahnt der Nutzer, wann und wo er Träger eines EPC ist Rückschlusse auf eine Personenidentität sind mittlerweile nicht nur durch biometrische Erkennungssysteme möglich, sondern auch durch elektronische Fingerabdrücke (Taucis-Studie, 2006, S. 27).

Mehr Transparenz über die Verfahren der Hintergrund-Datenverarbeitung des UC ist

dringend notwendig. Eine Bildung des Nutzer-Bewusstseins darüber, dass elektronische Fingerabdrücke sich nur schwierig wieder zurückholen lassen, kann erst entstehen wenn unsichtbare, ubiquitäre Datenverarbeitung sichtbar wird. Der Bundesdatenschutzbeauftragte Peter Schaar hält insbesondere die Intransparenz von UC und die Profilbildung durch Verdichtungen von Informationen für problematisch: *„[...] kann die Verknüpfung unterschiedlichster Informationen dazu führen, [...] sehr, sehr sensible Informationen über diese Person zu gewinnen: Wenn man das Surfverhalten auswertet, wenn man den Klickstream erfassen kann, wenn man den Inhalt von E-Mails erfassen kann, wenn man den Terminkalender heranzieht. [...] Das man alles Mögliche in die Welt einer Infrastruktur integriert und dabei alle möglichen Informationen, die an unterschiedlicher Stelle angefallen sind zusammenführt [...]"* (Schaar, 2012 B, Frage 10). Eine Zentralisierung verschiedenster Nutzerdaten ist vor allem dann nicht wünschenswert, wenn sie gegen den Nutzer verwendet wird. Sobald Institutionen wie z.B. die Schufa Zugriff und Auswertungsmöglichkeiten auf Facebook-Daten erhalten und diese Daten zur Bonitätsprüfung herangezogen werden, liegt eine Zweckentfremdung vor, denn *„aus dem Schufa-Durchschnittswert der Freunde ließen sich dann, bei einem genügend großen Datensatz, womöglich statistische Rückschlüsse über die Kreditwürdigkeit eines bestimmten Nutzers ziehen"*. (Horchert/ Reißmann/ Stöcker, 2012).

Die Vorteile der ubiquitären Datenverarbeitung, wie z.B. die stete und ortsunabhängige Verfügbarkeit von Computerunterstützung, die nur eine minimale Nutzer-Aufmerksamkeit fordert (calm computing), führen auch zu einer erheblichen Datenmenge. Deren Auswertung ermöglicht die Erstellung lückenloser Verhaltensprofile (Taucis, 2006). Der Nutzer erhält zwar einen Mehrwert dadurch, dass eine automatische Abwicklung standardisierter Abläufe nach Nutzerpräferenzen geschieht, jedoch bedeutet die Tatsache, dass die direkte Nutzerinteraktion nicht mehr gefordert wird, einen erheblichen Kontrollverlust über die eigenen Daten.

Während der Diskurs-Begründer Mark Weiser an einen positiven Effekt und die Rückkehr des „Menschlichen" in die digitale Welt glaubt, *„Machines that fit the human environment instead of forcing humans to enter theirs will make using a computer as refreshing as taking a walk in the woods."* (Weiser, 1991) sieht die Seite der Medienschaffenden heutzutage eher eine gegensätzliche Entwicklung. Der

Video-Essay „Neue Nähe“ der Berliner Axel Springer Akademie stellt sozialkritische Fragen: *„Ersetzen Glasfasern Nervenfasern? Ist die Gesellschaft eine die zwar den Kontakt sucht, aber Berührungsängste hat?“* (Vukovic, 2011).

Laut der Taucis-Studie von 2006 erwarten wir von unseren elektronischen Wegbegleitern ein menschen-ähnliches Verhalten: *„Alltagsgegenstände bekommen so die zusätzliche Eigenschaft, sich entsprechend wahrgenommener Umgebungsvariablen zu verhalten’“* (Taucis, 2006, S.27). Jedoch befreit uns das Verhalten unserer elektronischen Gefährten nicht davon uns selbst verantwortungsbewusst zu verhalten und unsere eigenen Daten zu kontrollieren, worauf Datenschützer wie Thilo Weichert (Landesbeauftragter für Datenschutz Schleswig-Holstein) nicht müde werden zu verweisen: *„Es müsse eine neue Verantwortungsethik her. Rechtliche und tatsächliche Verantwortung gingen nicht immer zusammen. . […] ‚Beschränkung der Meinungsfreiheit im Netz, systematische Überwachung und informationelle Ausbeutung der Nutzenden’ seien allgegenwärtig, sagte Weichert.“* (Höver, 2011).

2.3 Ökonomie der Aufmerksamkeit und „linguistic communities“

1998 verfasste der Geisteswissenschaftler und Ökonom Georg Franck einen Essay mit dem Titel „Ökonomie der Aufmerksamkeit“. In diesem Werk nimmt er anstelle der Individualziele an, dass jeder Mensch dem natürlichen Anreiz nach Anerkennung und Aufmerksamkeit zu streben, folgt. Begründen tut er diese Hypothese mit dem Vorhandensein des Phänomens der Intersubjektivität (Franck, 1998, S.19). Er ökonomisiert das ureigene menschliche Bedürfnis und macht „Aufmerksamkeit“ zu einer Währung, worauf Kapitel 2.2 noch näher eingehen wird.

Der Medientheoretiker Norbert Bolz sieht „Aufmerksamkeit“ eher als ein Gut auf einem Markt, der von den Medien gesteuert wird: *„Die Massenmedien regulieren diesen Markt für Achtung und Aufmerksamkeit“* (Bolz, 1999, S.17). Geht man allerdings von einem Markt der „Aufmerksamkeit“ aus, so wird menschliches Handeln stets auch in anderen Währungen bemessen. Der Ökonom und Philosoph Birger P. Priddat beschrieb im Jahr 2000 in seinem Essay *„moral hybrids - Skizze zu einer Theorie moralischen Konsums“* die Auswirkungen moralischen Konsums auf

Märkte: *„ [...] Moral wird dann zu einer Kommunikations-Währung, wegen ihres hohen Aufmerksamkeitswertes. [...] und es scheint rational zu sein, sich der Moral anzuschließen, die aktuell besonders kommuniziert wird. Sie hat die geringsten Reputationskosten.“* (Priddat, 2000). Übertragen auf aktuelle Web 2.0 - Phänomene wie z.B. dem Fall von Ariane Friedrich[3] bedeutet dies, dass der Aufmerksamkeits-Wert von Beiträgen in Sozialen Netzwerken gerade dann besonders hoch ist, wenn wir moralisieren (siehe auch: Bolz, 1999, S.16). Priddat meint sogar wir sollten Moral weniger als individuelle Eigenschaft begreifen, sondern als *„eine Eigenschaft von 'linguistic communities' auffassen, die die Zugehörigkeit zur Sprachspielgemeinschaften markiert, dann ist der Kommunikationswert der Moral höher zu gewichten als die individuelle Überzeugung“*. (Priddat, 2000). Er versteht den Prozess des Erlangens einer Überzeugung als kommunikativen Austausch, durch die Partizipation in einer „lingusitic community“. Priddat bemerkt in diesem Zusammenhang außerdem: *„Man mag es - als moralischer Mensch - als amoralisch empfinden, dass die Geltung von Moral an ihre Wirkung geknüpft wird, d.h. an ihre Effektivität.“* Aber um genau diese Effektivität handelt es sich kongruent in Sozialen Netzwerken, durch die Partizipation an und in einer „linguistic community“, misst die Anzahl der Kommentare und „Likes“ unserer preisgegebenen Äußerungen die Effektivität und die Intensität der uns entgegengebrachten Aufmerksamkeit. Je moralisierender wir uns innerhalb unseres Netzwerks äußern, desto anknüpfungsfreudiger ist unser Publikum und unser Lohn ist der höhere Grad an Aufmerksamkeit.

3 Analyse der Entstehung von Facebook und netzwerkökonomischer Anreize

3.1 Neurologischer Hintergrund der Selbstdarstellung in Sozialen Netzwerken nach Tamir

Mark Zuckerberg studierte Informatik und Psychologie. Welche Bedeutung seine Informatik-Kenntnisse für die Gründung des Sozialen Netzwerks gehabt haben ist

[3] Die Hochspringerin Ariane Friedrich erhielt via Facebook das Foto eines Stalkers, auf dem sein Genital abgebildet war. Als Reaktion darauf veröffentlichte sie auf ihrer Facebook-Seite das Foto inklusive Vornamen, Nachnamen und den Wohnort des mutmaßlichen Stalkers. Für diese Aktion stand sie in der Medien-Kritik und löschte schließlich ihr Facebook-Profil. Die Affäre eskalierte bis zur staatsanwaltschaftlichen Untersuchung. (Sueddeutsche, 2012 A).

angesichts des technischen Know Hows der ersten Website-Entwürfe offensichtlich. Aber welches psychologische Know How ist in die Facebook-Gründung mit eingeflossen? Was sind die psychologischen Beweggründe einer Social Community im Internet beizutreten? Eine Idee davon welcher neurologische Hintergrund hinter der „extremen Solidarität unserer Spezies“ steckt, publizierte Harvard-Hirnforscherin Diana Tamir mir ihrem Forschungsteam erst jüngst, im Februar 2012 (Tamir/ Mitchell, 2012).

Das menschliche Selbst ist Wissenschaftlern in vielerlei Hinsicht intransparent und in seiner Komplexität nicht greifbar. Vor allem die menschliche exzentrische Positionalität (Plessner, 2000) und sein Bedürfnis sich anderen Menschen mitzuteilen ist bislang empirisch kaum untersucht worden. Mutmaßungen darüber was den Menschen dazu antreibt gibt es viele. Das prickelnde Gefühl vor Publikum zu stehen, die Erwartungshaltung durch Selbstoffenbarung eine Gegenleistung zu erhalten, sogar die Möglichkeit ein Tabu zu brechen werden als Motivationen für die Darstellung des Selbst gegenüber anderen identifiziert (Collins/Miller, 1994). Als weitere Motive für die Öffnung des Selbst gegenüber anderen gelten u.a. die Vorzüge persönlichen Wohlergehens, die ansteigende Zuneigung zwischen Beziehungspartnern, die Erzeugung von sozialen Bindungen und Allianzen, sowie das Auslösen von Reaktionen Anderer (Tamir/ Mitchell, 2012). Dies alles sind der Kooperation und Gemeinschaftlichkeit dienende Motive. Außerdem werden jedoch neben der Kooperation auch Motive für den Wissenstransfer zwischen Individuen genannt. Dazu zählt neben der Erlangung von Wissen über sich selbst (Selbstreflexion) auch die Vermeidung der Selbstaneignung von Wissen, welches andere längst erlangt haben (Tamir/ Mitchell, 2012).

Aus diesem Grund hat sich Diana Tamir der empirischen Untersuchung der Selbstdarstellung in Sozialen Netzwerken gewidmet und herausgefunden, dass Selbstdarstellung, im Sinne des Mitteilens von persönlichen Gedanken, Empfindungen und Überzeugungen an Dritte, das Belohnungszentrum im Gehirn (mesolimbisches Dopamin-System) anspricht.

Seine Gedanken und sich selbst Anderen mitzuteilen erzeugt eine stark ausgeprägte intrinsische Motivation. Tamir fand heraus, dass 30-40% menschlicher Gespräche sich um die Weitergabe persönlicher und subjektiver Erfahrungen an Andere drehen. Das Belohnungszentrum des Gehirns, die Hirnregion die auch für die Ausschüttung des Glückshormons Dopamin verantwortlich ist, ist bei dem Teilen eigener, subjektiver Empfindungen und Meinungen mit Anderen aktiv. Dies ist eine

Eigenschaft die Spezies-spezifisch ist und die wir nicht mit den Primaten teilen. Das Belohnungszentrum im Gehirn wird beispielsweise immer dann aktiv, wenn wir (Primaten wie Menschen) gutes Essen genießen, oder sekundäre Belohnungen erhalten z.B. Geld oder Spielzeug. Im Gegensatz zu Primaten jedoch ist das Belohnungszentrum des Menschen ebenfalls dann aktiv, wenn wir eine soziale Anerkennung erfahren. Dies geschieht, wenn wir z.B. bemerken, dass jemand anderes unsere Meinung teilt, unseren Humor versteht, oder die Aussicht auf Bestätigung der eigenen sexuellen Attraktivität durch das andere Geschlecht besteht (Tamir/ Mitchell, 2012).

So kann ein unmittelbar nach einem Erlebnis geposteter Facebook- oder Twitter-Eintrag „*in derselben Hirnregion Befriedigung auslösen, wie Sex oder gutes Essen*“ (PNAS, 2012). Die Selbstreferenz des Menschen ist derart ausgeprägt, dass er bereit ist Geld zu zahlen, um etwas über sich selbst preisgeben zu können. Vorangegangene Studien hatten ergeben, dass auch Bilder des anderen Geschlechts den Anreiz zur Selbstdarstellung massiv erhöhen können. Tamirs Hypothese, dass der menschliche Drang zur Selbstdarstellung einen direkten intrinsischen Mehrwert darstellt, hat sich bestätigt. Sie beschreibt die Veräußerung unseres Innersten als „*Extreme Solidarität unserer Spezies*“ (Tamir/ Mitchell, 2012) und diese tritt in Sozialen Netzwerken ganz besonders deutlich zum Vorschein.

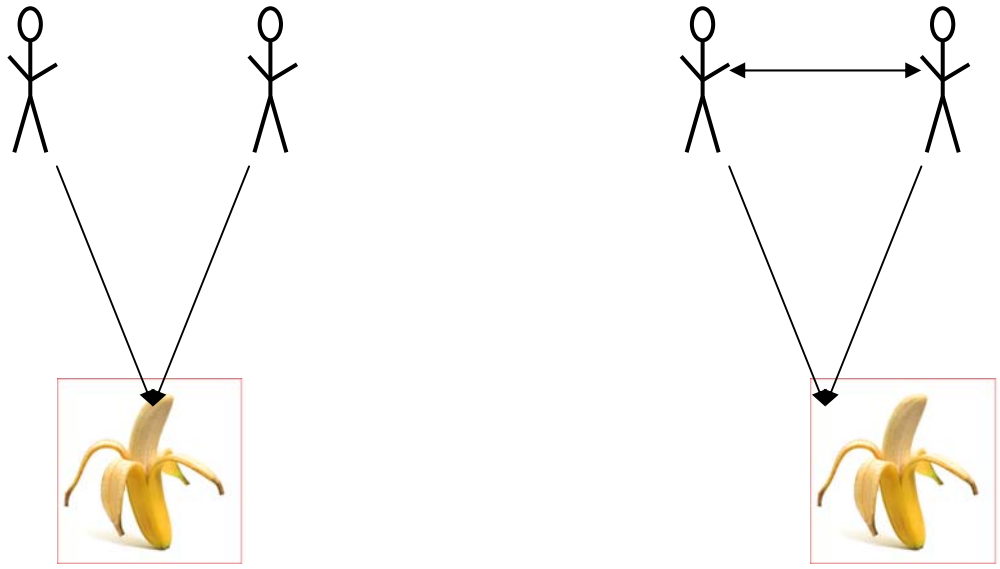
Angelehnt ist Tamirs Gedanke an eine spezifische Besonderheit unserer Spezies an eine Entdeckung des amerikanischen Anthropologen und Verhaltensforschers **Michael Tomasello**. Er entdeckte, dass ein zwischenmenschliches Selbst- und Weltverhältnis durch einen speziellen Sozialisierungsprozess menschlicher Kinder ausgebildet wird. Tomasellos Leitthese besagt, dass eine **besondere Form der soziokulturellen Interaktion**, innerhalb der Organisation menschlicher Gemeinschaft, zu der spezifischen Form menschlicher Kognition führt. Tomasello entdeckte, dass die geistige Fähigkeit des Menschen Aufmerksamkeit gemeinsam zu teilen menschliche Identität, ebenso wie die sprachliche Symbolverwendung bedingt. Er prägte mit dieser Entdeckung den Begriff der **joint attention (gemeinsame Aufmerksamkeit)**. Die joint attention ist vor allem durch die Intentionalität menschlichen Agierens charakterisiert. Innerhalb einer adaptiven Umgebung (menschliche Gemeinschaft), entwickelte sich menschliche Kognition phylogenetisch (Tomasello, 2002).

In Differenz zu Tieren, selbst zu Primaten, erkennt der Mensch andere Artgenossen als intentionale Wesen. Das menschliche Kind erkennt via Beobachtung Anderer,

dass Andere wie es selbst sind. Das Kind erkennt deren intentionales und geistvolles Handeln. Daraus ergibt sich die menschliche Möglichkeit sich über gemeinsame Aufmerksamkeit bewusst zu werden. Im Unterschied zu einer geteilten Aufmerksamkeit (zwei Wesen beobachten ein Objekt z.B. Nahrung) ist die gemeinsame Aufmerksamkeit eine trianguläre Beziehung zwischen Objekt und den beiden Individuen. Durch Blickwechsel wird ein gegenseitiges Interesse am Objekt bekundet.

Abbildung 2 „Blickwechsel geteilte / gemeinsame Aufmerksamkeit“ (Quelle: Forkefeld, 2009, S.16):

Geteilte Aufmerksamkeit: **Gemeinsame Aufmerksamkeit:**



Ein weiterer wichtiger von Tomasello geprägter Begriff, auf den sich Tamir bezieht, ist die sog. **Neunmonatsrevolution**. Erst ab einem ungefähren Lebensalter von 9 Monaten ist es Menschenkindern möglich gemeinsame Aufmerksamkeit **zu erleben.** Ein Katalysator für diese Fähigkeit ist die Sprache, denn sie ermöglicht das Erkennen der Vernunftbegabung Anderer und führt gleichzeitig zur Bildung eines Selbstverständnisses (Tomasello, 2012).

Eine Bestätigung für Tomasellos und Tamirs Ansatz findet sich auch in der Theorie des niederländischen Verhaltensforschers Frans de Waal. Er geht davon aus, dass der Mensch sich im Wesentlichen über seine eigene Identität und die Abgrenzung dieser zu fremden Identitäten definiert. Die eigene Identität jedoch wird gleichermaßen aus

internen wie auch aus externen Zuschreibungen Dritter konstruiert. Eine große Rolle spielen daher die Imaginationsformen des Menschen. Das Erkennen von Handlungsabsichten ist eine solche Imaginationsform, ebenso wie planendes und Zukunft antizipierendes Denken oder das Erkennen vorausschauenden Denkens bei Anderen (de Waal, 2008). Diese Fähigkeit zur Reflexion bezeichnet de Waal auch als die Errungenschaft einer speziellen Form der Intersubjektivität. Der amerikanische Pragmatiker Richard Rorty geht von einem menschlichen Aktivismus aus: Der Mensch sucht sich seinen Zugang zur Welt durch sein eigenes Handeln. Der Austausch von Information, Ideen, Idealen und Gründen ist dabei sein wichtigstes Werkzeug. Je mehr der Mensch versucht über die Welt zu erfahren, je mehr er versucht zu erkennen, desto stärker ist er schließlich auf sich selbst zurückgeworfen und lernt dabei über sich selbst (Rorty, 1992).

3.2 Die Entstehung von Facebook

Was ist Facebook? Die Facebook-Website, die ursprünglich „thefacebook“ hieß, erschien erstmalig am 04. Februar 2004 an der amerikanischen Universität Harvard. Harvard-Student und Hacker Mark Zuckerberg plante zunächst als studentische Spielerei ein soziales Harvard-internes Netzwerk mit den Profilen seiner Mitstudenten und Mitbewohner auf dem Harvard-Campus anzulegen. Die anfängliche Nutzungsmotivation von Zuckerbergs Publikum in Harvard war weder Macht noch Geld oder Reputation, sondern Sex (Baloun, 2007, S. 42). Jeder angemeldete Nutzer verfügte über eine eigene Profilseite mit Foto, einer Liste persönlicher Attribute und einer Liste von Freunden. Angaben zu Geschlecht, Beziehungsstatus und die Wahloption „Interessiert an...“ ermöglichten zu erkennen, wer von den Mitstudierenden zu den Marktteilnehmern gehörte und wer nicht. Facebook wurde zu einer Angebots- und Nachfrage-Plattform genährt durch horizontale Motivationen. Diese Anreizstruktur lockte innerhalb der ersten drei Wochen über 6.000 Harvard-Studierende, sich bei „thefacebook“ zu registrieren. Da es sich um ein exklusives Harvard-Netzwerk handelte und im Wintersemester 2004/2005 exakt 19.731 Studierende immatrikuliert waren (Harvard Online Factbook, 2004/2005), stieg die Mitgliederanzahl binnen eines Monats auf mehr als 30% aller Harvard-Studierenden (Baloun, 2007, S. 43).

Heute sind weltweit 838.384.720 Facebook-Nutzer angemeldet (Stand 02.04.2012, Allfacebook Userdata) im Vergleich zum Vorjahr sind 30.684.00 Nutzer hinzu gekommen, dies bedeutet einen Nutzerzuwachs von 3,66%. Zwar treffen diese

Zahlen zunächst keine Aussage über die aktive Facebook-Nutzung, jedoch deutet eine im Dezember 2011 erschienene Studie des Firewall Herstellers Palo Alto Networks auf eine weitere Zunahme der aktiven Nutzung von Sozialen Netzwerken hin. Die aktive Nutzung von Anwendungen Sozialer Netzwerke, gemessen an der Nutzung von Desktop-Anwendungen, Facebook-Apps, Postings, social-plugins und Spielen hat sich laut Aussage des Firewall-Herstellers von Oktober 2010 bis Dezember 2011 von 9% auf 28% verdreifacht (Palo Alto Networks Analysis, Dezember 2011). Grafiken...

Prognosen, ob die Facebook-Nutzung noch im Jahre 2011weiteres Wachstum generieren kann sind kontrovers.

3.3 Netzwerkökonomische Anreize in Sozialen Netzwerken: Facebook

Dieser Kapitelabschnitt beantwortet die Frage welche Anreize Social Media Nutzer dazu bewegen sich eine Internet-Identität zuzulegen. Um zu einer Analyse der Anreizstrukturen Facebooks zu gelangen, soll zunächst einmal der in dieser Arbeit vorherrschende Anreiz-Begriff festgelegt werden. Es ist ein organisationstheoretischer Begriff, angelehnt an die Definition von Frese. Er definiert Anreize in Organisationen wie folgt: *„Anreize sind von der Organisation gewährte materielle oder immaterielle Vergütungen für die Bereitschaft einer Person, in einer Organisation als Mitglied einzutreten und nach Annahme der Mitgliedschaft individuelle Beiträge in Form von Zeit, Energie oder anderen Ressourcen zur Realisation des Unternehmensziels zu leisten.“* (Frese, 2008). Diese Definition entzieht sich bewusst der voreiligen Ökonomisierung und schließt sowohl materielle wie auch immaterielle Güter ein, was bei der Betrachtung eines Sozialen Netzwerks wie Facebook eine wesentliche Prämisse ist. Freses interessanter Ansatz ist jedoch auf seine Validität zu prüfen, denn ob die Mitgliedschaft bei Facebook als Mitgliedschaft in einer Organisation zu interpretieren ist, bleibt offen. Nach Luhmann sind Organisationen Entscheidungssysteme – nach dieser Definition ist Facebook sicherlich keine Organisation (Luhmann, 2011).

Dennoch lassen sich in Sozialen Netzwerken interessante Anreizstrukturen analysieren. Im Falle Facebook’s lassen sich je nach Bedürfnis- und Präferenz-Lage drei unterschiedliche Anreizstrukturen der Nutzerseite zur Betätigung in Sozialen Netzwerken identifizieren. Die Betreiber-Anreize werden in Kapitel 2.3 näher erläutert. Als Nutzertypen lassen sich **Privatnutzer, staatliche Stellen und Unternehmen** charakterisieren. Alle drei Nutzertypen unterliegen spezifischen Anreizen und Bedürfnissen.

Privatnutzer: Welche Vorteile gewinnen private Social Network Nutzer durch die Partizipation im Netz? Das zunächst offensichtlichste Motiv der Nutzer ist es eine **Vereinfachung durch das so genannte Unified Messaging**[4], und somit eine **Erleichterung der eigenen Arbeitsorganisation und des Wissenstransfers**, zu erlangen. Axel E. Fischer, er ist Bundestagsmitglied und zugleich Vorsitzender der Enquete-Kommission Internet und Digitale Gesellschaft, erkennt folgende Vorteile: *„**Vereinfachte Kommunikation**, **schnellerer Zugang zu Information**, **neue Dienstleistungen** sind nur einige Aspekte, die unsere derzeitige Entwicklung in das digitale Zeitalter kennzeichnen. Wie jedes Ding haben auch die vielfältigen Neuerungen in diesem Zusammenhang zwei Seiten: **Einfacherer Zugang zu digitalisierten Musikwerken** erfreut jeden Einzelnen. Wenn damit jedoch im Rahmen einer Kostenloskultur z.B. durch illegale Kopien die Entlohnung von Kreativen in unserem Land nicht mehr in rechtlich vorgesehenem und gesellschaftlich erwünschtem Umfang sichergestellt ist, so müssen wir uns der Gefahr einer drohenden kulturelle Verarmung stellen.“* (Fischer 2012, Frage 1).

Fischer erwähnt zugleich auch die mit dem neuen Wissens- und Kommunikationskanal einhergehenden Gefahren, wie die **Verletzung von Urheberrechten und die Entstehung einer „Kostenlos-Kultur“**, was aber treibt die Nutzer dennoch dazu Ihre Werke geistigen Eigentums öffentlich für Jedermann und ungeschützt in Sozialen Netzwerken zu publizieren und zu verbreiten? Diese Frage lässt einen weiteren Rückschluss auf die Nutzermotivation zu.

Das Hauptanliegen des Privatnutzers ist es demnach die **Anerkennung und Aufmerksamkeit durch Andere** zu erlangen, denn „*Die Rolle, die wir im anderen Bewusstsein spielen ist Bestandteil unseres Selbstbildes.“* (Franck, 1998, S. 24) Franck ist der Auffassung, dass die eigene Identität sich gleichermaßen aus Selbst- und Fremdzuschreibung ergibt, denn eines der größten ungeklärten Rätsel der Anthropologie ist das Problem der Intersubjektivität, also das Erkennen des Selbst in anderen. **Die Intersubjektivität stellt gleichermaßen die Basis für jegliche menschliche Interaktion dar, sei es für kommunikativen Austausch oder für ökonomisches Handeln**. *„Die Aufmerksamkeit anderer Menschen ist die unwiderstehlichste aller Drogen. Ihr Bezug sticht jedes andere Einkommen aus.*

[4] Unified Messaging meint das Vorhandensein einer einheitlichen Benutzeroberfläche mit Zugriff auf z.B. E-Mail, Sprachnachrichten, SMS, Bilderdienste usw., es bezeichnet eine unkomplizierte all-in-one-Lösung.

Darum steht der Ruhm über der Macht, darum verblasst der Reichtum neben der Prominenz.“ (Franck, 1998). **Das Bedürfnis neben der realen Identität noch eine virtuelle Identität im Internet zu pflegen** und **einen größeren Freundeskreis zu unterhalten** als es in der Realität möglich wäre, ist ein starker Anreiz. Das Teilen privater Fotos, Videos, Meilensteine und Nachrichten in Sozialen Netzwerken scheint durch den menschlichen Urantrieb das „Leben teilen zu wollen“ manifestiert (vgl. Kapitel 3.5). Ob es dabei vordergründig um die Partnersuche und das „genetische Teilen“ oder um die „territoriale Jagd und Eroberung“ im gesellschaftlichen Sinne geht, ist je nach Persönlichkeitsstruktur und Lebenssituation der Nutzer different. **Als Beobachter der hohen Varianz von verschiedensten Attitüden in sozialen Netzwerken, kann man diese zunehmend als „designed identities“ bezeichnen.**

Auch Axel E. Fischer stellt eine Differenz zwischen virtueller und realer Öffentlichkeit fest: *„Handelnde Akteure, geltende Normen und andere Formen der Interaktion unterscheiden die virtuelle von der realen Öffentlichkeit. Eine verändert wahrgenommene Umgebung ändert die Verhaltensweisen der Nutzer im Internet. Virtuelle und reale Öffentlichkeit beeinflussen sich gegenseitig und wirken auf die Nutzer ein.“* (Fischer, 2012, Frage 2). Mit dieser Feststellung meint Fischer nicht nur den mittlerweile schwindenden Übergang zwischen Privatleben und Berufsleben, sondern auch und vor allem eine immer geringer werdende Hemmschwelle gegenüber der Würde Anderer in der virtuellen Kommunikation. So forderte Fischer im November 2010 ein Vermummungsverbot im Internet auf seiner Facebook-Seite *„Wir brauchen ein „Vermummungsverbot im Internet“. Es kann nicht sein, dass sich viele Bürger in Foren oder anderen Einrichtungen des Netzes hinter selbstgewählten Pseudonymen verstecken und sich so vermeintlich jeglicher Verantwortung für Äußerungen und Verhalten entziehen.“* (Fischer, 2012 B) Wenn Fischer mit der Klarnamen-Nennung im Internet gleichzeitig eine Sicherstellung der Übereinstimmung von realer und virtueller Identität fordert, ist dies ein Verweis darauf, dass sich aus Nutzer-Sicht ein entscheidender Vorteil aus der Teilnahme in sozialen Netzwerken ergibt, nämlich der, in variierende Rollen schlüpfen zu können, d.h. **das virtuelle Ich hat eine gesellschaftliche escape- und Entlastungsfunktion.** In der Medienpsychologie wird das Motiv eines Medienrezipienten seine individuellen Bedürfnisse auf die Medien zu projizieren **„Eskapismus“** genannt.

Dabei kann es sich sowohl um **affektive Bedürfnisse**, wie auch **kognitive Bedürfnisse** (Streben nach Wissen) handeln. Die Medienwelt erlaubt dem Rezipienten eine Ablenkung von Alltagsproblemen, Verpflichtungen und Regeln und eine damit einhergehende kurzzeitige Flucht (Katz / Foulkes, 1962).

Fazit: Es können **zwei Anreiz-Motivationsfelder** der Nutzer voneinander unterschieden werden:

1.) Der faktische, unmittelbare und zeitlich spürbare Nutzen, der **haptische Nutzen:**

- Reduktion von Komplexität

- Vereinfachung der Arbeitsorganisation

- Vereinfachung des Wissenstransfers

- Vereinfachung der Kommunikation

- Vereinfachung des Zugangs zu Unterhaltung: Literatur, Musik, Videos, etc.

2.) Der gesellschaftliche und nicht messbare Nutzen, der **Identität bildende Nutzen:**

- Anerkennung und Aufmerksamkeit durch Andere

- Bedürfnis neben der realen Identität noch eine virtuelle Identität zu pflegen

- Escape- und Entlastungsfunktion durch ein virtuelles Ich

- Vergrößertes Netzwerk z.B. Freundes – und Teilnehmerkreis für das eigene Handeln

Das zweite Motivationsfeld (der Identität bildende Nutzen) lässt sich der sich wandelnden Motivation der Internetnutzung aus Kapitel 1.3 zuordnen. Die eigene Identität und das Ansehen, welches es genießt, kann schrittweise monetarisiert werden, unterstellt man eine Kausalität zwischen Attraktivität und Sexappeal eines Individuums, daraus resultierender zunehmender Macht und dadurch entstehenden höheren Verdienst durch ökonomischen Erfolg (Franck, 2008).

Staatliche Stelle:

Dem Staat geht es weniger um das Bilden einer Identität, als um eine Vereinfachung des Administrationsapparates. Anstatt einen höheren Verdienst anzustreben, ist die

Verringerung von Transaktionskosten ein wesentliches Ziel staatlicher Social Media Nutzung.

Während die Nutzeranreize Identitäts-, Beziehungs- und Informationsmanagement miteinander vereinen (LfM Nordrhein-Westfalen, 2009, S. 3) liegt der Fokus des staatlichen Interesses an Sozialen Netzwerken eher auf dem **Informationsmanagement** und der **Kriminalitäts-Prävention**. Auch staatliche Institutionen wie Sicherheitsbehörden oder die Polizei nutzen Soziale Netzwerke für die **Aufklärung von Verbrechen**, **Vermisstenmeldungen oder Rasterfahndungen**. Die neuen Möglichkeiten zur Datenerfassung, könnten künftig aber auch unter dem Aspekt der **Telekommunikationsüberwachung**, der **Konsumüberwachung** oder der **Überwachung von Finanztransaktionen** von staatlicher Seite betrachtet werden. Durch die Datenanalyse der Social Media Nutzung ist es möglich neben der Verbrechensbekämpfung auch die **Aufdeckung von Steuerdelikten** anzustreben, da sich Standorte und Nutzerverhalten von potentiellen Tätern besser verfolgen lassen. Die Frage, ob das staatliche Interesse an der Social Media Nutzung proaktiv entsteht muss jedoch verneint werden. Das vermehrte Interesse des Staates an sozialen Netzen entsteht erst durch das bürgerliche Handeln. Ein staatliches Interesse ab ovo zu unterstellen wäre ein Irrtum.

Ist es möglich, dass Social Network Betreiber und werbetreibende Unternehmen gar nicht die einzigen Interessenten für die Social Media –Nutzerdaten sind? Auch der Staat könnte Vorteile in der freiwilligen Datenpreisgabe der Nutzer sehen. Wer also schützt den Nutzer davor, Opfer staatlicher Überwachung zu werden?

Dies liegt laut Auffassung des Bundesdatenschutzbeauftragen Peter Schaar beim Staat selbst. **Der Staat hat die Aufgabe selbst maßgeblich die Kapazitäten für Überwachung und Datenschutz festzulegen** (Lorenz, 2012). Schaar erkennt zudem, dass ein **Misstrauen zwischen staatlichen Institutionen, der Staatspolitik und den Bürgern** gibt. Daher sorgt er dafür, dass auch der Staat transparenter agiert und Daten preisgeben muss: *„Die Deutschen machen immer stärker von ihrem Recht auf Auskunft der Behörden Gebrauch. Im vergangenen Jahr wurden mehr als doppelt soviele Anträge auf Informationszugang gestellt“*, so lautete Schaars Zusammenfassung bei der Vorstellung seines Tätigkeitsberichts für die vergangenen zwei Jahre (Spiegel Online, 2012). Laut Aussage Schaars stieg die Anzahl von 1557

auf 3280 Anträge im Laufe des Jahres 2011. Schaar ist der Meinung, dass auch die Unterstützung durch Gerichte eine tragende Rolle bei der **Anwendung des Informationsfreiheitsgesetzes** in den Jahren 2010 und 2011 gespielt habe. Zweck dieses Gesetzes ist es Vorgehensweisen bei Datenanalyse und auch die Dauer und der Ort Datenhaltung gegenüber dem Bürger transparent zu kommunizieren. Die Erlangung einer **Political Awareness** gegenüber den Konsequenzen eines digital agierenden Bürgers, hält Schaar für essenziell.

Schaar weiß, dass eine Differenz zwischen der Datenerhebung in Sozialen Netzwerken und anderen Datenerhebungen erkennbar sein muss: *„In einem sozialen Netzwerk ist die Erwartung dass die Daten geschützt sind geringer, als wenn es sich um die Daten einer privaten Krankenversicherung handelt.“* (Schaar, 2012 B, Frage 4). Schaar erkennt in der Ausrichtung des aktuellen Deutschen Datenschutzes derzeit folgende Schwerpunkte (Schaar, 2012 B):

1.) Personen- und Identitätsschutz, sowie Wahrung der Persönlichkeitsrechte

2.) Vermeidung von Profilbildung

3.) Vermeidung von Monopolen

Auch der Ansatz der Mobbing-Vermeidung im Internet hat politische Vertreter gefunden. Bundestagspräsident Norbert Lammert ist der Meinung: *„Der Rechtsstaat muss sich auch im Internet behaupten.“* Er spricht sich gegen anonyme Beleidigungen im Netz aus, da diese zumeist in *„Aggressivität, Wortwahl und Tonlage die Grenzen überschreitet, die dieselben Leute auf der Straße für sich setzen würden“* (Spiegel, 2012 A, S.23).

Axel E. Fischer fordert sogar *„unmittelbar im Anschluss an das Ende der Enquete-Kommission ‚Internet und digitale Gesellschaft’ einen gleichnamigen Ausschuss im Deutschen Bundestag einzurichten.“* (Blogfraktion, 2012). Neben einer höheren Beteiligung der Bürger an politischen Prozessen durch das Internet verspricht sich Fischer außerdem einen *„funktionierenden Ordnungsrahmen für das Netz*“:

„Die Kontrolle über die weitere Verbreitung einmal freigegebener Informationen bzw. Daten im Internet entzieht sich weitgehend dem eigenen Einfluss. Ein "digitaler Radiergummi" zur allgemeinen Beförderung eines "Vergessens" im Internet würde aus heutiger Sicht Manches vereinfachen. Er kann jedoch im Zweifelsfall z.B.

juristisches Vorgehen gegen unrechtmäßige Nutzung von Daten im Zweifel nicht ersetzen.“ (Fischer, 2012 A, Frage 7).

Abschließend lässt sich feststellen, dass es u.a. ein Hauptanliegen des Staates ist, dem Bürger sein Selbstbestimmungsrecht über digitale Datenpreisgaben zurück zu geben.

Klassische Staatsinteressen sind ansonsten:

1.) Verbesserung des Informationsmanagements

2.) Kriminalitäts-Prävention und Aufklärung von Verbrechen

3.) Überwachung von Finanztransaktionen, sowie die Aufdeckung von Steuerdelikten.

4.)

Unternehmen:

Welche Interessen verfolgen Unternehmen bei der Nutzung Sozialer Netzwerke? Gemeint sind hier Unternehmen die auf sozialen Plattformen aktiv werden, im Gegensatz zu den Unternehmen die selber Soziale Netzwerke betreiben. Erstere nutzen offensichtlich die Multiplikator-Möglichkeiten zur **Umsatz- und Produktabsatzsteigerung**, bei der das Internet den Zugang zu neuen Kundengruppen eröffnet. Um sich eine Meinung über die Bestandskunden zu bilden, wird häufig das so genannte **„Targeting“** eingesetzt. Dabei handelt es sich um Mess

- und Marktforschungsmethoden, die bereits bestehende Kundenstrukturen analysieren. Bei diesem Verfahren werden keine personenbezogenen Daten gespeichert oder an Werbende weitergegeben. Analysen entstehen durch die Auswertung von **IP-Adressen und durch den Einsatz von Cookies**. Forschungsgemeinschaften bieten die Analyse - der auf diese Weise gesammelten statistischen Daten - den Unternehmen an. Im Gegensatz zum „Targeting“ wird beim **„Tracking“ (Nachverfolgung)** im Internet eine Aufzeichnung und Auswertung des Nutzerverhaltens vorgenommen. Unternehmen sind vor allem daran interessiert, die **Abbruchraten auf ihren Internetseiten nachzuvollziehen** und möglichst zu

minimieren. Auch die Klickpfade der Nutzer können einem Unternehmen wertvollen Einblick in die **Präferenzen der Kunden** bieten, z.B. darüber welche Produkte und Hersteller besonders stark nachgefragt werden. Das „Tracking“ bietet sogar Einblick in die vom Nutzer verwendete Software, so dass Webseiten gemäß den aktuell vorherrschenden Standards programmiert und optimiert werden können. Auf diesem Wege können z.B. **Bestellvorgänge** für Kunden **vereinfacht werden** (VPRT, 2011). An diesem Punkt stellt sich allerdings die Nutzen-Frage. Sind denn Unternehmen nicht vormals auch ohne „Targeting“ und „Tracking“ ausgekommen? Diese Frage berührt den **Kern des Say’schen Theorems**. Es besagt, dass bestimmte Angebote sich ihre Nachfrage selbst schaffen. Say erklärte die Möglichkeit dieses Verhaltens in seinem Aufsatz „Traité d'economie politique“ wie folgt: „*Wenn der Produzent die Arbeit an seinem Produkt beendet hat, ist er höchst bestrebt es sofort zu verkaufen, damit der Produktwert nicht sinkt. Nicht weniger bestrebt ist er, das daraus eingesetzte Geld zu verwenden, denn dessen Wert sinkt möglicherweise ebenfalls. Da die einzige Einsatzmöglichkeit für das Geld der Kauf anderer Produkte ist, öffnen die Umstände der Erschaffung eines Produktes einen Weg für andere Produkte.“* (Say, 1803). Wie groß der tatsächliche Nutzen der Unternehmen an den statistischen Erhebungen Sozialer Netzwerke ist, bleibt intransparent. Die Datenauswertung Sozialer Netzwerke schafft jedoch eine Möglichkeit zu einer Umsatzsteigerung in Unternehmen. Außerdem sind folgende weitere Vorteile für Unternehmen interessant:

1.) Verbessertes Personalmanagement: Eine **Effizienzsteigerung kann durch die Überwachung der Mitarbeiter** erreicht werden, wann z.B. nutzt der Mitarbeiter das Soziale Netzwerk innerhalb seiner Pausen oder außerhalb? Zudem kann die Präsenz von Unternehmen in Sozialen Netzwerken neue **Recruiting-Wege** eröffnen. Insbesondere die junge Zielgruppe ist besser online zu erreichen, als über Printmedien. Manche Unternehmen melden sogar eigene, geschützte Firmennetzwerke innerhalb sozialer Netzwerkstrukturen an. Diese können für **die Aufklärung und Kontrolle bei Compliance-Fällen** hilfreich sein, z.B. durch whistle-blowing-Systeme.

2.) Verbessertes Marketing: Durch die **Erstellung von Kundenprofilen** können Unternehmen besser auf die **Kundenbedürfnisse** eingehen und beispielsweise ihre Produkte und Leistungen dem Kundenwunsch entsprechend verbessern. Soziale

Netzwerke helfen hauptsächlich bei der **Identifikation von Kundenbedürfnissen**. Sie können aber auch bei der Kommunikation eines verbesserten Produkts und beim **Aussenden von Botschaften über Innovationen nutzen**, sobald ein Unternehmen via eines Netzwerks eine **„Brand Community“** generiert hat (Lüdicke, 2006, S.76 ff.).

3.) Besseres Daten- und Finanzmanagement: Soziale Netzwerke eröffnen vor allem neue Möglichkeiten zur **Datenerfassung, Datenweitergabe, Datenhaltung- und Verarbeitung**. Zudem bringen sie auch neue Methoden und Tools für **Finanztransaktionen** mit sich, z.B. **elektronische Zahlungsmethoden** wie PayPal etc. Auch die **Preis- und Informations-Recherche**, die z.B. für einen Benchmark notwendig ist, fällt durch die Teilnahme in Sozialen Netzwerken erheblich leichter.

4.) Bonitätsprüfung von Kunden:

Auch wenn die Möglichkeit Auskünfte über die **Zahlungsfähigkeit von Kunden** einzuholen wiederläufig zum Verbraucherdatenschutz ist, besteht dennoch die Möglichkeit Zahlungskraft und die **Dauer von Bestellung bis zur Rechnungsbegleichung** anhand der Online-Erhebungen nachzuvollziehen.

Das Spannungsverhältnis zwischen unternehmerischen Interessen und den Bedürfnissen der Nutzer sich im Internet geschützt fortbewegen zu können, bleibt durch das unternehmerische Kontrollbedürfnis erhalten.

3.4 Anreizstrukturen der Betreiber Sozialer Netzwerke

Die Betreiber Sozialer Netzwerke haben erkannt, dass die Nutzer einen Mehrwert erfahren, wenn möglichst viele Teilnehmer bei einem Sozialen Netzwerk mitmachen. Facebook zum Beispiel generiert allein durch seinen „Like“-Button Multiplikator-Effekte wie sie im realen Leben nur schwierig realisierbar sind. Höchstens die lokale Presse kann eine derartige Respons für ein Individuum erzeugen, welches keine Person des Öffentlichen Interesses ist (Bolz, 1999). **Neben der Schaffung eines gefühlten Mehrwerts für den User streben die Betreiber Sozialer Netzwerke danach, möglichst viele Nutzer-Daten zu akkumulieren**. Ist das dahinter stehende Geschäftsmodell der Betreiber auch zunächst unklar definiert, so ist doch das Ziel einer Datensammlung ein „Gut“ zu erzeugen, dass getauscht werden kann. Es entstehen direkte Vergütungsansätze zur Monetarisierung der Nutzerdaten, wie z.B. die Erstellung von Nutzerprofilen, um somit gezielte Werbung verkaufen zu können.

Zudem entstehen für die Betreiber aber auch indirekte Vergütungsansätze, bei denen „virtuelle Güter“ im Vordergrund stehen (Kurz/Rieger, 2011, S. 21). Bevor ein Soziales Netzwerk Nutzerprofile erstellen kann, geschieht eine Monetarisierung des Potentials des Netzwerks, bei dem weder ein Produkt noch ein realer Umsatz bewertet werden können. Oftmals engagieren sich Investoren frühzeitig pekuniär und orientieren sich an Klickraten und dem schwer verifizierbaren Grad der Aufmerksamkeit, den eine Webseite generiert (Kurz/Rieger, 2011, S. 20).

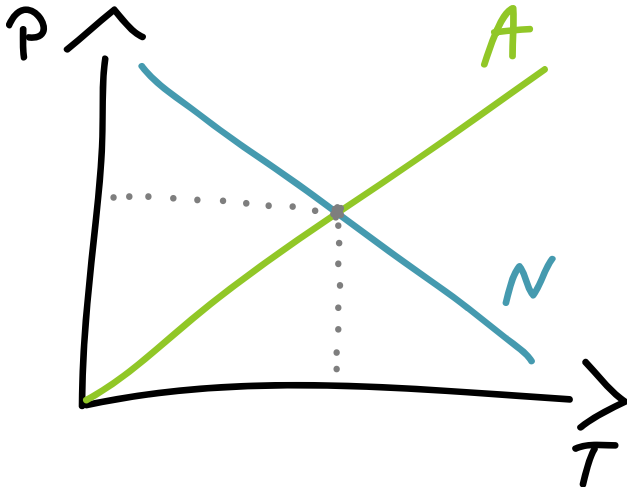
Das Geschäftsmodell von Sozialen Netzwerken wie Facebook ist jedoch instabil, denn es existiert ein Grenzpunkt, an dem genug Nutzer mitmachen, damit "gefühlt" alle drin sind - nach Überschreitung dieses Grenzpunktes nehmen alle teil. Die Instabilität dieses Konstrukts erklärt sich jedoch aus dem Prinzip der Freiwilligkeit der Teilnahme: Jedem Nutzer steht es offen auszutreten, sein Nutzer-Profil zu löschen und sich ganz abzumelden.

Netzwerkökonomisch bedeutet dies, dass sich der Punkt eines Datentransparenz-Optimums trotz der Netzwerkeffekte verlagert. Wenn Nutzer durch einen Austritt aus dem Sozialen Netzwerk für ausreichend Datenschutz sorgen, wird der optimale Punkt nicht erreicht. Es findet eine Selektion des positiven Risikos statt. Das Optimum der zufriedenen Nutzer liegt somit nicht bei "zu wenig Datenschutz".

Prognosen antizipieren einen Nutzer-Rückgang in Sozialen Netzwerken, denn auf Dauer sei die Zunahme von maßgeschneiderten Werbeanzeigen für Nutzer belastend und eine Schmälerung des Aufmerksamkeits-Mehrwerts (Baloun, 2012). Der Auffassung, dass ein Konflikt zwischen den Werbeinteressen der Betreiber und dem Privatsphäre-Bedürfnis der Nutzer besteht, ist auch der Bundesdatenschutzbeauftragte Peter Schaar:

„Bei diesen Interessen [...] - muss man dann fragen, wie groß ist das Interesse des Unternehmens an der Verwendung der Daten für Werbezwecke oder zum Zuspielen von bestimmten Informationen, also Targeting versus dem Interesse des Einzelnen alleine gelassen und nicht gestört zu werden, nicht Objekt der Datenverarbeitung Dritter zu sein.“ (Schaar, 2012 B, Frage 4)

Abbildung 3 „Datentransparenzoptimum“ (Quelle: selbst erstellt)



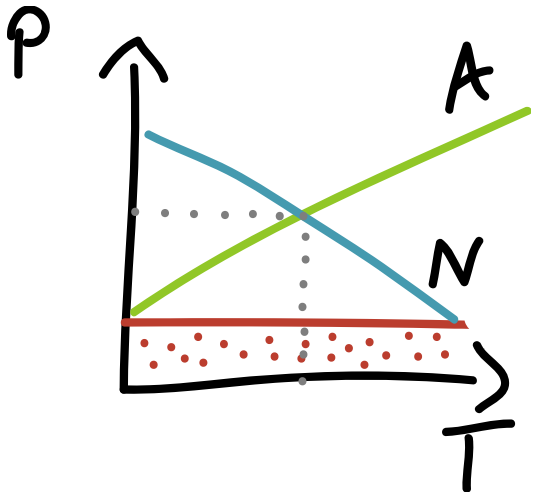
Das Spannungsverhältnis von Privatsphäre und Transparenz zeigt die obige Abbildung 3: Achse P zeigt die Privatsphäre, während Achse T die Transparenz darstellt. Kurve A ist die Anbieterseite, die hier den Betreiber eines Sozialen Netzwerks als Dienstanbieter meint. Kurve N ist die Nachfragekurve, die in diesem Zusammenhang die Nutzer skizziert. Verglichen mit einem regulären Marktmodell würde sich das Optimum der Nutzerdatentransparenz im Schnittpunkt beider Kurven finden (hier dargestellt durch die grauen Linien). Dies bedeutet je mehr Privatsphäre-Einstellungen möglich sind, desto mehr Nutzer vertrauen dem Netzwerk. Dies kollidiert jedoch mit dem Anbieter-Interesse, je mehr Privatsphäre-Einstellungen möglich sind, desto weniger Datentransparenz kann der Anbieter für sich und seine Werbekunden nutzen. Es muss also ein Optimum der Privatsphäre-Einstellungen geben, die dem sozialen Netzwerkbetreiber noch immer ausreichend Datentransparenz gewährt, um sein Geschäftsmodell aufrecht zu erhalten.

Diese wohlfahrtsökonomische Überlegung stößt jedoch dadurch an Ihre Grenzen, dass die Nutzer nicht dazu bereit sind bei einem bestimmten Grad der Öffentlichkeit ihrer Daten, oder bei einer übergroßen Menge an Werbung, weiterhin am Netzwerk teilzunehmen.

Daher wird ein Netzwerkangebot erst ab einem bestimmten Grad garantierter Privatsphäre von den Nutzern angenommen, hier dargestellt durch die rot-gepunktete Fläche in Abbildung 4. Ein Angebot unterhalb dieser Fläche wird von den Nutzern als zu werblich und unfair wahrgenommen. Bei Missfallen der Datensicherheit treten die Nutzer aus dem Netzwerk aus oder melden sich erst gar nicht an. Dadurch verschiebt sich das Datentransparenz-Optimum auf der Privatsphäre-Scala nach oben und landet bei „weniger Privatsphäre“ als das eigentliche Optimum die Abbildung 3

erwarten lassen würde (Talbot, 2012 und Schneider, 2007).

Abbildung 4 „Verschiebung Datentransparenzoptimum“ (Quelle: selbst erstellt)



Ein Beispiel hierfür ist das Scheitern von Google +, da ein maßgeblicher Grund der mangelnden Teilnahme ein fehlender Zusatznutzen und die hohe Werbefrequenz des Netzwerkes war (Fröhlich, 2011). Als weitere Erklärungen für das Scheitern von Google + muss jedoch auch die enorme Facebook-Präsenz verantwortlich gemacht werden, denn kaum jemand betreibt gleichzeitig zwei pflegeintensive soziale Netzwerke. Google + lieferte zunächst keinen erkennbaren Mehrwert gegenüber Facebook. Die Facebook-Nutzer vollzogen ein „Lock In“, schotteten sich geradezu vor neuen Angeboten ab. Ein Verhalten, welches Williamson in seiner sunk costs-Theorie näher betrachtet. Williamson geht vom Abbruch eines Investitionsprojektes aus, bei dem ein Verlust entsteht. Die ursprüngliche Investitionsauszahlung entspricht nicht der Höhe des Liquidationserlöses des neuen Projekts (Williamson, 1996). Im Falle von Google + ist dabei Zeit die beachtenswerte Währung.
Überdies muss natürlich die Differenz des Datenmarktes zu herkömmlichen Märkten mit berücksichtigt werden.

3.5 Besonderheiten des Datenmarkts

Der bereits in Kapitel 2.3 erwähnte Unterschied, dass es sich beim Datenmarkt um ein **virtuelles und kein haptisches Gut** handelt, ist insofern bedeutend, als dass Daten beliebig häufig vervielfältigt werden können, **ohne dass eine**

Abnutzungserscheinung oder eine Rivalität im Konsum entsteht. Daten sind eine Wissensressource, anders jedoch als bei Wissen in Form von Informationen ist Wissen in Form persönlicher Daten rechtlich geschützt. Der rechtliche Schutz (z.B. durch das Datenschutzgesetz und durch Urheberrechte) ist die einzige Limitierung, denn der technischen Verbreitung allein sind zunächst keine Grenzen gesetzt. So können Spiele und Apps beliebig oft heruntergeladen, gespeichert und verbreitet werden. Auf diese Besonderheiten des Datenmarktes verweist auch Peter Schaar: *„Der Datenmarkt unterscheidet sich natürlich in erster Linie dadurch von anderen Märkten, dass es sich um einen Markt mit virtuellen Produkten handelt. Insofern ist es so, dass die Daten nicht verschwinden, wenn Sie gedoppelt werden. Der Datengebrauch ist (das ist auch der Kern der Urheberrechtsdebatte) sofern keine Regulierung stattfindet, prinzipiell mit keinen Grenzkosten verbunden. Das ist natürlich der entscheidende Unterschied. Man kann jetzt über rechtliche Begrenzungen, siehe Urheberrecht, siehe Datenschutz, den Markt versuchen in ein konventionelles Raster einzufügen, was natürlich nicht immer so ganz einfach ist.“* (Schaar, 2012 B, Frage 5).

4 Problematisierung der divergierenden Social Networking Interessen

4.1 Datenschutzbestimmungen und Nutzungsbedingungen Facebooks

Es folgt nun eine Bestandsaufnahme über Facebook’s Datenschutz-Richtlinien 2012, da sich durch Abstimmungen im April und Mai 2012 in Deutschland einige Veränderungen ergaben, zeichnet sich eine gewisse Häufigkeit verschiedener Schwerpunkte ab. Hier eine Auswahl, der von der Öffentlichkeit am häufigsten diskutierten Themen, beginnend mit der Grundsatzfrage wer bei einem Sozialen Netzwerk eigentlich zur Verantwortung gezogen werden sollte:

Wer oder was ist Facebook?

Wer hat den größeren Anteil? Sind es die Betreiber oder die Nutzer? Die Nutzer zumindest sind den Betreibern (Facebook hat rund 2.200 Mitarbeiter weltweit[5]), rein numerisch überlegen. Jedoch sind die Nutzer keine organisierte Gemeinschaft, die

[5] Stand 2010, Quelle: www.statista.de

einen homogenen Rechtskörper formt. Im Gegenteil. Der einsame Einzelkämpfer, der seine Selbstverpflichtung und Eigenverantwortung wahrnimmt muss jedenfalls der Archetyp der Facebook-Betreiber gewesen sein. Die Datenschutzbestimmungen zu denen sich die Betreiber eines sozialen Netzwerks eigentlich bekennen sollten, werden im Falle Facebooks zu einem Verhaltenskodex für die Nutzer umformuliert. Die Nutzungsbedingungen übertragen z.B. die Verantwortung für die Sicherheit Facebooks gleichsam auf die Nutzer, was der Anfang von Abschnitt 3 zum Thema Sicherheit im Facebook-Impressum belegt: *„Wir bemühen uns nach besten Kräften, die Sicherheit von Facebook zu wahren, können diese jedoch nicht garantieren. Wir benötigen dazu deine Hilfe. Dies umfasst folgende Verpflichtungen:...“* (Facebook, 2011) Zu den weiteren Nutzungsbedingungen gehören zudem u.a. die Selbstverpflichtung das eigene Facebook-Profil nicht werblich z.B. für Spam zu nutzen, nicht rechtswidrig zu agieren oder rechtswidrige Inhalte zu veröffentlichen. Außerdem wird geboten wahrheitsgemäße Angaben über die eigenen Person zu machen und andere Nutzer respektvoll zu behandeln und sie weder zu schikanieren, noch zu tyrannisieren. Auch das Einwirken auf die Funktionsweise von Facebook ist untersagt, Viren hochladen oder zur Überlastung des Netzwerkes beitragen sind ebenso wenig gestattet, wie das Durchführen von *„irreführenden Handlungen“*. Der Nutzer verpflichtet sich zudem *„jegliche Verstöße gegen diese Erklärung weder zu unterstützen noch zu fördern“* (Facebook, 2011).

Die **Wichtigkeit der Privatsphäre** scheint bei immer mehr Facebook-Nutzern abzunehmen, diesen Schluss zumindest lässt die Entwicklung der zunehmenden Benutzung sozialer Netzwerke zu. Dennoch kann die Verallgemeinerung dieser Entwicklung und die Übertragung auf andere Lebensbereiche nicht ohne weiteres vorgenommen werden. Der **soziale Tausch** unterscheidet sich wesentlich von dem ökonomischen. **Die Währung des sozialen Tauschs ist Reziprozität**. Die vordergründige Motivation, das Anlegen eines eigenen Profils, um auch zu den Profilen anderer Zugang zu erhalten, reflektiert nicht das Geschäftsmodell Facebook’s. Dass sich ein Nutzer mit seinem Handeln zugleich zielgerichteter Werbung aussetzt, wird erst sekundär bedacht. Vielen Nutzern ist dieser Sachverhalt gar nicht bewusst (Jentzsch, 2012).

Ungeachtet der Kosten, nämlich der Preisgabe der persönlichen Daten, ist es ein Anliegen der Nutzer ihre Profile für eine **positive Selbstdarstellung** zu Nutzen.

Negative Aspekte der eigenen Persönlichkeit, z.B. die Preisgabe von sensiblen Informationen wie z.B. über Sucht oder Krankheiten, werden zumeist verschwiegen. (Jentzsch, 2012). Daher obliegt die Selektion der Netzwerkteilnehmer eindeutig Facebook. Jedoch sind die Einschränkungen der Teilnahme nicht so hoch wie erwartet.

Wer kann sich bei Facebook anmelden?

Nicht jeder kann sich bei Facebook anmelden, eine Beitrittsbedingung ist die Altersbeschränkung, dass nur Personen über 13 Jahre einen Facebook-Account anlegen dürfen. Zudem werden registrierte Sexualstraftäter von der Facebook-Nutzung ausgeschlossen, wie im Unterpunkt „Registrierung und Sicherheit“ der Konten vermerkt ist (Facebook, 2012 A). Gerüchten zu Folge überlegt Facebook, ob es künftig auch ein Angebot für Kinder unter 13 Jahren geben wird. Konten jüngerer Kinder sollten in diesem Fall mit denen ihrer Eltern verknüpft werden (Beiersmann, 2012).

Löschung des Facebook Kontos

Wer sein Facebook-Konto löschen möchte, hat **zwei verschiedene Wahlmöglichkeiten**:

1.) Das **Deaktivieren des Kontos** mit der Funktion „Konto deaktivieren“ (facebook.com/deactivate.php) bewirkt, dass das Facebook-Profil nicht mehr sichtbar ist. Die Daten bleiben jedoch gespeichert. Die E-Mail-Benachrichtigungen von Facebook müssen gesondert deaktiviert werden. Der Nutzer erhält dann keine weiteren E-Mails von Facebook. Jedoch ist es möglich zum Account zurückzukehren, indem man sich erneut einloggt. Die Funktion „Deaktiveren“ löscht den Account nicht, sondern sie friert ihn lediglich ein.

2.) Mit der Funktion **„Mein Konto löschen“** (facebook.com/help/delete_account) ist eine endgültige Löschung des Facebook-Kontos möglich. Diese Funktion ist unwiderruflich und alle gespeicherten Daten zu einem Profil sind nicht mehr via Facebook aufrufbar. Unklar bleibt jedoch, inwiefern diese Funktion auch eine Unauffindbarkeit in Suchmaschinen bewirkt. Meist sind hier noch Reste des eigenen Profile (z.B. das Profil-Foto) über längere Zeiträume recherchierbar.

Facebook wurde in der Vergangenheit dafür kritisiert, dass es diese beiden Deaktivierungsmöglichkeiten gut versteckt. Auch die Tatsache, dass Facebook zwei ähnliche, aber nicht identische Funktionen anbietet, seien höchst intransparent, so der Vorwurf (Stern, 2012).

Datenspeicherung

Seit der deutschen Abstimmung über die Facebook-Nutzungsbedingungen im Mai 2012 plante Facebook eine **verlängerte Datenspeicherung**, die es auch durchsetzte, da zu wenig Nutzer dagegen stimmten. *„Wir werden Daten so lange einbehalten, wie dies erforderlich ist, um sie den Nutzern und anderen Dienstleistungen zur Verfügung zu stellen. Diese umfassendere Verpflichtung gilt für alle Daten, die wir über Dich sammeln und erhalten, einschließlich Informationen von Werbetreibenden“* (Facebook, 2012 D). Bei diesem Zitat handelt es sich um eine Übersetzung aus dem Englischen. Unklar bleibt in diesem Abschnitt, was Facebook mit Dienstleistungen meint. Sind tatsächlich Facebook-Anwendungen und Apps gemeint, oder vielmehr andere Dienstleister? Der Zweck der verlängerten Datenspeicherung bleibt intransparent. Zuvor war eine Datenspeicherung von **180 Tagen** veranschlagt, diese Frist wurde nun ab 09. Juni 2012 auf **unbestimmte Zeit** verlängert (Focus, 2012).

Cookies

Wie genau die **Nutzeridentifizierung bei Facebook** von statten geht, war den meisten Nutzern bis jetzt weitestgehend unbekannt. Angeblich speichert Facebook die letzten drei besuchten Internetseiten, bevor der Nutzer sich bei Facebook anmeldet. Seit dem 26. Mai 2012 sind die neuen EU-Datenschutzregeln in Kraft getreten, die u.a. Werbetreibende und Betreiber sozialer Netzwerke dazu verpflichtet die Nutzer davon in Kenntnis zu setzen, wann und auf welchen Seiten Cookies eingesetzt werden (Pluta, 2012). **Cookies sind elektronische Datenkrümel**. Diese Datenkrümel werden von besuchten Internetseiten auf dem PC des Nutzers (im Browser) hinterlassen um den Nutzer identifizieren zu können. In seiner neuen deutschen Richtlinie bemüht sich Facebook erstmals seine Nutzer über die Verwendung sogenannter Cookies aufzuklären. Zu diesem Zweck hat Facebook Cookies in seinen neuen Richtlinien ausführlich erklärt: *„Cookies sind kleine Dateneinheiten, die wir auf deinem Computer, Handy oder anderen Geräten*

speichern. Pixel sind kleine Code-Blöcke auf Webseiten, die Dinge tun wie beispielsweise einem anderen Server die Messung der Besucher einer Webseite erlauben und die oft im Zusammenhang mit Cookies verwendet werden. Wir verwenden Technologien wie Cookies, Pixel und lokale Speicherung [...] um verschiedene Produkte und Dienste zur Verfügung zu stellen und zu verstehen." (Facebook Privacy, 2012 C). Facebook gibt an, die cookies u.a. für folgende Maßnahmen zu nutzen: *„[...] Werbeanzeigen zu schalten, zu verstehen und zu verbessern und [...] die Nutzung unserer Produkte und Dienstleistungen zu überwachen und zu verstehen; und dich, andere und Facebook zu schützen."* (Facebook Privacy, 2012 C). Facebook stellt die **werbliche Nutzung** klar heraus und spricht auch von einer **überwachenden Funktion zum Schutze des Nutzers**. Zuvor muss der Nutzer aber erst auf den Menüpunkt Datenverwendungsrichtlinien und den Unterpunkt „Cookies Pixel und andere Systemtechniken" klicken, um zu diesen Informationen zu gelangen.

Der „Like"- Button

In welcher Weise sich Facebook gegenüber Nicht-Mitgliedern verhält ist vielen Nutzern noch immer unklar. Eine Stellungnahme von Facebooks Europa-Verantwortlichen Richard Allen am 07. September 2011 gegenüber Datenschützern des Innen- und Rechtsausschuss des Kieler Landtags verriet, dass zumindest das Vorhandensein von Like-Buttons ein „Tracking", auch von Nicht-Nutzern ermöglicht. Zwar versicherte Allan: *"Wir erstellen keine Profile von Menschen, die keine Mitglieder sind"* (Heise, 2011), jedoch werden Daten aller Internet-Teilnehmer gespeichert, die Webseiten mit vorhandenem Like-Button besuchen.

Das Erfassungssystem Facebook's differenziert zwischen folgenden drei Typen:

1.) **Nicht-Mitglieder**, die facebook.com noch nie besucht haben.

Von ihnen registriert Facebook die IP-Adresse, stammt diese aus Deutschland bleibt sie anonym.

2.) **Nicht-Mitglieder,** welche bereits einmal auf facebook.com geklickt haben.

Diese Nicht-Mitglieder sind mit einem Cookie versehen. Wird nun ein Like-Button auf einer Internetseite geladen, überträgt sich der Cookie an Facebook. Laut Facebook handelt es sich nicht um einen Tracking-Versuch. Im Sinne des Schutzes registrierter Mitglieder handelt es sich um eine Präventionsmaßnahme um "*schadhaftem Verhalten*" entgegen zu wirken.

3.) **Mitglieder**. Durch den Like-Button gelangt Facebook an Nutzerdaten über Zeitpunkt und Datum des Besuchs, sowie über Browsertyp und URL. Diese Erfassung ist laut Facebooks Angaben zeitlich limitiert und nur über eine Dauer von 90 Tagen hinterlegt (Heise, 2011).

Der Like-Button hemmt das Vertrauen in soziale Netzwerke. Private Nutzer, wie auch Unternehmen müssen mit einer Datenübertragung rechnen, sobald Webseiten einen solchen Button enthalten - und dies ganz ohne darauf zu klicken. 2011 veröffentlichte PwC eine Studie laut der Bußgelder für das unerlaubte Einbetten eines Like-Buttons auf Internetseiten verhängt werden können. Die rechtliche Grundlage für den Umgang mit dem Like-Button fehlt noch immer (Kallus, 2012).

Filter Bubble

Der von dem US-Internetaktivisten Eli Pariser geprägte Begriff „Filter Bubble“ (Pariser ist Autor des gleichnamigen Buches) meint das **Filtern von Themen und Informationen im Internet hinsichtlich der Nutzerinteressen**. Dabei handelt es sich um eine nicht selbst verschuldete **selektive Wahrnehmung** bei der Internet-Nutzung. Die Tatsache, dass durch z.B. Cookies Rückschlüsse auf unser Surfverhalten und unsere Interessen gezogen werden können, sorgt für eine automatische Vorsortierung der Themen auf den vom Nutzer gewählten Internetseiten (Pariser, 2011). **Algorithmen bestimmen welche Informationen der Internetnutzer mit großer Wahrscheinlichkeit gerne sehen möchte**. Durch das Filtern kann es sein, dass sich ein vorübergehendes Interesse auf zukünftige Suchergebnisse auswirkt (Schmitt, 2011). Praktisch bedeutet dies, wer einmal in einer Suchmaschine nach einem „Feuerlöscher“ suchte, wird zukünftig auch mit anderen, diesem Themenbereich entsprechenden Werbeanzeigen, konfrontiert. Plötzlich ist das Internet voll von Feuermeldern, Sicherheitsbekleidung, oder gar Schaumfestiger für die Haare, eben weil es sich um Schaum aus der Dose handelt. **Einzelne Klicks und Suchworte der Vergangenheit können mehr oder weniger sinnvoll beeinflussen, was bei späteren Internetbesuchen auf dem Monitor erscheint** (Schmitt, 2011).

Besonders stark genutzt wird dieser Filter für individuelle Werbung (Küchemann, 2012). Obwohl uns das Internet als objektiver Informant erscheint, wird es durch das filter bubbling zu einem Spiegel eigener subjektiver Interessen und Suchanfragen.

Kritiker sehen hierin einen klaren Nachteil, denn die für die demokratische freie Meinungsbildung notwendige Informationsfreiheit wird eingeschränkt. Maschinelle Algorithmen ersetzen den menschlichen Verstand, anstatt einer redaktionell-ausgewogenen Vielfalt erscheinen Prognosen ermittelt aus Klickraten auf den Bildschirmen der Nutzer (Pariser, 2012). In Parisers Internet-Blog erschien kürzlich ein Artikel über Yahoo's Themenauswahl in der Rubrik „Heute". Es kann vorkommen, dass politisch relevante Artikel von den maschinellen Algorithmen aussortiert werden. Yahoo hat für diesen Fall aber ein zusätzliches, redaktionelles Team, welches die finale Entscheidung über die von den Algorithmen vorgeschlagenen Themen trifft (Pariser/Kamin 2012). **Besonders problematisch ist, dass rein maschinell erstellte Nachrichtenseiten im Internet zunächst schwierig als filter bubbles zu identifizieren sind**. Das Nutzer-Bewusstsein über das Zustandekommen einer Internetseite (zumindest darüber ob sie redaktionell oder maschinell erstellt ist) ist mangelhaft. Soziale Netzwerke tragen zu weiterer Intransparenz bei, da auch viele Nachrichtenanbieter eine Präsenz in sozialen Netzwerken pflegen, was zwangsläufig Verwirrung stiftet. Die Zentralisierung und mögliche Beeinflussung der Informationen durch Soziale Netzwerke findet auch FoeBuD e.V.- Datenschützerin Rena Tangens unangebracht: *„Verschärfend kommt dazu, dass die öffentliche Hand, Städte und der Rundfunk so blauäugig sind, sich mit ihren Angeboten zu Facebook begeben, anstatt ihre eigenen unabhängigen Webseiten zu pflegen. Sie liefern damit nicht nur sich selbst, sondern zugleich ihre Nutzer/innen der Willkür von Facebook aus."* (Tangens, 2012, Frage 8). Die Meinungen über den Nutzen des Filterns von Informationen im Internet sind kontrovers. CDU-Politiker Axel E. Fischer beispielsweise spricht von einer fehlenden Filterfunktion im Sinne einer fehlenden Medienkompetenz der Nutzer:
„Dem Vorteil, über mehr Informationen aus mehr Quellen verfügen zu können, steht eine fehlende Filterfunktion teilweise unbekannter Medien gegenüber. Nutzer brauchen daher eine höhere Medienkompetenz, d.h. erhöhte Leistungen bei Themenfilterung, Wahrheits- und Relevanzbeurteilung." (Fischer, 2012). **Die mangelnde Medienkompetenz der Nutzer aufgrund ihrer Unkenntnis des filter-bubble-Verfahrens** und die dadurch mangelnden Möglichkeiten zur informationellen Selbstbestimmung können eine starke Einschränkung der Nutzer Sozialer Netzwerke verursachen.

Facebook's Anpassung an Deutsche Gesetze

Einschränkungen finden sich auch in den Sonderbestimmungen für Deutsche Nutzer, auch hier muss erst ein Untermenü geöffnet werden, welches sich in der „Erklärung der Rechte und Pflichten" befindet. Die Sonderbestimmungen für Deutsche Nutzer wurden am 20. April 2012 überarbeitet. Anders als bei den US-Bestimmungen ist in Deutschland u.a. die Nutzung preisgegebener Inhalte auf Facebook beschränkt und auf keine anderen Anbieter übertragbar. Zudem ist das In-Kraft-Treten von Änderungen in der „Erklärung der Rechte und Pflichten" erst nach 30 Tagen wirksam. Der Nutzer akzeptiert diese Änderungen stillschweigend nach Ablauf der Frist, wenn er sein Facebook-Konto nicht löscht. Der Nutzer hat eine Holschuld sich regelmäßig eigeninitiativ über Änderungen auf „Facebooks Site Governance" zu informieren. (Facebook, 2012 E)

Facebook's Gerichtsstandort

Als Gerichtsstandort für Facebook USA ist **Delaware** angegeben. *„Die Facebook, Inc. ist eine nach dem Recht des States Delaware gegründete und registrierte Gesellschaft"* (Facebook, 2012 A). Delaware als Gerichtsstandort gilt unter Juristen als Steuerparadies und ist besonders für die lockere Auslegung von Urheberrechten bekannt. Grund hierfür ist Delaware's liberales Gesellschaftsrecht (Delaware General Corporation Law, 2011). Für den Europäischen Raum ist der Gerichtsstandort Irland verzeichnet. Die rechtliche Zugehörigkeit Facebooks scheint zwar grundsätzlich festgelegt, jedoch gibt es keinen eindeutigen Europäischen Rechtsraum. Ebenso wenig sind eindeutige juristische Maßnahmen festgelegt, die für die Sanktionierung eines Unternehmens wie Facebook bei Urheberrechtsverletzungen Regelungen vorgeben würden. Facebook sieht sich daher häufig in der Kritik Gesetzeslücken auszunutzen und die jeweiligen Datenschutzgesetze Europäischer Einzelnationen zu ignorieren.

In einem Artikel des Focus-Online-Magazins im Juni 2012 konnten Leser darüber abstimmen, welche der u.a. oben aufgeführten Kritikpunkte sie an Facebook am meisten stören. Rund 940 Leser beteiligten sich in den ersten zwei Tagen an der Umfrage. Die meisten Leser fanden vor allem die versteckten Datenschutzeinstellungen negativ. Sie stören sich besonders an den Schwierigkeiten Voreinstellungen beizubehalten, da ständig unangekündigte Änderungen seitens

Facebook durchgeführt würden. (Frickel, 2012):

Abbildung 5 „Was nervt sie bei Facebook am meisten“ (Quelle: Frickel / 2012 IN: Focus Online)

4.2 Kritik an Facebook in der Vergangenheit und aktuell

Facebook steht regelmäßig im Fokus der medialen Aufmerksamkeit wenn es um seine Datenschutzpraktiken geht. Facebook’s Geschäftsmodell ist umstritten, denn Facebook handelt mit einem Gut, dass rein rechtlich gesehen den Nutzern gehört (Kurz/Rieger, 2011, S.14ff.). Dennoch stellt es Nutzerdaten Werbetreibenden zur Verfügung da personalisierte Werbung eine höhere Einnahmequelle darstellt als herkömmliche. Peter Schaar stellt die verschiedenen Interessen von Nutzer- und Unternehmensseite wie folgt klar: *„[...] Insofern gibt es keine Probleme damit, dass man Informationen über sich selber preisgibt. Wenn man jetzt aber Informationen über Dritte preisgibt, dann ist das natürlich eine Beeinträchtigung von deren Interessen und rein rechtlich gesehen bedeutet das dass man deren Einwilligung braucht oder eben einen Rechtfertigungsgrund. [...] Im Hinblick auf das Verhältnis Kunde – Unternehmen, also Facebook vs. Facebook-Nutzer ist es so, dass ja nicht nur die Informationen preisgegeben werden, die man dem Unternehmen bewusst gibt, sondern durch sein Verhalten im Netzwerk [...] werden Informationen auch über das Nutzungsverhalten offenbart.“* (Schaar, 2012 B)

Einer der Hauptvorwürfe gegen Facebook ist die starke **Einschränkung der Nutzerrechte**, während den Betreibern großzügig Rechte zur Daten-Nutzung und –Verbreitung eingeräumt werden. Ein 2010 veröffentlichter Bericht der Stiftung Warentest bemängelte sogar vielfältige Verstöße Facebooks gegen das Deutsche Datenschutzrecht (Spiegel, 2010). Im Vergleich mit zehn anderen führenden Sozialen Netzwerken wie Myspace und LinkedIn landete Facebook auf dem drittletzten Platz, wegen „erheblicher Mängel" beim Datenschutz. Allein 2012 vor dem geplanten Börsengang Facebook's hat das Soziale Netzwerk mit vielerlei Negativschlagzeilen von sich reden gemacht. Von einem **Wachstumsrückgang** der Facebook-Mitglieder (Biermann, 2012 & n-tv.de/jga/dpa/rts/DJ, 2012) ist die Rede, von einem **Ausstieg wichtiger Werbekunden** (FTD Online, 2012 & Sueddeutsche, 2012 B) und von **Ideenklau bei Patenten** (Focus Online/DPA, 2012 & n-tv.de/jga/dpa/rts/DJ, 2012). Da Facebook selbst neben IT-Strukturen kein geistiges Eigentum erstellt, soll der **Rückgang der Nutzerzahlen** im Lichte eines Abstrafungsvorgangs der Nutzer gegenüber Facebook gesehen werden. Der Vorwurf man würde durch Patente-Käufe den Mangel an eigenem geistigen Eigentum kaschieren wollen, wird deutlich (Härting, 2012, S.265 ff.). In der Kritik steht auch der Versuch von Facebook **neue Nutzungsbedingungen in Deutschland** zu etablieren. Eine Auflage, die das Irische Parlament dem Unternehmen auferlegte (Focus Online, 2012 B).

Die Vorwürfe hier gelten vor allem der **Intransparenz der Funktionsweise von Cookies** und der **Dauer der Datenvorratsspeicherung** (FAZ, 2012). Auch neutrale Instanzen wie das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD), allen voran ULD-Leiter Thilo Weichert äußern Misstrauen gegenüber der Veränderung der Datenschutzrichtlinien Facebook's. Die Presse zitiert Weichert wie folgt: *„Das Unternehmen müsse nicht nur das Kleingedruckte in den Richtlinien ändern, sondern seine Geschäftspolitik und seine Datenverarbeitung."* (Sobiraj, 2012) Weicherts aktueller Hauptvorwurf ist, dass die neuen Facebook-Datenschutzrichtlinien zwar detaillierter und verständlicher seien, dass durch sie aber auch der gesamte Habitus des Unternehmens gegenüber der Datenschutz-Debatte an den Tag treten würde. Dieselbe Lockerheit, die sich wie ein roter Faden durch Facebook's Geschäftspolitik zieht und sonst einen Sympathiebonus für das Unternehmen bedeutet, ist auch bei den Datenschutzrichtlinien vorhanden. Die

Ungezwungenheit Facebook's wird jedoch bezogen auf die Einhaltungen gesetzlicher Standards von Datenschützern, Medien und Nutzern und als unangemessen wahrgenommen. Ein weiterer Vorwurf gegenüber FB ist daher, dass das Unternehmen diesem Vertrauensverlust mit minimalen und weiterhin intransparenten Änderungen der Datenschutzrichtlinien zuvorkommen will. Facebook, wie auch Google tun jedoch noch immer nicht genug für den Datenschutz, wie Weichert betont: *„Google und auch Facebook haben gemerkt, dass sie in Sachen Transparenz mehr machen müssen. Aber in beiden Fällen bleiben die bisherigen Aktivitäten hinter dem verbraucher- und datenschutzrechtlich absolut Nötigen weit zurück. Sie müssen umfassende Transparenz schaffen, die aber bis heute nicht besteht. Es sollten zudem auch Wahlmöglichkeiten – etwa bei der Profilerstellung – eingeräumt werden "* (Sorge, 2012).

Ein weiterer Vorwurf den Facebook von Seiten anderer Unternehmen erhält, ist der Vorwurf der **Monopolbildung** für Internetdienste. Google-Entwickler Sergej Brin äußerte in einem Interview mit dem Guardian im April 2012 Bedenken gegenüber Facebook und Apple. Die Datenübertagung auf andere Dienste würde durch Facebook blockiert und dies verhindere eine Freiheit des Internets und unterdrücke Innovationen, so lautete der Hauptvorwurf von Informatiker Brin (Beiersmann, 2012). *„In an interview with the Guardian, Brin warned there were ‚very powerful forces that have lined up against the open internet on all sides and around the world'. ‚I am more worried than I have been in the past,' he said. ‚It's scary.'* (Katz, 2012).

Auch die Deutschen Datenschützer Peter Schaar und Rena Tangens teilen die Ansicht, dass die Monopolbildung Sozialer Netzwerke im Internet problematisch, wenn nicht sogar gefährlich, sein kann. Rena Tangens kritisiert vor allem die dahinter stehende Systematik: *„Der systematische Verstoß gegen Datenschutzgesetze, die systematische Intransparenz, die dazu dient, die Nutzer/innen im Dunkeln zu lassen über [...] Profilbildung und Auswertung von Klickraten. Das größte Problem aber ist die Monopolbildung und die Ausweitung des Einflussbereichs von Facebook über Like-Buttons etc. – kurz gesagt, dass Facebook die zentrale Plattform für die Internet-Nutzer/innen werden will."* (Tangens, 2012).

Beide Sorgen, sowohl die der Monopolbildung als auch die der Rechtmäßigkeit der Datenspeicherung bei FB, teilt auch der Österreichische Jura-Student und Datenschutz-Aktivist Max Schrems. Er gründete eigens eine Internetseite, um diesen Entwicklungen vorzubeugen, worauf Kapitel 4.4 näher eingehen wird.

4.3 Vorwürfe der BigBrother- Awards & der Stiftung Warentest

Seit 1987 existiert in Bielefeld der FoeBuD e.V., es ist ein bürgerrechtlicher Verein der sich brisanten Datenschutz-Themen annimmt (FoeBuD, 2012). Einmal jährlich verleiht der Verein die so genannten BigBrotherAwards, einen Preis, der besonders schlechte Datenschutz- und Privatsphäre- Praktiken von Unternehmen und Organisationen aufzeigen soll (BigBrotherAwards, 2012). Im Jahr 2011 erhielt Facebook einen BigBrotherAward in der Kategorie Kommunikation. Die Laudatio, verfasst und gehalten von der FoeBuD e.V. Vorsitzenden Rena Tangens, enthielt einige Vorwürfe gegen Facebook. Tangens schilderte zunächst die Parallelen von Facebook zu George Orwell's Roman „1984". Tangens wirft Facebook vor, eine globale **Gated Community** zu sein, eine geschlossene Gemeinschaft, in der die Unternehmensinteressen der Betreiber die Verhaltensregeln der Mitglieder bestimmen. Der Konzern, den Tangens u.a. als **Datenkrake** bezeichnet, lockt Freiwillige mit **geschicktem Eigenmarketing** in die Datenpreisgabe. Im Hintergrund bleibe jedoch stets der Zweck Datenerhebung Facebook's, denn die wirklichen **Profiteure der Datensammlung**, neben Mark Zuckerberg, sind und bleiben intransparent. Tangens hält eine Verbindung des Facebook-Vorstandes zu **amerikanischen Geheimdiensten** für möglich. Die Kritik gilt dem **Investoren-Einfluss auf Facebook**, ebenso wie der unklaren **Dauer der Vorratsdatenspeicherung**. Tanges ist davon überzeugt, dass die **Profilbildung und die Auswertung von Klickraten** so weit gehen, dass sogar eine Textanalyse persönlicher Nachrichten durchgeführt wird. Durch diese ist es möglich das Verhalten der Nutzer zu erkennen und problemlos zu identifizieren (Tangens, 2011). Besonders kritisch bewertet Tangens Facebooks „Instant Personalization"-Anwendung (umgehende Personalisierung), die Facebook selbst wie folgt bewirbt: *„Das Internet ist besser mit Freunden – Zeige die Rezensionen von Freunden zuerst an, wenn du nach einem Film suchst. Höre deine Lieblingslieder automatisch, wenn du eine Musikseite besuchst. Erfahre ein auf dich und deine Freunde zugeschnittenes Interneterlebnis."* (Facebook, 2012 B). Diese Anwendung geriet im Jahr 2010 vor

allem wegen ihrer Sicherheitslücken in die Kritik. Durch die Programmierung eines seitenübergreifenden Scriptings war es fremden Webseiten möglich Facebook-Daten auszulesen (Hedemann, 2010).

Stiftung Warentest:

In einer Studie aus dem Jahr 2010 hat die Organisation „Stiftung Warentest" erhebliche Mängel beim Datenschutz von Sozialen Netzwerken festgestellt. Insbesondere Facebook erhielt eine sehr schlechte Bewertung, da sich das Unternehmen nicht dazu bereit erklärte, sich dem Hacking-Test der „Stiftung Warentest" zu unterziehen. Facebook war der „Stiftung Warentest" zudem besonders negativ aufgefallen, als das führende Soziale Netzwerk im Dezember 2009 „*von einem Tag auf den anderen die Datenschutzeinsteillungen änderte*" (Stiftung Warentest, 2010, S.41). Fortan waren private Profileinstellungen bei Facebook, u.a. Nutzername, Profilfoto und Gruppenzugehörigkeit öffentlich. Aufgrund von der Verweigerung der Test-Teilnahme und auch wegen Facebooks „*problematischem Umgang mit Nutzerdaten, den Nutzerrechten und den AGB*" (Stiftung Warentest, 2010, S.43) erreichte Facebook nur Platz 8 von 10 getesteten Sozialen Netzwerken mit Note 3,9 ausreichend. Als äußerst kritisch stufte die „Stiftung Warentest" auch Facebooks **Freunde-Finder** ein, der E-Mail-Daten aus den Postfächern von Facebook-Mitgliedern saugt und somit auch **Nichtmitglieder ohne eigenes Zutun vom Sozialen Netzwerk erfasst werden**.

Die Mindestanforderungen, die die „Stiftung Warentest" an Soziale Netzwerke stellt sind basal: **Login-Name und Passwort auf mobilen Endgeräten** sollen genauso **verschlüsselt** werden, wie **sensible Nutzer- Informationen**. **Passwörter** sollen generell aus **mindestens sechs Zeichen** bestehen. Nach einer bestimmten **Anzahl erfolgloser Anmeldungen** erfolgt die **Sperrung des Accounts**. Betreiber sollen regelmäßig **die reale Nutzer-Identität überprüfen**, damit diese vor Identitätsdiebstahl geschützt sind. Auch in Sachen **Jugendschutz und Cybermobbing** erkennt die „Stiftung Warentest" Änderungsbedarf, denn laut einer Studie der Landesanstalt für Medien in Nordrhein-Westfalen nutzen 85% der 12-24-jährigen zwei Stunden täglich die Angebote Sozialer Netzwerke (LfM Nordrhein-Westfalen, 2009). Die **Alterskontrollen jedoch sind dürftig** bis gar nicht vorhanden

und auch die Möglichkeiten zur **Entfernung jugendgefährdender Inhalte** sind stark eingeschränkt.

Überraschend ist jedoch, dass die „Stiftung Warentest“ die Verantwortung für mangelnde Alterskontrollen nicht bei den Betreibern Sozialer Netzwerke, sondern partiell auch bei den Deutschen Behörden sieht: *„Einen Personalausweis haben Jugendliche in der Regel erst mit 16 Jahren. Bis zu diesem Alter können die Anbieter nicht sicherstellen, dass jemand, der vorgibt 14 zu sein, auch wirklich 14 Jahre alt ist.“* (Stiftung Warentest, 2010, S. 44). Es ist fraglich, ob das Problem des fehlenden Ausweis-Dokuments nicht via PostIdent-Verfahren[6] oder Einverständnis-Erklärung der Eltern gelöst werden kann. Auch die Frage, ob Soziale Netzwerke generell mit einer Altersbeschränkung ab 16 belegt werden sollten, ist bei Facebook noch nicht final geklärt.

Große Kritik an Facebook äußerte die „Stiftung Warentest“ außerdem an der **Datenspeicherung,** der **Vereinnahmung geistigen Eigentums** und der **Ohnmacht der Nutzer** gegenüber **personalisierter Werbung**. Das Datenschutzmanagement anderer Sozialer Netzwerke wie z.B. studiVZ sei erheblich besser, da diese ihre Software sogar einer TÜV-Prüfung unterzögen, so lautet ein weiterer Vorwurf. Der Vergleich mag nahe liegen, jedoch muss beachtet werden, dass die VZ-Netzwerke in Deutschland entstanden und somit kongruent zu Deutschen Datenschutzvorstellungen sind. Die „Stiftung Warentest“ hebt auch den kulturellen Unterschied zwischen US-Nutzern und Deutschen hervor: *„Denn Datenschutz spielt in den USA traditionell eine untergeordnete Rolle, und die wirtschaftliche Nutzung von persönlichen Daten als Gegenleitung für einen kostenlosen Dienst akzeptieren, die Amerikaner viel eher als die Deutschen.“* (Stiftung Warentest, 2010, S. 44).

Möglicherweise reicht jedoch die Betrachtung kultureller Differenzen allein nicht aus, um aktuellen Datenschutz-Ansprüchen gerecht zu werden und den Herausforderungen des ubiquitären Internets zu entsprechen. Eine Problematik, die im weiteren Verlauf noch Beachtung finden wird.

[6] Ein Verfahren, bei dem gegen Vorlage des Personalausweises bei der Post eine Identifikation erfolgt.

4.4 Vorwürfe der Nutzer: Aktualisierung der Facebook Rechte und Pflichten

Einer der Hauptvorwürfe gegenüber denen sich Facebook verantworten muss, ist die Kritik der Nutzer daran, dass Facebook heimlich, still und leise die Erklärung der Rechte und Pflichten Facebooks verändert, ohne dass der Nutzer proaktiv über diese Veränderungen unterrichtet wird. Facebook-Nutzer erfahren Neuerungen meist aus der Presse oder müssen selbst aktiv nach **Veränderungen und Einstellungsmöglichkeiten** suchen. **Neue Facebook-Produkte** werden lanciert, ohne dass der Nutzer eine Benachrichtigung darüber erhält. Bestimmungen des offiziellen SRR (Statement of Rights und Responsibilities) werden verändert und neue Funktionsweisen werden eingeführt, ohne dass der Nutzer es überhaupt bemerkt. Zuletzt hatte die Umgestaltung des klassischen Facebook-Profils in die „Chronik“ viel Unmut bei den Nutzern erregt (Beleg). Vor allem bei der Datenspeicherung der persönlichen Nutzerdaten und geteilten Inhalte herrscht **Komplexität statt Transparenz**. Facebook behält sich vor selbst von gelöschten Daten über einen **„angemessenen Zeitraum“ eine Sicherheitskopie** zu verwahren (Facebook, 2012 A), wie lange genau dieser Zeitraum andauert, darüber gibt es keine Auskunft seitens Facebook. Auch darüber welche Daten nach Jahren der Facebook-Nutzung noch bestehen bleiben, gibt es keine genauen Informationen.

Als aktueller Präzedenzfall für diesen Sachverhalt gilt derzeit der Österreichische Jura-Student und Datenschutz-Aktivist Max **Schrems**. Dieser verlangte von Facebook Auskunft über alle seine persönlichen Daten, die ihm der Konzern nach 23 Anfragen endlich zur Verfügung stellte. Das Ergebnis war erschreckend, gegen Schrems Willen und zudem rechtswidrig waren alle seine Nutzerdaten komplett erhalten, selbst gelöschte Inhalte, Kontakte und private Nachrichten. **Laut Europäischem Datenschutzrecht ist die unbefristete Speicherung von Nutzerdaten verboten** (Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten). Seit einem Jahr versucht Schrems nun Facebook’s europäische Tochter, mit Firmensitz in Irland, unter Berücksichtigung des EU-Datenschutz-Rechtes zu verklagen. Erreichen konnte er mit seinen Klagen bisher immerhin, dass Facebook sich einer Unternehmensprüfung unterziehen musste und irländische Datenschützer dem Konzern die Empfehlung auferlegten, seine Datenvorratsspeicherung und seine SRR zu verändern. Die Frist für Facebook seine Datenschutzrichtlinien zu simplifizieren ist am 31.März 2012 abgelaufen. Irland räumt dem Konzern

sanktionsfrei eine Verlängerung der Frist bis Ende Sommer 2012 ein (Goldgraber/Henselmans, 2012 & Prummer in: Süddeutsche Zeitung Online, 2012).

Seit Facebook den Börsengang für Mai 2012 plant und Schrems seine Plattform mit dem Titel **"Europe versus Facebook"** (Europe versus Facebook, 2012) betreibt, treibt der Internetkonzern die Veränderungen der Datenschutzbestimmungen im deutschsprachigen Raum voran. Das Resultat ist eine **„Aktualisierung der Erklärung der Rechte und Pflichten“**, welche Facebook am 20.April 2012 auf der Facebook Site Governance-Seite zum kommentieren frei gab (Facebook Site Governance A, 2012).

5 Lösungsansätze für divergierende Stakeholder-Bedürfnisse der Datentransparenz in Sozialen Netzwerken

Um den verschiedenen Anreizstrukturen und den Bedürfnissen der drei oben identifizierten Stakeholder[7]-Gruppen gerecht zu werden. Gibt es verschiedene Lösungsansätze. Man kann das Datentransparenz-Problem z.B. dadurch näher betrachten, dass man sich mit den Informationsasymmetrien zwischen Prinzipalen (alias die Nutzer Sozialer Netzwerke) und den Agenten (alias die Betreiber Sozialer Netzwerke) eingehend beschäftigt, siehe Kapitel 4.1. Eine Erweiterung dieses Ansatzes ist die Entwicklung einer Risiko-Bewertung, wie George Akerlof sie in seiner „Informationsasymmetrie“-Theorie vorschlägt, siehe Kapitel 4.2. Der Dritte Ansatz entstammt der Bildungs-Theorie und ist angelehnt an das demokratische Konzept des „mündigen Bürgers“, siehe Kapitel 4.3.

5.1 Wie viel Datenschutz kaufe ich ein? – Ein Signalling- Ansatz

Im ersten Quartal das Jahres 2012 veröffentlichte die Wirtschaftsprüfungsgesellschaft und Unternehmensberatung PwC im dritten Jahr in Folge das Ergebnis einer Umfrage von Datenschutzbeauftragten der größten deutschen Unternehmen[8]. Auch wenn das Thema Datenschutz in Unternehmen im

[7] Stakeholders meint interne wie externe Anspruchsgruppen, die von der unternehmerischen Aktivität Sozialer Netzwerke direkt oder Indirekt betroffen sind (Gabler Wirtschaftslexikon).
[8] www.pwc.de/datenschutz2012

Zuge der stetig wachsenden Digitalisierung bereits mehr und mehr Beachtung findet, so wurde dennoch in gut jedem vierten der 1.000 befragten Unternehmen mindestens ein Datenschutz-Verstoß bekannt (finanznachrichten.de, 2012). Gleichzeitig erachten die befragten Datenschutzbeauftragten jedoch die Wahrung der Datenschutzrichtlinien auch im Hinblick auf die geplante EU-Datenschutzverordnung für zunehmend wichtiger. Sie fühlen sich in Bezug auf den Einsatz von Sozialen Netzwerken und Cloud Computing innerhalb des Unternehmens stark verunsichert (Fechte/Görtz, 2012). Die allgemeine Verunsicherung der Unternehmensvertreter verweist auf die vorherrschende **Informationsasymmetrie zwischen Agenten (Betreibern) und Prinzipalen (Nutzern)**.

Der Ansatz der neoklassischen **„theory of the firm" von Ronald Coase** setzt ebenfalls bei den Informationsasymmetrien an. Er erklärt die Existenz von Unternehmen damit, dass die Transaktionskosten innerhalb einer Firma geringer sind, da die Informationsasymmetrie innerhalb einer Firma nicht so hoch ist, wie auf dem freien Markt (Coase, 1937). Informationsasymmetrien hemmen unternehmerisches Handeln, da mangelnde Kommunikation auch gleichzeitig weniger Verhaltensoptionen bedeutet. Dennoch besteht das Prinzipal-Agenten-Problem insbesondere zwischen unterschiedlichen Markt-Akteuren weiterhin (Milgrom / Roberts, 1992, S.38 ff.). Daher gilt es Betreiber und Nutzer Sozialer Netzwerke ebenfalls in diesen Kategorien zu betrachten. Wie aber kann das Ungleichgewicht zwischen Agent und Prinzipal verringert werden?

Innerhalb der Vertragstheorie hat sich das **Signalling-Modell von Michael Spence** behauptet, da es Prinzipale und Agenten wieder zu einem Vertrauensverhältnis zurückführt. Zentral ist die Idee, dass der Agent glaubhaft Informationen über sich selbst an den Prinzipal vermittelt[9]. Der Agent erwirbt erstrebenswerte Transparenz-Attribute und signalisiert diese gegenüber dem Prinzipal (Spence, 1973). Ein Beispiel hierfür wäre, dass ein Netzwerkbetreiber wie z.B. Google (in diesem Fall der Agent) die genaue Datenverarbeitung und -Speicherung eines Dienstes wie „Google Analytics" [10]gegenüber seinem Kunden (Prinzipal) kenntlich macht. Dieser Vorgang erhöht die Datentransparenz und würde das Vertrauen in die Produkte von

[9] Spence entwickelte das Signalling-Modell anhand des Beispiels des Personalmarkts.
[10] Ein Webseiten-Optimierungstool, welches die Zugriffe auf eine Website anzeigt.

Google fördern.

Mit dem klaren „signalling“ von Funktionsweisen, Speicherverfahren und Zugriffsbeschränkungen, würden Netzwerk-Betreiber nicht nur die eigene Authentizität verbessern, sondern sie würden auch zum Schutz persönlicher Daten ihrer Nutzer beitragen. Eine Forderung, die auch seitens des Bundesdatenschutzbeauftragten Peter Schaar deutlich wird: *„Die Möglichkeit wäre zu differenzieren zwischen Kern-Informationen und Informationen die in extenso die Hintergründe noch einmal beleuchten: Wir bearbeiten das und das Datum, für den und den Zweck und die Daten werden dort verarbeitet. Vielleicht drei Kerninformationen, Art der Daten, verantwortliche Stelle, Zweck der Datenverarbeitung, und dann könnte man natürlich in einem gestuften System dem Interessierten mehr Informationen zur Verfügung stellen.“* (Schaar, 2012 B, Frage 6). Schaar bemängelt, dass im Zuge der Interessen der Werbetreibenden (also der Agenten) keine Transparenz bezüglich der Kerninformationen vorhanden ist. Lorenz schlägt ein proaktives Vorgehen seitens der Netzwerkbetreiber vor: *„Betreiber könnten beispielsweise gezwungen werden diese Löschung für den Nutzer bequem zu gestalten. Über Formulare auf der Website könnte der Nutzer die Löschung der eigenen Daten beantragen. [...] Es wäre ein minimaler Eingriff seitens der Politik, den Nutzern die Möglichkeit zu geben Daten löschen zu lassen. Dennoch ist eine solche Löschung bei Sozialen Netzwerken technisch nicht ganz leicht. Problematisch ist das z.B. bei Facebook, die Daten werden in drei Way-Back-Maschinen nachgehalten, auch wenn Facebook diese bereits gelöscht hat. Dieser Prozess führt dazu, dass das Internet nichts vergisst.“* (Lorenz, 2012)

Zu einem solchen Vorgehen müssten Betreiber Sozialer Netzwerke wesentlich transparenter auf die Datenverarbeitung hinweisen. Die Scheu der Agenten vollständige Informationen zu vermitteln, lassen bei wirtschaftlichen Transaktionen, z.B. beim Austausch von Waren, Dienstleistungen und Daten ein generelles Misstrauen auf Prinzipal-Seite entstehen. Der Nutzer (Prinzipal) bemerkt diese Informationsasymmetrie. Das „signalling“ ist eine Aussage über die Qualität der Produkte und Angebote des Anbieters (Agenten) (Milgrom/Roberts, 1992, S.156). Betreibt der Anbieter jedoch kein „signalling“, können seine Nutzer die Qualität des komplexen und intransparenten Netzwerk-Systems nicht beurteilen. Der Nutzer läuft somit seinerseits Gefahr rechtswidrig zu agieren, da die von ihm für Transaktionen

notwendigen Daten ungeschützt sind. Gerade Unternehmen können sich dem digitalen Datentransfer nur begrenzt entziehen. Umso wichtiger ist ein sorgfältiges Daten-Management.

Betreibt aber die Agenten-Seite „signalling“, zumindest mit Fragmenten von relevanten Informationen, so interpretiert der Prinzipal diese und passt dementsprechend sein Datenpreisgabe- und Kauf-Verhalten an (Milgrom/Roberts, 1992, S.154 ff.). In der Regel, sind Prinzipale dann bereit einen höheren Preis für das gewünschte Produkt (in diesem Fall für mehr Datentransparenz bei Online-Diensten) zu zahlen, als wenn kein Signal ausgesendet worden wäre (Adamek, 2011, S.28).

Kongruent zu der Personalmarkt-Annahme von Michael Spence, dass es zwei Arten von Mitarbeitern gibt – produktive und unproduktive – ist auch der Gedanke, dass es auch unter den Betreibern Sozialer Netzwerke ebenfalls gute und schlechte Agenten gibt. Man kann von transparenten und intransparenten Dienstanbietern ausgehen. Die Nutzer, insbesondere Unternehmen, die bei Inkrafttreten der neuen EU-Datenschutzverordnung mit erheblichen Sanktionszahlungen bei Datenschutz-Verstößen rechnen müssen, können sich ein schlechtes Daten-Management nicht leisten: Dies lässt den Schluss zu, dass Unternehmen für einen vertrauenswürdigen Dienstanbieter bereit sind zu zahlen. Dazu müssten Betreiber für einen bestimmten Preis ein Datenspeicherungs- und Datennutzungs- Vorgehen anbieten, welches mehr Transparenz und Kontrolle für die Nutzer, die nunmehr zu Kunden werden, schafft.

Transparenz des Datenmanagements ist eine Dienstleistung für die bisher noch kein Zahlungsmodell vorhanden ist. Kaum ein Nutzer hat jedoch die Kontrolle über die von ihm digital preisgegebenen Daten. Die Frage „Wie viel Datenschutz kaufe ich ein?“ erscheint im Sinne einer vertrauensfördernden Transaktionskosten- Theorie als ein Lösungsansatz.

Zwar erscheint es zunächst als paradox, dass der Urheber der Daten, diese nicht selbst kontrolliert. Jedoch gibt es bereits heute Geschäftsmodelle von Agenturen, die privaten Nutzern die Rückholung der versehentlich publizierten Daten ermöglichen. *„Doch auch im digitalen Kapitalismus gibt es Unternehmen, die diese Not zu Geld machen: Die neue Branche heißt Reputationsmanagement und kümmert sich darum, den im Internet angeschlagenen Ruf von Menschen wiederherzustellen.“* (Adamek, 2011, S.28).

Aus grundgesetzlicher Perspektive gehören persönliche Daten zwar dem Nutzer selbst, allerdings nur so lange, wie der Nutzer nicht zur Preisgabe einwilligt. Hat er allerdings einmal eingewilligt ist die Rechtslage schwierig, denn über die Halbwertszeit der Datenpreisgabe gibt es noch keine feste Regelung. Daher ist es denkbar, dass meine geschäftlich oder privat verursachte Datenpreisgabe (die bislang nicht zeitlich limitiert ist) nicht unendlich lange im Umlauf sein sollte.

Die Deutsche IT-Firma Backes-SRT[11] GmbH entwickelte eigens zu diesem Zweck eine Lösungsmöglichkeit, die in der Presse gemeinhin als „Digitales Radiergummi" bekannt wurde. Gänzlich richtig ist diese Bezeichnung jedoch nicht. Stefan Lorenz Mitentwickler der X-Pire! [12] -Software äußert sich zum Begriff „Digitales Radiergummi" wie folgt: „*Ein Digitales Radiergummi im Internet kann es nicht geben. Das ist technisch nicht möglich. Das hat folgenden Grund. In dem Moment, in dem ich ein Bild oder irgendwelche persönlichen Daten veröffentliche gebe ich sie aus meinem Kontrollbereich ab, in den Kontrollbereich von Anderen. Sie können sich beispielsweise mein Bild herunter laden auf Ihren Rechner. Wollte ich jetzt sicherstellen, dass ich dieses Bild löschen kann, bräuchte ich Zugriff auf Ihren Rechner. Das wiederum kann nicht in Ihrem Sinne sein.*" (Lorenz, 2012)

Um der Problematik der sich dezentral verbreitenden Daten im Internet vorzubeugen hat die Firma Backes-SRT GmbH die Software X-Pire! entwickelt, diese funktioniert wie folgt: „ *Sie geben eine Datei z.B. ein Bild in das X-Pire!-Programm. Dort wird die Datei verschlüsselt. Dieser Schlüssel wird auf einen Schlüsselserver hochgeladen. Dieser Schlüsselserver gehört Ihnen entweder selbst oder einer Instanz der sie vertrauen. Dann wird in diese Datei die Information eingebettet, wo dieser Schlüssel sich befindet. Geht nun jemand mit seinem Browser auf das Bild und möchte es betrachten, fragt das Plugin automatisch beim Schlüsselserver an, ob er dieses Bild freigeben kann. Ist das Bild abgelaufen, kann es nicht mehr betrachtet werden.*" (Lorenz, 2012).

Für die technische Finesse, persönliche Daten mit einem Ablaufdatum zu versehen, müssten die Betreiber einen erhöhten Aufwand betreiben und Kosten tragen. Daher ist es denkbar, dass Nutzer für diesen Mehr-Aufwand zahlen müssen. Dieses ist für

[11] SRT= Security research & technologies
[12] X-Pire! ist eine Software, die es mit Hilfe von Verschlüsselung ermöglicht, Daten, Bilder und Dokumente mit einem Verfallsdatum zu versehen.

Einzelnutzer nur schwierig realisierbar, da diese nicht im selben Maß rechtlich belangt werden können wie Unternehmen.

Eine weitere Möglichkeit, wie Betreiber Sozialer Netzwerke ein erfolgreiches Signalling betreiben können, ist eine Vorgehensweise bei der das Netzwerk beispielsweise **datenschutzkritische Blogger einbezieht**. Eine **selbstkritische Auseinandersetzung mit den eigenen Datenschutz- Einstellungen** schafft vertrauen, da ein Bemühen seitens der Netzwerkbetreiber nachvollziehbar wird. Ein regelmäßiger Test der eigenen Einstellungen, sowie eine Dokumentation darüber zeigt, dass dem Betreiber das Thema wichtig ist. Auch Facebook möchte nun einen ersten Schritt in diese Richtung wagen, so erklärt Dr. Gunnar Bender, seit April 2012 Facebooks neuer Director of Politics in Deutschland, seine Arbeit wie folgt: *„Im Wesentlichen geht es darum Aufklärung über Facebook zu betreiben. Das bedeutet ich werde dann kontaktiert, wenn irgendwo mal wieder eine öffentliche Facebook-Party stattfindet oder wenn es darum geht der Politik Hintergründe zu Facebooks Anwendungen zu erläutern.“* (Bender, 2012). Laut Bender hat Facebook verstanden, dass die Informationsasymmetrien gravierend sind und vermehrte Aufklärung nötig ist.

5.2 Gute und schlechte Datentransparenz – Ein Risikobewertungs-Ansatz nach Akerlof

Im Jahre 1970 veröffentlichte der Ökonom George Akerlof seinen Essay *"The Market for Lemons: Quality Uncertainty and the Market Mechanism"* (Akerlof, 1970). Akerlof entwickelt in ihm Grundgedanken zu Informationsasymmetrien in Märkten und erhielt für deren Weiterentwicklung zusammen mit Michael Spence und Joseph Stiglitz 2001 den Wirtschaftsnobelpreis. Anhand des Gebrauchtwagenmarktes entwirft Akerlof beispielhaft das Problem der **adversen Selektion bei Marktgütern** mit Qualitätsunterschieden. Die Annahme, dass qualitativ minderwertige Güter (z.B. Gebrauchtwagen) aufgrund ihres niedrigeren Preises und der **mangelnden Informationslage der Nachfrager**, vermehrt gekauft werden, führt zu einem Marktergebnis welches **nicht dem Pareto-Optimum entspricht** (Pareto, 1906). Der **Qualitätsunterschied des Gutes** ist nur der Anbieterseite bekannt, nicht aber den Nachfragern. Die Nachfrager bilden daher anhand eigener Erwartungswerte einen **Vorbehaltspreis**. Überschreitet der reale Preis diesen Vorbehaltspreis, kaufen die Nachfrager das Gut nicht länger. Es entsteht

eine negative Selektion, wobei die **qualitativ hochwertigen Güter ihren Absatzmarkt verlieren** und die Anbieter von Qualitätsprodukten vom Markt gedrängt werden. Um dieser Marktverdrängung entgegenzuwirken ist es dem Anbieter möglich, dass bereits in Kapitel 6.1 erwähnte „signalling“ zu betreiben. Der Gebrauchtwagen kann beispielsweise mit einem **Siegel vom TÜV** oder einer anderen Institution versehen werden um die **positiven Qualitätsmerkmale zu verifizieren**. Ein weiterer Ansatz um ein Qualitätsprodukt von einem „lemon“-Produkt zu unterscheiden, ist das kostengünstige **Angebot einer Gewährleistung oder Garantie** auf das Gut.

Der Akerlof’sche Entwurf legt nahe den **„market of lemons“ auch auf dem Datenmarkt zu vermuten**. Kongruent zu den Informationsasymmetrien auf dem Gebrauchtwagenmarkt, sind auch die Nutzer Sozialer Netzwerke verunsichert. Was den Umgang mit persönlichen Daten angeht, so bieten die Internetseiten der Betreiber nur **wenig Transparenz**. Lediglich die Anbieter haben einen Überblick, über Sicherheit und Zugänglichkeit, sowie Verbreitung, Verkauf und Speicherung der Daten. Der IT-Spezialist Stefan Lorenz sieht es vor allem als eine Aufgabe der Politik an, das Bewusstsein der Nutzer über die Datenverarbeitung zu stärken. Seiner Meinung nach sind sich zu wenig Nutzer über die Verhaltensweisen Sozialer Netzwerke bewusst: *„Das wichtigste was sie Politik tun kann, ist über Gefahren aufzuklären, den Benutzer dazu zu bringen eine Haltung einzunehmen, bei der er selbst umsichtig und vorsichtig ist mit seinen Daten umgeht. Es geht darum, dass der Nutzer realisiert, dass einmal preisgegebene Daten weg sind – das haben die meisten nämlich noch nicht realisiert. Es gibt sehr viele die haben das noch nicht verstanden und an diesem Punkt wäre Aufklärungsarbeit angebracht.“* (Lorenz, 2012)

Es muss auch im IT-gestützten Umfeld Sozialer Netzwerke von Qualitätsunterschieden in der Datensicherheit und der Datenverarbeitung ausgegangen werden. Warum aber ein TÜV-Siegel oder Qualitätsprädikat im Falle der Sozialen Netzwerk-Angebote nicht ausreichend ist, darüber gibt ein anderer Text von Akerlof Aufschluss:

In seinem Werk „Animal Spririts“ beschreibt George Akerlof zusammen mit Robert Shiller, dass die Ökonomie in ihren makroökonomischen Modellen, das Konzept der Fairness zumeist außer Acht lässt (Akerlof/Shiller, 2009, S. 41ff.). Neben der

Rationalität ist Fairness jedoch ein wichtiger Vertrauen stiftender Faktor des Wirtschaftens. **Demnach wird die Datentransparenz von Betreibern nicht nur nach rational-ökonomischen Maßstäben bemessen, sondern auch und vor allem nach dem Grad der Fairness den diese Angebote liefern**. Ernst Fehr und Simon Gächter, bekannt für ihre empirischen Fairness-Studien fanden im Jahr 2000 heraus, **das unfair agierende Kooperationspartner nach wiederholter Interaktion entlarvt und nach Möglichkeit sogar von ihren Interaktionspartnern bestraft werden** (Fehr/Gächter, 2000, S.45 ff.). Menschen, wie auch Affen, verfügen über eine Abneigung gegenüber egoistischem Verhalten ihrer Artgenossen. Bestrafungsaktionen von egoistischen Individuen lösten im dorsalen Striatum des Gehirns, eine ebenfalls für das Belohnungs-Empfinden bekannte Hirnregion, erhöhte Aktivität aus. Der Prozess der Sanktionierung der unfair agierenden Kooperationspartner fand auch dann statt, wenn den Bestrafenden dafür Kosten entstanden (Fehr/Gächter, 2000). Akerlof und Shiller transferieren diese Studienergebnisse auf den **Einfluss von Fairness auf das Wirtschaftsleben**. Ein Beispiel für als unfair empfundenes Wirtschaften ist die Erhöhung der Kraftstoffpreise an Ferien- und Feiertagen. Diese Preiserhöhung wird vom Endverbraucher als unfair empfunden, da dem Tankstellenbetreiber keine höheren Beschaffungskosten des Sprits entstanden sind. Die Preiserhöhung wird als egoistische Bereicherung des Tankstellenbetreibers wahrgenommen (Akerlof/Shiller, 2009, S. 43ff.).
Übertragen auf die Betreiber Sozialer Netzwerke bedeutet dies, dass auch sie fair agieren müssen. Die **Zahlungsbereitschaft für gefühlte Datensicherheit** könnte im Rahmen bisher vorherrschender Kostenlos-Leistungen vom Endverbraucher als unfair empfunden werden.

Zudem zeigte die Abstimmung über die neuen Facebook-Nutzungsbedingungen am 08.06.2012 eine mangelnde Nutzerbeteiligung. Diese mag zum einen daraus resultieren, dass nicht alle deutschen Facebook-Nutzer über die Abstimmung informiert waren (Reißmann, 2012). Jedoch ist die mangelnde Teilnahme zum anderen sicherlich auch darauf zurückzuführen, dass eine generelle Nutzerträgheit beim Lesen der Nutzungsbedingungen und bei AGB’s zu verzeichnen ist (Kempf, 2012). Das Belohnungszentrum im Gehirn erhält keinen Reiz-Impuls bei der Beteiligung an einer derartigen Abstimmung oder bei der Selbstselektion

nutzerfreundlicher Profil-Einstellungen. Die Betreiber Sozialer Netzwerke müssen daher Anreize für die Nutzer finden, damit sie sich ihrer „pivacy-by-default"-Möglichkeiten stärker bewusst werden. Gleichzeitig müssen **die Betreiber das Vertrauen ihrer Nutzer gewinnen und fördern**. Für Facebook, dass sich seit dem Börsengang in der Öffentlichkeit wesentlich geschäftstüchtiger präsentiert und laut Spiegel Zuckerberg zum Chef erhebt und nicht länger die Nutzer oder gar die Aktionäre *„Zuckerberg ist Chef, nicht die Aktionäre, nicht die Nutzer. Außerdem bezeichne sich Facebook nun als "Controller" und nicht mehr als "Host"* "(Reißmann, 2012), wird dies eine besondere Herausforderung werden.

So ungewohnt der Ansatz scheint, dass Nutzer für den Schutz selbst preisgegebener Daten zahlen sollen, so ungewöhnlich ist auch der Gedanke dass die Betreiber Sozialer Netzwerke die eigenen Nutzer zu mehr Datenschutz anregen sollen.

Ein Unternehmen wie Facebook kann nur dann mit einem Reputationswachstum rechnen, wenn es Strukturen baut, die innerhalb der Facebook-Gemeinschaft Vertrauen stiften. Wie aber können die trägen User dazu angeregt werden, sich an Abstimmungen und Privatsphäre-Einstellungen vermehrt zu beteiligen?

Eine Möglichkeit neben der Bildung von Vertrauen oder der Zuweisung eines Qualitätsmerkmals, ist es, das Netzwerk-Angebot mit einem Nutzen zu versehen.

Ein Appell an den menschlichen Spieltrieb, stellt beispielsweise für viele einen Zusatznutzen dar. Werden die Abstimmungsprozesse über Privatsphäre-Einstellungen mit einer geringen Hemmschwelle, z.B. in Form eines interaktiven Spiels präsentiert, würden die Betreiber der Sozialen Netzwerke einen „gambling"-Nutzen für ihre Mitglieder generieren.

Die Ökonomie berücksichtig bei der Betrachtung von Spielmechanismen zumeist den Grad der Risikoaversion von Einzelakteuren (Benz, 2004, S. 18ff.). Jedoch trifft die Beobachtung von menschlichem Spielverhalten ebenfalls eine Aussage über den Nutzengewinn, den ein inkonsistenter Entscheidungsprozess wie er beim Spielen vorliegt, mit sich bringt (Le Menestrel, 2001). Je nach Ausgangssituation, kann ein Akteur Wohlbefinden im Spielprozess erfahren (Pascal, 1970). Dieses kann durch zwei Bedürfnisse entstehen. Das Spiel um einen potentiellen Gewinn, der einen Glücksmoment auslöst. Oder aber das Spiel um des Spielens willen, um Langeweile zu überwinden oder z.B. Geselligkeit zu erfahren. *„Die Lust oder Unlust zum Spielen ist eine Frage des Prozesses nicht der Konsequenzen"* (Le Menestrel, 2001).

Wenn Menestrels Aussage zutreffend ist, dann wäre eine spielerische Abstimmung über AGB's ein Zusatznutzen für die Teilnehmer und zwar unabhängig vom Ausgang der Abstimmung.

5.3 Mündige Digital Natives – Ein „privacy-by-default"- Ansatz nach Elinor Ostrom

Aus den beiden voran gegangenen Kapiteln 6.1 und 6.2 lässt sich die Unterscheidung von drei verschiedenen ökonomischen Lösungsansätzen für das Datenschutz-Dilemma ableiten:

1. Die **marktliche Lösung** in Form von Wettbewerbsmodellen unterstützt durch „signalling".

2. Die **staatliche Lösung**, z.B. durch die Einführung einer dritten Instanz, die eine Risikobewertung vornimmt, so wie Akerlof es vorschlägt.

3. Die **Lösung durch ein Kooperationsmodell**, wie Elinor Ostrom es vorschlägt. Sie spricht sich für kooperatives Ressourcen-Management unter den beteiligten Stakeholdern aus und entbindet somit Markt und Staat aus ihrer alleinigen Vormachtstellung **(Ostrom, 2011)**.

Elinor Ostrom (Wirtschafts-Nobelpeisträgerin 2009) reflektiert in ihren Arbeiten wirtschaftswissenschaftliche Modelle wie Garrett Hardins „The tragedy of the Commons" **(Hardin, 1968)**, die Spieltheorie nach John Forbes Nash **(Nash, 1996)**, und der Theorie des Marktes nach Adam Smith **(Smith, 1976)**. Ostrom legte in ihrem Werk „Governing the Commons" **(Ostrom, 1990 A)** besonderes Augenmerk auf Olsons Theorie „The Logic of collective action" **(Olson, 1965)**. Dieses Kapitel beschäftigt sich damit, inwiefern der Datenschutz- Interessenskonflikt in Analogie zu einem kollektiven Ressourcen-Management-Ansatz gesehen werden kann.

Ostrom interessiert in ihrem Werk „*Was mehr wird wenn wir teilen*" durch welche Bedingungen Kooperation entsteht und wie kooperatives Ressourcen-Management gelingen kann **(Ostrom, 2011, S.12)**. Diese Überlegungen lassen sich auch auf die Datenschutz-Debatte übertragen. Angenommen die **digitale Information hat komplexe tangible und intangible Attribute**, dann ist es für den Datenschutz eine Herausforderung insbesondere den Bereich der intangiblen Attribute zu ordnen, ohne

ihn allzu stark zu regulieren. Ostrom befasste sich bereits mit den Besonderheiten des Prozesses der fortschreitenden Digitalisierung und machte folgende Beobachtung:

Digitale Ressourcen (Daten) unterliegen intransparenten Nutzungsregelungen. Es gibt keine eindeutigen Grenzregelungen für die Wandelbarkeit der Eigentumsrechte, ebenso wie für Reproduktions-Möglichkeiten digitaler Daten. Auch geographisch, sonst ein verlässliches Attribut bei Eigentumsansprüchen, ist der Datentransfer schwierig einschränkbar, denn **Nutzer-Gruppen kommunizieren nicht mehr nur lokal, sondern auch regional, national und global (Hess/Ostrom, 2003).** Am Beispiel von Facebook wird auch die zeitliche Uneinschränkbarkeit von Daten-Eigentum deutlich. Ein Unternehmen, welches eine Information über ein neues Produkt bei FB veröffentlicht, verliert die Kontrolle über Häufigkeit der Rezeption und Reproduktion des Beitrags, ebenso wie über die eigenen Speicher-Spuren im Internet **(Netzwertig, 2010)**.

Die allgemeine Verunsicherung und Intransparenz über Daten-Eigentum wird dadurch verstärkt, dass die Gesetzgebung den Online-Verbreitungsmechanismen zeitlich erheblich unterlegen ist. Eine zentrale Regulation ist auch dadurch zum Scheitern verurteilt, da ein **Bündel von Institutionen existiert, welche Regeln vorgeben. Dadurch entsteht eine enorme Intransparenz und Regelvielfalt (Ostrom, 1990 A).** Ostroms Reaktion auf diese Problematiken ist die Ablehnung einer Zentralisierung. Bezogen auf Ressourcen mit partiell oder temporär unklaren Besitzstrukturen im Allgemeinen entwickelt sie folgenden Vorschlag:

Eigenverantwortung für Entscheidungen z.B. durch einen privacy-by-default- Ansatz sollte gefördert werden. Konsequenzen und Verantwortung für Datenschutzmanagement-Entscheidungen oder auch Teilnahme in einem bestimmten Netzwerk sollten besonders den Nutzern im Vorfeld klar sein. Ostrom erklärt diesen Prozess anhand der Regeln der Straßenverkehrsordnung (das Straßenverkehrsamt hat eine ähnliche Rolle wie die Betreiber Sozialer Netzwerke). Das Straßenverkehrsamt erlässt und gestaltet Regeln für alle Verkehrsteilnehmer, um dem Verkehr Ordnung und Struktur zu verleihen. Wenn aber das Straßenverkehrsamt sich nicht über die Konsequenzen dieser Regeln im Klaren ist, kann es zu unerwarteten und

verheerenden Auswirkungen kommen. Lösbar ist dieses Dilemma dann nur, indem sich die Nutzer der Konsequenzen bewusst werden **(Ostrom, 2005, S. 4)**.

Selbstverpflichtung und Selbstbestimmung der Beteiligten sind in Ostroms Konstrukt essenziell. Auch der Grad der Datentransparenz zwischen Nutzern und Betreibern steht in einem derartigen Konflikt. Sogar die Theorie des „free ridings" von Milton Friedman (Wirtschafts-Nobelpreisträger, 1976), findet Anschluss an Ostroms Gedanken. Friedman negierte die Existenz von kollektiver Vernunft. Gerade bei größeren Gruppen verwies er stets auf das Problem des „free ridings", der Nutzung einer gemeinsamen Ressource ohne dafür zu zahlen **(Friedman, 1975)**. Im Falle von Sozialen Netzwerken muss gefragt werden, wer eigentlich die „free rider" sind? Denn diejenigen die Daten nutzen ohne dafür zu zahlen sind die Betreiber. Also kann folglich auch von den Betreibern eine Gegenleistung erwartet werden z.B. eine Schutzleistung. Hierzu müssten aber die Nutzer ein Arrangement mit den Betreibern finden.

Ostrom, die ebenfalls das Problem des „free ridings" bemerkt, ist der Auffassung dass institutionelle Arrangements nur dann zu Stande kommen, wenn sie durch eine Selbstregulation charakterisiert sind. Der Nutzer muss also eine Kontrollmöglichkeit über die ihm vom Betreiber entgegengebrachte Leistung erhalten **(Ostrom, 1990 B)**. Ostrom definierte Voraussetzungen für den Erfolg des gemeinschaftlichen Ressourcen-Managements **(Ostrom, 2005, S.253)**:

1.) Ein gemeinschaftliches Verständnis für die Situation und die jeweilige Situation anderer Interessensgruppen muss entstehen (Konsensbildung).
2.) Die Transaktionskosten für die Beteiligten müssen gering bleiben, um eine geringe Eintrittsbarriere zu garantieren.
3.) Ein Vertrauensvoller Austausch bildet die Basis.
4.) Die Arrangements entstehen in Autonomie, Freiwilligkeit und Eigenständigkeit.

Ein Lösungsansatz, der zur **Aufklärung der Nutzer** über ihre Verhandlungsposition beiträgt, ist bereits in Schulen für die Problematik zu sensibilisieren und den Nutzer zu einem Selbstschutz zu befähigen.

Der Mecklenburg-Vorpommersche Datenschutzbeauftragte Reinhard Dankert setzt auf mündige Bürger, die sich auch **im Internet bewusst und verantwortungsvoll bewegen**. Aus diesem Grund wird es an Mecklenburgischen Schulen ab dem Schuljahr 2013 Unterrichtsstunden für Fünftklässler geben, in denen Schüler einen verantwortungsbewussten Umgang mit persönlichen Daten im Internet lernen sollen. *"Nicht alles, was möglich ist, sollte man im Internet tun und preisgeben"* (Dankert in: dpa 2012 B). Geplant ist, dass zwei Schüler pro Klasse die Rolle von **Medienscouts** übernehmen. **Sie sollen ihre Mitschüler über Datenschutz in Sozialen Netzwerken aufklären**, da die Lehrerschaft vermutet, dass die Schüler eher auf Gleichaltrige hören. Geplant ist eine Laufzeit des Projektes bis 2016. Während dieser Zeit sollen auch Schulsozialarbeiter und Lehrer eine Fortbildung in Sachen Datenschutz erhalten, um die Medienscouts zu unterstützen.

Die Überlegung, dass jüngere Generationen ein anderes, selbstverständlicheres Empfinden von digitaler Mediennutzung und Datenpreisgabe haben steckt bereits im Begriff **Digital Natives** (Palfrey und Grasser, 2008). Gemeint ist die **junge Generation von Internet-Nutzern**, die in einer Umwelt mit digitalen Technologien (z.B. dem Ubiquitous Computing ermöglicht durch das Internet) aufwachsen. Der Trend geht dahin, dass gerade jüngere Generationen zu den „early adopters", also zu den Pionieren, von Sozialen Netzwerk- Angeboten zählen. Dankerts Idee erscheint aus dieser Perspektive plausibel: Es sollten nicht die **Digital Immigrants** (also ältere Generationen, die Soziale Netzwerke skeptisch sehen, da sie nicht mit ihnen aufgewachsen sind) die pädagogische Aufgabe übernehmen auf die Risiken von zu viel Datentransparenz hinzuweisen (Palfrey und Grasser, 2008)

6 Prüfung der Eingangshypothese und Resümé

Die Eingangshypothese, dass Nutzer und Betreiber ein gemeinsames wohlfahrtsökonomisches Datentransparenz-Optimum wählen, **muss sowohl als falsch wie auch als richtig betrachtet werden.**

Als falsch muss die Hypothese gelten, da sich kein wohlfahrtsökonomisches Datentransparenz-Optimum in dem Sinne eines tatsächlichen Optimums finden lässt. Die Kurven-Verschiebung, die aufgrund der adversen Selektion der Nutzer

geschieht, lässt eine Differenz zwischen dem „gefühlten“ und dem „wirklichen“ Optimum entstehen (siehe Kapitel 3.4 Abb. 3 und Abb. 4).

Als richtig muss die Hypothese gelten, weil die Betrachtung der handelnden Akteure zeigt, dass das Erreichen eines Datentransparenz-Optimums durch ein Arrangement von Betreibern und Nutzern wahrscheinlicher ist, als durch politische und gesetzliche Interventionen. **Die Deutsche Gesetzgebung** (wie auch der generelle Ablauf demokratischer Prozesse), **ist aufgrund ihrer Trägheit nicht geeignet punktuelle Lösungsmechanismen für die Datentransparenz-Problematik zu generieren**. Die Entwicklung der technologischen Möglichkeiten ist um ein vielfaches schneller als die Entschlussfreudigkeit der Gesetzgeber im demokratischen Prozess.

6.1 Rolle der Politik

Die Rolle die der Politik zufällt, ist vielmehr die Schaffung eines ausgeprägten **Nutzer- Bewusstseins** und somit auch eine **Schärfung der Wahrnehmung** für die Problematiken der Datenpreisgabe in sozialen Netzwerken. Der Staat hat in Bezug auf die Datentransparenz im Internet eine Schutzfunktion inne, die er am besten durch eine umfassende **Aufklärungsarbeit** und **retrospektive Sanktionierungsmaßnahmen** erfüllen kann. Die Entwicklung von **Gesetzen für den Internet-Datenmarkt ist dringend erforderlich**. Diese Auffassung teilen Politiker wie Datenschützer. Bundestagspräsident Norbert Lammert ist der Ansicht, dass *für die so genannten Neuen Medien, für Facebook, Twitter, Xing und Co. dieselben Rechtsstrukturen gelten müssen, wie auch in der sonstigen Wirtschaft und für die haptischen Medien. Es sollte keine Zensuren oder Beeinträchtigungen geben, dennoch muss der Deutsche Rechtsstaat auch im Internet Geltung haben* (sinngemäßer Wortlaut Norbert Lammerts am 18. Juni 2012 auf einer Veranstaltung der Konrad Adenauer Stiftung in der Ruhr-Universität in Bochum). Rena Tangens von der Datenschutzorganisation FoeBuD e.V hält eine *„Durchsetzung geltendes Rechtes“* ebenfalls für dringend notwendig, sie fordert, dass die staatlichen Stellen *„die Aufsichtsbehörden mit den entsprechenden Mitteln ausstatten und unabhängige Kontrollen und Sanktionen durchsetzen. Innenminister Friedrich muss aufhören, dem Verbraucherschutzministerium und allen Datenschutzbeauftragten [...], in den Rücken zu fallen. Der Innenminister lässt sich von Facebooks Lobbyisten instrumentalisieren, wenn er öffentlich sagt, dass eine Selbstverpflichtung ja schon ok sei. Nein, ist sie nicht. Auch Facebook muss sich an geltendes Gesetz halten.“*

(Tangens, 2012). Außerdem befürchtet Tangens, dass sich andere Social Networks, die sich um angemessene Datenschutz-Praktiken bemühen benachteiligt fühlen könnten, wenn Politiker Großnetzwerken wie Facebook zu viele Freiheiten einräumen.

Seitens politischer Maßnahmen müssen wir, trotz der berechtigt geforderten Durchsetzung bestehenden Rechts, jedoch eine **nachgelagerte Ahndung von Vergehen akzeptieren**. Ein **präventives Wirken ist weitaus schwieriger**, weil die technologischen Neuerungen des Datenmarktes kaum absehbar sind.

Eine häufig diskutierte Überlegung der Politik ist jedoch die Überlegung **Betreiber Sozialer Netzwerke einem sogenannten Marktortprinzip zu unterwerfen**. Dies bedeutet, dass das Datenschutzrecht des Landes gilt, in dem die Dienstleistungen angeboten werden. Bislang herrscht ein rechtliches Niederlassungsprinzip, dass das Unternehmen an die Rechte des Niederlassungs-Standorts bindet (Schröder, 2012).

Aufgabe der Politik wird es ebenfalls sein die Monopolbildung der Betreiber Sozialer Netzwerke einzudämmen. Axel Fischer schlägt eine Fallspezifische Regelung vor: „*Welche Maßnahmen zur Sicherung eines funktionierenden Wettbewerbs von Marktteilnehmern zum Wohle deren Kunden mit Blick auf das Internet sinnvoll sein können, hängt vom konkreten Fall ab.*“ (Fischer, 2012, Frage 7). Während Peter Schaar für eine klare Entkopplung plädiert: „*Es gibt Ansätze die ähnlich sind wie im Kartell-Recht. Das heißt, dass man durchaus nicht nur bei verkauften Gütern, sondern auch bei solchen Datendiensten den Markt beobachtet und gegebenenfalls zu Entflechtungen beiträgt. Ein Anbieter der E-Mail und andere Kommunikationsmöglichkeiten anbietet kann dann in Zukunft nicht mehr zusätzlich auch noch ein soziales Netzwerk betreiben. Das wäre ja eine Form von Entflechtung, die denkbar wäre.[...]*“ (Schaar, 2012, Frage 13).

Die Deutsche Politik steht vor folgenden Herausforderungen:

1.) **Eine Durchsetzung des geltenden Rechts nach dem Marktortprinzip anzustreben.**

2.) **Das Bewusstsein der Bürger über das strukturelle Ungleichgewicht zwischen den Betreibern Sozialer Netzwerke und deren Nutzern (Schaar, 2012, Frage 12) zu Fördern. Beispielsweise durch Aufnahme von IT- und**

Datenschutzthemen in den regulären Lehrplan, sowie durch verstärkte Presseberichterstattung.

3.) **Monopolbildung der Betreiber Sozialer Netzwerke zu verhindern.**

4.) **Personen- / Identitätsschutz, sowie Wahrung der Persönlichkeitsrechte**

5.) **Vermeidung von Profilbildung** (Punkt 4 und 5 sind abgeleitet aus Peter Schaars Vorschlägen in Kapitel 3.3)

6.) **Nach Lorenz: Anreize setzen und Angebote schaffen um den Nutzer zu mehr Vorsicht bei der Datenpreisgabe zu bewegen.**

6.2 Rolle der Wirtschaft/Unternehmen

In diesem Kapitel-Abschnitt wird die Rolle von Unternehmen analysiert, die nicht der IT-Branche angehören. Welche **Verantwortung** müssen Unternehmen tragen, wenn es um den Datenschutz im digitalen Zeitalter geht?

Meist wird bei dem Thema Datenschutz in der Wirtschaft von der **Vorratsdatenspeicherung** ausgegangen. Die Vorratsdatenspeicherung wurde zunächst vom Bundesverfassungsgericht im Jahr 2010 als verfassungswidrig erklärt. („Stoppt-VDS“-Blog, in: Tangens, 2012, Frage 3). Unser Innenminister und die EU-Innen-Kommissarin haben das Thema kürzlich erneut zur Diskussion gebracht. Die Vorratsdatenspeicherung sieht vor u.a. Telekommunikationsdaten (einschließlich SMS- und Internetdaten) von Bürgern auch nach Rechnungserstellung noch zu speichern, um bei der **Verbrechensaufklärung im Verdachts- oder Ermittlungsfall auf Sie zurückgreifen zu können.** Durch diese Speicherung ist jedoch u.a. die Erstellung von Bewegungsprofilen möglich, die auch für **Arbeitgeber im Rahmen der Mitarbeiterüberwachung interessant sein können**, z.B. bei der Frage welche Zwischenstopps der Mitarbeiter auf einer Dienstreise einlegt. Aus privater, wie geschäftlicher Kommunikation können **Verhaltensanalysen** nicht nur von Bürgern, sondern auch von Mitarbeitern erstellt werden. Diese Kontrollmöglichkeiten generieren in Wirtschaftsunternehmen die unter einem gewissen Marktdruck stehen, allein durch ihr Vorhandensein eine große Versuchung. **Gutes Unternehmertum jedoch erfordert Handlungsspielräume anstatt Kontrolle. Daher sollten Unternehmen eine akribische**

Vorratsdatenspeicherung ablehnen, auch wenn dies den Kontrollverlust über die eigenen Mitarbeiter oder Mitwettbewerber bedeutet.

Die Einhaltung dieser Norm begrüßt auch Peter Schaar. Er tritt dafür ein, *„dass die freie und unbeobachtete Telekommunikation als ein wesentliches Element unserer demokratischen Wissens- und Informationsgesellschaft gewährleistet bleibt. ‚Es darf nicht so weit kommen, dass jeder Mausklick oder jeder Abruf von Inhalten aus dem Internet protokolliert wird.' "* (BFDI, 2006).

Zudem ist Schaar davon überzeugt, dass Unternehmen den Datenvorrat, egal durch Soziale Netzwerke oder durch eigene Datenerhebung entstanden, ökonomisch zu Nutzen gedenken: *"Der Staat bedient sich hier der Hilfsdienste der Wirtschaft, indem er sie verpflichtet, von ihr nicht bzw. nicht mehr benötigte Daten zu speichern. [...] Ich befürchte, dass diese Daten nicht nur für die Aufklärung schwerer Verbrechen genutzt werden. So fordert die Musikindustrie bereits seit längerem den Zugang zu Verkehrsdaten von Teilnehmern sog. Tauschbörsen im Internet."* (BFDI, 2006).

Für Unternehmen bedeutet dies, zugleich ihre eigenen Daten vor dem Zugriff Dritter zu sichern und gleichzeitig einen **eigenen Verhaltenskodex für den Umgang mit digitalen Daten und auch mit Sozialen Netzwerken zu entwickeln**. Um eine höhere Datenschutz-Qualität vor allem bei der Nutzung Sozialer Netzwerke zu entwickeln und eine Spionage-Kultur zu vermeiden, sollten Unternehmen, wie bereits in Kapitel 5.1 und 5.2 vorgeschlagen in den Datenschutz investieren. Ob Betreiber Sozialer Netzwerke künftig vertrauenswürdige Produkte speziell für Unternehmen anbieten werden. Oder ob eine Bepreisung von Datenschutzgarantien stattfindet, hängt auch davon ab, wie stark Unternehmen diese Leistungen nachfragen.

Unternehmen haben daher die Pflicht:

1.) Sich selber über die Relevanz von Datenschutz bewusster zu werden und eine Verhaltensweise festzulegen.

2.) Sicherere Dienstleistungen bei den Betreibern Sozialer Netzwerke einzufordern und nachzufragen.

3.) Druck auf Betreiber Sozialer Netzwerke und IT-Dienstleister auszuüben, indem eine Vermeidung von Werbeschaltungen und der Integration des Like-Buttons so lange stattfindet, bis eine Verbesserung der Leistungen eingetreten ist.

6.3 Rolle der Betreiber

Die große Herausforderung der Betreiber Sozialer Netzwerke wird es sein, **das Vertrauen der Nutzer langfristig für sich zu gewinnen und aufzubauen**. Bislang erwecken die Betreiber Sozialer Netzwerke **den Eindruck sich auf Kosten der Nutzerdaten selbst bereichern zu wollen**. Insbesondere Facebook verzeichnet seit seinem Börsengang geringe Einnahmen. Rena Tangens rechnet mit einem verstärkten Investoren-Einfluss auf das Soziale Netzwerk: *Aktiengesellschaften sind Treuhänder des Geldes ihrer Aktionäre. Das heißt, Facebooks oberste Aufgabe ist, das Geld der Aktionäre zu mehren. Und das heißt im Klartext [...]: noch mehr Auswertung von Daten, mehr Werbung, und Aneignung der Inhalte der Nutzer/innen (wie in den neuen Nutzungsbedingungen geschehen.)"* (Tangens, 2012, Frage 9). Auch die mediale Aufmerksamkeit richtet sich vermehrt auf Facebooks Geschäftsmodell und seine Zukunftsperspektiven: „*Facebook steht unter Zugzwang. Die Werbung ist die mit Abstand wichtigste Einnahmequelle.[...] Die Anzeigen-Plattform «Facebook Exchange» soll es einfacher und damit attraktiver machen, in dem Sozialen Netzwerk zu werben. Und endlich tut das Unternehmen etwas, um die bislang weitgehend werbefreie Fläche auf Smartphones und Tablet-Computern zu füllen."* (Welt Online, 2012).

Durch die vermehrte Werbung und die steigende Anzahl von so genannten „sponsored stories" lassen sich zwar höhere Einnahmen generieren, dennoch muss Facebook mit einem **kongruent sinkenden Nutzerinteresse** rechnen, wenn der **Übersättigungspunkt für personalisierte Werbung** erreicht wird. Eine wichtige Gegenmaßnahme muss es daher sein, das **Nutzervertrauen** zu gewinnen und weiterhin einen **Mehrwert für Facebook-Mitglieder** bereit zu stellen. Geschieht das nicht, stehen die Nutzerinteressen den Betreiberinteressen entgegen.

Nutzervertrauen generieren, aber wie? Eine wertvolle Maßnahme um das Nutzervertrauen zu fördern ist es den Nutzern ein **Mitbestimmungs- und Mitgestaltungsrecht an den Facebook-Richtlinien** zu gewähren. (Artikelzitate

über die Abstimmung einfügen) Zum einen muss dafür eine **umfassende Transparenz** über die Verwendung der Nutzerdaten hergestellt werden. Zum anderen muss dem Nutzer Autonomie bezogen auf die eigenen Daten eingeräumt werden. Zu diesem Zweck kündigte Facebook im Juni 2012 eine neue Funktion für Nutzer an: *„Künftig sollen die mehr als 900 Millionen Mitglieder von Facebook ihre Einträge korrigieren können. [...] Ein Posting komplett zu löschen ist nach wie vor möglich. Allerdings gilt die Editierfunktion nur für Kommentare, nicht für Statusmeldungen.“* (Sueddeutsche, 2012 C). Die Möglichkeit einmal veröffentlichte Beiträge und Fotos ganz zurückzuziehen besteht nach wie vor nicht. Das von der Politik geforderte **digitale Radiergummi**, wäre eine sehr gute Möglichkeit den Nutzern das **Selbstbestimmungsrecht** zurück zu geben (Heise, 2011A), sofern es nicht nur auf Bilder beschränkt bleibt. Datenschützerin Tangens sieht die Einführung eines digitalen Radiergummis kritisch: *„Das Verfallsdatum wird wenig helfen. Denn wer weiß schon heute, was ihm oder ihr morgen peinlich oder schädlich sein könnte? Das vom Innenministerium sogenannte "Radiergummi“ [...] ist ein irreführender Begriff. Die vorgestellte Implementation war das Mitgeben eines Verfallsdatums bei Bildern. Und das ist a) aus oben genannten Gründen nicht praktikabel und b) kann es die Löschung nicht garantieren.“* (Tangens, 2012, Frage 6). **Ein digitales Radiergummi, wäre nur dann sinnvoll wenn es von Facebook, bzw. dem Betreiber selbst, eingeführt würde**. Ein Nutzer sollte dadurch die Chance bekommen, von ihm veröffentliche Nachrichten, Statusmeldungen und Videos ebenso zurückzunehmen, wie Bilder. **Bislang werden nur partielle Lösungen seitens der Betreiber präsentiert.** Das die technische Lösung nur für Bilder gilt, stellt IT-Spezialist Stefan Lorenz richtig: *„Das X-Pire!-Verfahren[13] ist ohne weiteres auf andere Dateien ausweitbar. Was wir durch die Verschlüsselungs-Mechanik erreicht haben ist, dass nach zeitlichem Verfall des Schlüssels das Bild oder die Datei nachträglich nicht mehr verfügbar ist oder eingesehen werden kann. Hätten Sie Ihre Fotos also mit einem Schlüssel geschützt, könnte ich heute nicht mehr sehen, was Sie früher in Sozialen Netzwerken getan haben.“* (Lorenz, 2012, Frage 2). Auch die Aussage, dass der technische Datenschutz nur eine Teil-Lösung darstellt, rückt der X-Pire!-Entwickler ins rechte Licht. Denn bevor eine veröffentlichte Datei verfällt, ist sie für alle sichtbar und es besteht die Möglichkeit diese Datei zu

[13] X-Pire! ist eine Verschlüsselungs-Software, die es ermöglicht Dateien, Dokumente und Fotos mit einem Verfallsdatum zu versehen.

kopieren bzw. zu Vervielfältigen, wie Lorenz schildert: „*Ich könnte mir aber durchaus heute all Ihre ungeschützten Bilder und Dateien kopieren und sichern und könnte über eine Dauer die mir beliebt darüber verfügen. Die Kritik ist aus diesem Grund, dass die Software nur einen unzureichenden Datenschutz bietet.*“ (Lorenz, 2012, Frage 2).

Die Frage ob ein unzureichender Datenschutz nicht immer noch besser ist als gar kein Datenschutz werden Nutzer wie Betreiber künftig näher erörtern müssen. Die aktuelle Situation in der Daten unwiderruflich freigegeben sind, wird sich ändern müssen, will man beiderseitig Vertrauen bilden und nicht als halbherzig in der Durchführung gelten.

Zudem ist es wichtig, dass Betreiber Sozialer Netwerke generell die Problematik der Nutzervoreinstellungen adressieren und öffentlich (z.B. in Blogs/Foren) reflektieren. Der Nutzer muss den Eindruck haben, dass auf der Betreiberseite ein Bewußtsein, über die von ihm festgestellten Unzulänglichkeiten herrscht.

6.4 Betreiber müssen Nutzern Anreize zum Datenschutz bieten

Eine weitere Schwierigkeit der Betreiber, den Nutzer über seine Datenschutzmöglichkeiten nicht nur aufzuklären, sondern ihn auch zu einer aktiven Partizipation zu bewegen, ist die bereits in Kapitel 5.2 erwähnte **Trägheit der Nutzer** (Kempf, 2012). Datenschutzeinstellungen regelmäßig vorzunehmen, ist wenig attraktiv, der Nutzer verspürt keinen direkten Mehrwert.

Umso selbstverständlicher sollte es für Betreiber sein, diesen Mehrwert zu generieren, denn nur zufriedene Nutzer bleiben dem Netzwerk dauerhaft erhalten. Welche Anreize aber könnten zu einer Steigerung des Vertrauens führen?

Der **Schutz der Urheberrechte von Musik und Videos** auf der einen Seite und die **Unlust der Nutzer sich mit den Schutzmöglichkeiten des eigenen Profils zu befassen**, ergeben zusammengenommen eine Lösungsmöglichkeit. Musikplattformen wie Youtube gehen vermehrt dazu über Musikvideos zu sperren, da der kostenfreie Konsum von Musik überhand nimmt und die Musikindustrie Ihre Produkte nicht mehr absetzen kann**. Kostenlos-Musik ist und wird immer mehr ein knappes Gut**, das wiederum weckt Begehrlichkeiten des Nutzers. Der Nutzer ist nun gezwungen seine Musik bei den gängigen Musikportalen wie iTunes und

Amazon zu bezahlen. Ein Song im iTunes-Store kostet durchschnittlich 1,29 €, ein Lied bei Amazon im Schnitt 0,99 €. Im Vergleich zum Vorjahr haben beide Anbieter bereits jetzt eine Preiserhöhung von 0,20 € pro Titel durchgeführt. Soziale Netzwerke wie Facebook könnten dank dieser Entwicklung nun als Anreiz Kostenlos-Musik bzw. einen kostenfreien Zugang zu einer TV-Sendung als Lohn für das Ändern der Nutzereinstellungen oder das Lesen der AGB freigeben. **Durch Werbekooperationen oder den Erwerb von Lizenzrechten, kann dem Nutzer nun ein vermisster Mehrwert angeboten werden.** Die zusätzlichen Kosten für einen administrativen Mehraufwand könnten Soziale Netzwerke durch das vergünstigte Anbieten von Content wieder zurückholen, z.B. durch den Einkauf von 3 Songs zu dem Preis von 0.99€ nach getätigter Sicherheitseinstellung des Nutzers. Selbiges Angebot könnte auch für Apps und Onlinespiele entstehen.

Ein paralleler Prozess zum Schutz der Urheberrechte ist bei der Preiserhöhung von Speichermedien zu beobachten (ZDF Heute, 01.06.2012). Die geplante Preiserhöhung von USB-Sticks, Festplatten und Laptops, die daraus resultiert, dass anteilig der Musik- und Filmindustrie eine Entschädigung für den Diebstahl geistigen Eigentums gezahlt werden soll, ist problematisch. Bislang waren Speichermedien wie USB-Sticks u.a. kostenlos als Werbegeschenke etabliert. Erhöhte Preise könnten die Endnutzter zu einer stärkeren Auslagerung ihrer Daten in Clouds oder Soziale Netzwerke bewegen. Die Betreiber Sozialer Netzwerke könnten dieser Situation mit Speicherplatzangeboten entgegenwirken.

Eine weitere Schwierigkeit die Nutzer dazu zu bewegen, selbst aktiv Datenschutz-Einstellungen vorzunehmen, liegt in der **intransparenten und somit zeitaufwendigen Nutzeroberfläche**. Wer seine Einstellungen ändern möchte, muss viel Zeit und Geduld investieren um dies zu tun (Frickel, 2012). Das bedeutet eine **hohe Hemmschwelle** auf der Nutzer-Seite. Um diese Hemmschwelle zu verringern wäre eine Möglichkeit ähnlich wie Fluggesellschaften es tun, **Sicherheitsvideos anzubieten**, die dem Nutzer eine **interaktive Anleitung** gewähren. Es ist auch möglich in Form eines Quiz den Nutzer regelmäßig eine Selbstprüfung seiner Einstellungen vornehmen zu lassen.

Sobald es einem Sozialen Netzwerk Betreiber gelingt, den **Spieltrieb der Nutzer zu wecken** oder ihm eine **Unterhaltung** zu bieten, stehen einer weiteren Interaktion (auch über Datenschutz-Themen) alle Wege offen.

6.5 Rolle der Nutzer

Die Nutzer sozialer Netzwerke stecken in einer Paradoxie. Zum einen gewährt ihnen die Teilnahme an sozialen Netzwerken einen **Mehrwert durch einen Zugewinn an Anerkennung, durch spaßige und spielerische Zerstreuung, sowie durch vereinfachte Arbeitsorganisation**. **Zum anderen geben die Nutzer die Kontrolle über ihre Daten, Bilder und Inhalte komplett ab und können fortan nicht mehr nachvollziehen wann und wo ihre Daten gespeichert und kopiert werden**. Über das was mit den eigenen Daten geschieht ist sich der Nutzer völlig im Unklaren. Er gibt persönliche Daten auf **unbestimmte Zeit** Preis und stellt keine Verbindung zu vermehrten Spam-Mails und passgenauer Werbung her (Lorenz, 2012, Frage 3). Warum also sollte der Nutzer auf den Facebook-Nutzen verzichten, entstehen ihm doch offensichtlich keine größeren Nachteile?

Bewusstwerdung – Ausübung von Druck auf Betreiber

Eine wichtige Aufgabe der Nutzer Sozialer Netzwerke wird es sein, ihre **Autonomie über eigene Daten von den Betreibern sozialer Netzwerke zurück zu fordern**. Die Datenschützerin Rena Tangens befürchtet nach dem Börsengang Facebooks eine noch stärkere Ausbeutung der Nutzer-Daten. Tangens schlägt vor Datenportabilität gesetzlich durchzusetzen: *„[...] Um Wettbewerb zu ermöglichen, muss Datenportabilität durchgesetzt werden. Damit wäre es Nutzer/innen möglich, über die Grenzen einer Plattform hinaus mit anderen in Kontakt zu treten. [...] Sobald diese plattformunabhängige Vernetzung durchgesetzt ist, können die Nutzer/innen sich endlich frei für eine Plattform entscheiden, etwa auch eine, die Datenschutz, Privatsphäre und europäische Gesetze achtet.* (Tangens, 2012, Frage 12).

Insbesondere Facebook setzt darauf, der führende Rundum-Serviceanbieter im Bereich sozialer Netzwerke zu werden. In einer derartigen Monopol-Position ist es den Nutzern kaum möglich einen anderen Anbieter zu wählen, da Freunde und veröffentlichte Inhalte nicht zu einer anderen Plattform mitgenommen werden können.

Der zweite kritische Punkt bei einer Vormachtstellung eines einzigen Sozialen Netzwerk-Betreibers wie z.B. Facebook ist eine **Einschränkung der Nutzer bei der Nutzung der Privacy-by-Default Einstellungen**. Aufgrund **mangelnder Vergleichsmöglichkeiten und einer Regulationsintransparenz** seitens des einzigen Anbieters, sind die Wahlmöglichkeiten sehr begrenzt. Peter Schaar äußert seine Bedenken darüber, wie eine Übersichtlichkeit für den Endnutzer hergestellt werden kann: *„Da gibt es verschiedene Ansätze. Das eine ist die Möglichkeit diese sehr komplexen Strukturen öffentlich zu machen, das führt aber zu dem Problem, dass der Rezipient dieser Information sehr hohen Aufwand betreiben muss, um diese Information überhaupt zu verstehen und zu bewerten. Ob er das überhaupt kann ist fraglich, weil die Komplexität riesig ist.“* (Schaar, 2012, Frage 6).

Aus diesem Grund wünscht Schaar sich eine Art Basis-Schutz für alle Nutzer und stellt sich den privacy-by-default-Ansatz wie folgt vor. *„Er (der privacy-by-default-Ansatz) setzt voraus, dass der nicht sensible Nutzer eine Art Grundschutz genießt. Das heißt ich werde Kunde bei einem Dienst und kann mir sicher sein, dass in der Umgebung in der ich mich bewege, meine Daten angemessen gesichert sind.“* (Schaar, 2012, Frage 15).

Die Metapher der Kunden, die Schaar in seiner Antwort wählt, lässt sich weiter entwickeln. Wäre der Nutzer wirklich bereit einen geringen Betrag für die Rückhol-Möglichkeit seiner eigenen Daten zu entrichten? Vermutlich würden sich Nutzer in diesem Fall unfair behandelt fühlen und das Netzwerk durch Nicht-Nutzung sanktionieren. **Aus diesem Grund ist es eine wesentliche Aufgabe der Nutzer den Betreibern Sozialer Netzwerke faire Strukturen abzuverlangen und klarere Bedingungen einzufordern.**

Nutzer haben daher die Verantwortung:

1.) Sich selber über die Relevanz von Datenschutz bewusster zu werden und sich bei der Publikation von Inhalten verantwortungsbewusst zu verhalten.

2.) Sicherere und klarer definierte Dienstleistungen bei den Betreibern Sozialer Netzwerke einzufordern und nachzufragen.

3.) Abstimmungen einzufordern und sich daran stärker zu beteiligen.

4.) Druck auf Betreiber Sozialer Netzwerke und IT-Dienstleister auszuüben, indem man sich gemeinschaftlich gegen personalisierte Werbung ausspricht oder die Netzwerk-Nutzung einschränkt.

7 Fazit & Ausblick

Gibt es sie tatsächlich, die unsichtbare Hand des Datenmarktes? Ja und nein, denn durch das Wirken Sozialer Netzwerke wird **die Komplexität des Datenmarktes lediglich verlagert, aber nicht gelöst**. Nutzer die versuchen eine Reduktion von Komplexität zu erlangen (z.B. durch verbesserte Arbeitsorganisation), erhalten eine neue Form von Komplexität.

7.1 Die außergewöhnlich hohe Nutzer-Akzeptanz gegenüber den Angeboten Sozialer Netzwerke

Abbildung 6 „Neuer Facebook-Button“ Quelle: Facebook [14]

Nutzer verhalten sich in Sozialen Netzwerken außergewöhnlich. Nutzer geben etwas von sich Preis, ohne zunächst eine direkte Gegenleistung erwarten zu können. Während sie der Zufallsbegegnung auf der Straße, im Supermarkt oder in der U-Bahn nicht sofort ihr Innerstes offenbaren würden (von Ausnahme-Situationen einmal abgesehen), ist die Akzeptanz und der Grad der Selbstoffenbarung in der virtuellen Welt viel ausgeprägter. Die Annahme, dass die generelle Hemmschwelle zur Selbstoffenbarung heutzutage gesunken ist, ist jedoch falsch (Jentzsch, 2012).

Vielmehr muss davon ausgegangen werden, dass das Nutzer-Bewusstsein darüber fehlt, dass eine persönliche Äußerung in Sozialen Netzwerken eine ebensolche Wertigkeit hat, wie die reale, physische Kommunikation. Die virtuelle Publikation ist

[14] Eine seit 2012 bei Facebook kursierende Grafik mit unbekanntem Urheber.

im Gegenteil sogar **langlebiger als das gesprochene Wort**, weil diese Information dezentral gesichert wird und über Jahre hinweg abgerufen werden kann. Dennoch vertrauen die Nutzer dem Angebot Sozialer Netzwerke, **ohne dieses Vertrauen zu reflektieren**. **Der Nutzer bewegt sich im Internet in einem naiven Modus der Entdeckung**, von dem er sich vor allem deswegen distanzieren kann weil es keine **physische Teilnahme** an der Entdeckungsreise gibt (Fischer, 2012).

Zudem bringt der Nutzer die ihm gezeigte Werbung und den Spam nicht mit seinem eigenen Verhalten im Internet in Verbindung. **Der Nutzer verzeiht bereitwillig die Patzer Sozialer Netzwerke**, wie z.B. das verschwinden von Adressbüchern oder die Weitergabe von E-Mail-Kontakten an Dritte. Auch die Tatsache, dass der Account nicht einfach zu löschen ist oder die Einstellungen, die man zur eigenen Sicherheit gerne vornehmen möchte, intransparent bis nicht vorhanden sind, wird mit Nachsicht behandelt. Man kann **ein irrationales Herden-Verhalten[15] der Nutzer beobachten**: Andere vertrauen dem Netzwerk, also vertraue ich ebenfalls darauf.

Darüber, dass das Kerngeschäft Sozialer Netzwerke der Datenhandel oder die Profilbildung für gezielte Werbung ist, reflektiert der Nutzer selten und wenig intensiv, was auch die Untersuchungen der Filter Bubble Forschung, ebenso wie die Beobachtungen von X-Pire!-Entwickler Stefan Lorenz, belegen.

Die Nutzer sind sich gar nicht im Klaren darüber, dass sie datenschutzrechtlich benachteiligt werden und nehmen somit auch ihre Abstimmungsinteressen nicht wahr, was u.a. das Scheitern der jüngsten Nutzungsbedingungs-Abstimmungen bei Facebook dokumentiert.

Das mangelnde Bewusstsein der Nutzer darüber, dass sie einmal preisgegebene Daten im Internet nicht wieder zurück holen können, führt dazu, dass die Nutzer nicht den Versuch unternehmen Ihre datenschutzrechtlichen Ansprüche gegenüber den Betreibern geltend zu machen.

---

[15] Herdentrieb nach dem Begriffsverständnis von Alexander Weyland, siehe Text „Kapitalistische Spekulation im globalen Finanzsystem. Versuch zur Semantik der modernen Finanzspekulation“ im Anhang.

Da sich die Nutzer weder in einem hohen Maße verunsichert fühlen, noch sich über die zu Grunde liegenden Geschäftsmodelle Soziale Netzwerke im Klaren sind, geben sie die **Autonomie über die eigenen Daten bereitwillig ab und sind sich nicht über die Konsequenzen bewusst** (Lorenz, 2012, Frage 1). Außergewöhnlich daran ist, dass Soziale Netzwerke einen Vertrauensvorschuss der Nutzer genießen, den andere Unternehmen sich erst langwierig erarbeiten müssen.

7.2 Die langfristige Entwicklung des strukturellen Ungleichgewichts im Datenmarkt

Der Datenmarkt ist ein besonderer Markt. Das **strukturelle Ungleichgewicht** des Marktes ist unverkennbar, denn die Urheber der Daten haben kaum Rechte an ihnen. Ist ein Foto, eine Nachricht oder ein Video erst einmal veröffentlicht, verliert der Urheber die Kontrolle wo und wie oft diese Daten auf fremden Rechnern gespeichert und kopiert werden. Die privaten Daten unterliegen einer **dezentralen Streuung, die eine vollständige Löschung nahezu unmöglich macht**. Ob der verspürte Nutzen Sozialer Netzwerke dieses Ungleichgewicht auf Dauer aufwiegt ist fraglich. Solange nur einige wenige Nutzer ihre Datenpreisgabe hinterfragen und die Konsequenzen aus ihrem Handeln ziehen, wird es schwierig werden die Betreiber Sozialer Netzwerke ebenfalls zu einem nutzerfreundlichen Umdenken zu bewegen. **Ein langwieriger Prozess der Bewusstwerdung ist daher notwendig**.

Als langfristige Entwicklung werden Soziale Netzwerke wie Facebook und Co. Sicherlich der **Kontingenz** unterworfen sein, dass es dieses Netzwerk sein könnte oder auch ein anderes. Zumindest sobald Nutzer beginnen misstrauisch zu werden und sich nicht länger fair behandelt fühlen.

Die **Schieflage des Datenmarktes** wird den Nutzern, die sich mit mehr und mehr personalisierter Werbung konfrontiert sehen, mit der Zeit deutlich bewusster werden. Eine bereits aktuell vermehrte Presseberichterstattung über das unternehmerische Verhalten Sozialer Netzwerke wird dazu beitragen, das Kostenlos-Angebot skeptischer zu Betrachten. Ist Facebook wirklich der gute Duz-Kumpel, der den Alltag erleichtert? Laut Gunnar Bender gibt sich Facebook nun Mühe genau dieser faire Ansprechpartner zu sein: *„Facebooks größtes Anliegen ist nach wie vor die Zufriedenheit der Nutzer. Natürlich geht es Facebook auch um den*

unternehmerischen Erfolg, aber Facebook bemüht sich um mehr Transparenz, was das Agieren am Datenmarkt angeht. Meine Rolle ist es u.a. auch die Lücke zwischen Amerikanischem Handeln und Deutschem Handeln zu füllen. In Deutschland herrschen eben ganz andere Vorgaben als in den USA. Ich denke, dass Facebook zeigt, in dem es Leute wie mich einstellt, dass es die Schieflage verstanden hat.“ (Bender, 2012). Datenschützer Thilo Weichert ist jedoch der Meinung, dass diese Bemühungen noch nicht ausreichen, wie er in einem Gespräch am 24. Juli 2012 mit Gunnar Bender äußerte (Sawall, 2012 &).

Der Hebel, der zu dieser Bewusstwerdung und zu mehr Datenschutz führt, liegt weder bei den Betreibern noch bei der Politik allein. Wie auch bei anderen Unternehmen, haben die Kunden (im Falle sozialer Netzwerke die Nutzer), die größte Macht.

Die relativ träge Politik kann zwar Spielregel festlegen und Gesetze, wie auch Sanktionierungsmaßnahmen, erlassen. Jedoch täte die Politik besser daran, statt Sanktionierungen Anreize und Angebote zu schaffen. Solange die Betreiber Sozialer Netzwerke aber die einzigen Anbieter für effizientes „Identity-Design“ bleiben, bleibt der Markt konkurrenzlos und Datenschutz wird wenig nachgefragt.

7.3 Eine Zusammenfassung der Lösungsmöglichkeiten

1. Der Markt reguliert sich selbst, so die ursprüngliche Hypothese. Nutzer und Betreiber finden ein Optimum der Datentransparenz ohne Einmischung des Staates: Problematisch ist, dass dieses Optimum nicht wie erwartet eintritt, sondern bei zu wenig Datenschutz aufgrund hoher Nutzerakzeptanz liegt.

2. Die Internet-Gesetzgebung ist zu langsam. Diese Trägheit wird durch die Notwendigkeit eines europäischen und nicht allein nationalen Ansatzes noch verstärkt.

3. Betreiber werden sich ihr Kerngeschäft, den Datenhandel, durch Gesetze nach Möglichkeit nicht zerstören lassen. Die Gerichtsstandorte der größten Sozialen Netzwerk- Betreiber sind zudem EU-extern.

4. Vor allem die Nutzer können den größten und raschesten Druck auf die Betreiber ausüben, diese haben aber ein extrem mangelhaftes Bewusstsein über die Konsequenzen ihrer Datenpreisgabe – das Bewusstsein muss prozessual wachsen.

5. Letztlich liegt es doch an Staat und Medien eine Aufklärung diesbezüglich zu betreiben, das Bewusstsein zu stärken und Nutzer-Anreize zu schaffen, die eine Datenschutz-Bereitschaft der Bevölkerung erhöht.

6. Die Betreiber Sozialer Netzwerke haben zudem die Möglichkeit auf ihren Websites nutzerfreundliche Löschformulare für die Löschung persönlicher Daten anzulegen. Über dieses Verfahren haben Betreiber die Chancen das Vertrauensempfinden der Nutzer durch das Aussenden von Signalen zu steuern.

Eine Einigung der Nutzer und Betreiber Sozialer Netzwerke über ein Idealmaß an Datenpreisgabe kann nur dann erreicht werden, wenn auf beiden Seiten die Anreize stimmen. Es wird zudem kein Pareto-optimaler Grad der Nutzerdatentransparenz erreicht werden können. Langfristig sind die Geschäftsmodelle von Sozialen Netzwerken neu zu definieren, ab einem bestimmten Punkt wird der Datenhandel durch den Druck der Nutzer abgestraft werden. Im schlimmsten Falle verlagern die Nutzer ihre Aktivitäten in andere als fair empfundene Netzwerke.

Was die Einschränkung des Datenmarktes anbelangt, können nicht wie üblich rechtliche Besitztums-Aussagen getroffen werden, da bisherige Rechte wie z.B. das Urheberrecht den digitalen Datenmarkt nur am Rande erfassen.

Es gilt, jeder der etwas lesen oder sehen kann, kann es kopieren. Die Nutzer-Gruppe lässt sich technisch einschränken, z.B. durch begrenzten Zugriff auf eine Datei durch Passwort-Schutz oder Verschlüsselung. Bestimmte Personen können also von der Nutzung ausgeschlossen werden. Will ich Missbrauch unter den Personen, die einen Zugriff haben vermeiden, kann ich diese Personen eine Geheimhaltungsvereinbarung unterzeichnen lassen. Damit mache ich dann mein Besitztum rechtlich geltend und kann Zuwiderhandlungen nachverfolgen. Dies funktioniert jedoch nur in geschlossenen zentral gesteuerten Strukturen; Immer dann wenn ich in einer derart

dezentralen Struktur wie dem Internet Daten preisgebe gehen jegliche Kontrollmöglichkeiten verloren.

Um die rechtliche Eingrenzung zu vermeiden gibt es in Sozialen Netzwerken auch die Möglichkeit über Anreiz-Modelle das Nutzerbewusstsein zu erhöhen. Wie genau diese Anreizmöglichkeiten gestaltet werden müssen, muss offen und situationsabhängig bleiben. Denkbar wäre z.B. eine staatliche Intervention, wie Lorenz sie vorschlägt. Wenn Betreiber nicht von sich aus für die Löschung von Nutzerdaten sorgen, könnte der Staat Schlüsselserver einsetzen, um Nutzern eine automatisierte Löschung der Daten zu ermöglichen.

Eine weitere Möglichkeit ist die Nutzer-Anreize zu steigern, indem ein neuer Mehrwert zu mehr Datenschutz verleitet. Betreiber Sozialer Netzwerke oder auch der Staat könnten beispielsweise Musik- und Filmrechte erwerben. Nutzer erhalten in diesem Fall eine Belohnung für die Beteiligung am Datenschutz in Form von kostenloser Musik oder eines Films. Auch der Markt der Musik- und Filmindustrie, der durch die Kostenlos-Kultur starke Einbußen hatte, könnte auf diesem Weg eine Kompensation erfahren.

Ein generell Anreiz-orientiertes Vorgehen kann das strukturelle Ungleichgewicht des Datenmarktes im wohlfahrtsökonomischen Sinne lösen. Der wichtigste Schritt hierzu ist jedoch eine prozessuale Bewusstwerdung über das Vorhandensein des Ungleichgewichts in einem Markt, der oftmals gar nicht als Markt wahrgenommen wird.

Quellenverzeichnis

7.4 Literaturangaben

Adamek, S. (2011). *Die Facebook-Falle – Wie das soziale Netzwerk unser Leben verkauft.*

München: Wilhelm Heyne Verlag.

Akerlof, G. A. (1970). *The Market for "Lemons": Quality Uncertainty and the Market Mechanism.* Boston: The Quarterly Journal of Economics, Vol. 84, No. 3. (Aug., 1970), S. 488-500.

http://www.iei.liu.se/nek/730g83/artiklar/1.328833/AkerlofMarketforLemons.pdf

Akerlof, G. A. / Shiller R. J. (2009). *Animal Spirits – Wie Wirtschaft wirklich funktioniert.* New York/Frankfurt: Campus Verlag.

Baloun, K. M. (2007). *Inside Facebook – Life, Work and Visions of Greatness.*

Canada: Trafford Publishing.

Bateson, G. (1985). *Ökologie des Geistes.* Berlin: Suhrkamp Verlag

Benz, M. (2004). *Die Einheit der Gesellschaftswissenschaften.*

Tübingen: Mohr Siebeck Verlag

Beiersmann, S. (2012). *Sergey Brin: Facebook und Apple gefährden das freie Internet.*

In zdnet.de:

http://www.zdnet.de/news/41561619/sergey-brin-facebook-und-apple-gefaehrden-das-freie-internet.htm

Bender, G. (2012).) *Persönliches Interview 11.07.2012.* Berlin

BFDI (2006). *Vorratsspeicherung von Telekommunikationsdaten: Wirtschaft nicht in die Rolle des „Hilfssheriffs" drängen.* In:

http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Pressemitteilungen/2006/PM-05-06VorratsspeicherungVonTelekommunikationsdaten.html?nn=409394

BigBrotherAwards (2002). http://www.bigbrotherawards.de/

Beiersmann, S. (2012). *Facebook will sich für Kinder öffnen.*

http://www.silicon.de/41567640/facebook-will-sich-fur-kinder-offnen/

Biermann, K. (2012). *Facebook entdeckt den Mobilen Markt.*

In Zeit-Online: http://www.zeit.de/digital/internet/2012-04/facebook-mobil-nutzer/seite-1

Blogfraktion. (2012). *Wir brauchen einen Ausschuss für „Internet und digitale Gesellschaft“ im*

Deutschen Bundestag

http://blogfraktion.de/2012/02/08/wir-brauchen-einen-ausschuss-fur-internet-und-digitale-gesellschaft-im-deutschen-bundestag/

Bolz, N. (1999). *Die Wirtschaft des Unsichtbaren.* München: Econ Verlag.

Brandeis L. D. / Warren S. (1890). *The right to privacy.*

Boston: Harvard Law Review. Vol. IV.

Brill A. / de Vries M. (1998). *Virtuelle Wirtschaft, Virtuelle Unternehmen, Virtuelle Produkte, Virtuelles Geld und Virtuelle Kommunikation*. Opladen/Wiesbaden: Westdeutscher Verlag.

B.Z. News aus Berlin (2011). *Facebook-Milliardär plant Anarchie-Staat.*
In: B.Z. online: http://www.bz-berlin.de/aktuell/welt/facebook-milliardaer-plant-anarchie-staat-article1250459.html

Coase, R. H. (1937). *The nature of the Firm*. London: London School of Economics.

Economica, New Series, Vol. 4, No. 16. (Nov., 1937), pp. 386-405.

http://www.sonoma.edu/users/e/eyler/426/coase1.pdf

Collins N. L. / Miller L.C. (1994). *Self-disclosure and liking: A meta-analytic review.*

Psychological Bullettin Journal No. 116. S. 457-475.

Corchado E. et al. (2011). *Soft Computing Models in Industrial and Environmental Applications-*

6th International Conference SOCO 2011. Berlin-Heidelberg: Springer-Verlag.

Delaware General Corporation Law. (2011).

http://www.corp.delaware.gov/DElaw.shtml

De Waal, Frans. (2005). *Der Affe und der Sushimeister*. München: DTV Verlag.

dpa, Deutsche Presse Agentur (2012). *Facebook-Einträge ähnlich befriedigend wie Sex.*
In Welt-Online:
http://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article106270120/Facebook-Eintraege-aehnlich-befriedigend-wie-Sex.html

dpa, Deutsche Presse Agentur (2012 B). *Mecklenburg-Vorpommern: Datenschutz soll in den Lehrplan.* In: news4teachers.de:
http://www.news4teachers.de/2012/05/datenschutz-im-internet-soll-in-die-lehrplane-in-mecklenburg-vorpommern/

European Commission (2012 A).

http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf

European Commission (2012 B).

http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

Europe versus Facebook (2012).

http://europe-v-facebook.org/DE/de.html

FAZ (2012). *Facebooks Datenschutz- Die Mitbestimmung ist rein virtuell.* http://www.faz.net/aktuell/feuilleton/medien/facebooks-datenschutz-die-mitbestimmung-ist-rein-virtuell-11775246.html

Facebook Site Governance. (2012 A). *Aktualisierung der Erklärung der Rechte und Pflichten.*

Facebook: https://www.facebook.com/note.php?note_id=10151547216160301

Und die neue Version vom 08. Juni 2012 : http://www.facebook.com/legal/terms

Facebook (2012 B). *Umgehende Personalisierung.* http://www.facebook.com/instantpersonalization/

Facebook Privacy. (2012 C). *Cookies, Pixel und andere Systemtechniken.*

http://www.facebook.com/about/privacy/cookies

Facebook Privacy. (2012 D). *Datenverwendungsrichtlinien.*

http://www.facebook.com/about/privacy/

Facebook (2012 E). *Für Nutzer mit Wohnsitz in Deutschland.*

http://www.facebook.com/terms/provisions/german/index.php

Fechte T. /Görtz B. (2012). *Von einem stumpfen Schwert zu einer scharfen Rasierklinge* http://www.pwc.de/de/corporate-governance/von-einem-stumpfen-schwert-zu-einer-scharfen-rasierklinge.jhtml

Fehr E. / Gächter S. (2000). *Cooperation and Punishment in Public Goods Experiments.* In: The American Economic Review, 90 (4) September, S. 980-994.

Finanznachrichten. de (2012). http://www.finanznachrichten.de/nachrichten-2012-05/23454044-datenschutz-im-fokus-jedes-vierte-unternehmen-stellt-verstoesse-fest-007.htm

Fischer, A. (2012 A). *Persönliches Interview vom 25.04.2012.* Berlin

Fischer, A. (2012 B). *Vermummungsverbot im Internet - Pflicht zur Klarnamen-Nennung im Internet - Radiergummi entwickeln.* Facebook, 15. November 2010: http://www.facebook.com/notes/axel-fischer/vermummungsverbot-im-internet-pflicht-zur-klarnamen-nennung-im-internet-radiergu/456370668358

Focus Online/DPA (2012). *AOL, Facebook, Microsoft, YahooInternetgiganten pokern um Patente – Facebook kauft AOL-Ideen.* In Focus Online: http://www.focus.de/digital/computer/aol-facebook-microsoft-yahoo-internetgiganten-pokern-um-patente-facebook-kauft-aol-ideen_aid_741942.html

Focus Online (2012 B).
Neue Daten-Richtlinien: Facebook will Daten länger speichern. FOCUS Online: http://www.focus.de/digital/internet/facebook/neue-daten-richtlinien-facebook-will-daten-laenger-speichern_aid_751663.html

Focus Online (2012 C). *Neue Daten-Richtlinien: Facebook will Daten länger speichern*. FOCUS Online: http://www.focus.de/digital/internet/facebook/neue-daten-richtlinien-facebook-will-daten-laenger-speichern_aid_751663.html

FoeBuD e.V. (2012). http://www.foebud.org/

Forkefeld, N. (2009). *Bachelor-Thesis: Yes we can! – Wie generiert sich das Phänomen der*

Zwichenmenschlichkeit? Witten: Universität Witten/Herdecke.

Frese, E. (1980). *Grundlagen der Organisation – Die Organisationsstruktur der Unternehmung.*

Wiesbaden: Gabler Verlag.

Frickel, C. (2012). *Datenschutz und Pseudo-Freunde: Die zehn größten Facebook-Aufreger* . In: FOCUS Online.
http://www.focus.de/digital/internet/facebook/tid-26230/datenschutz-privatsphaere-mitglieder-die-zehn-groessten-facebook-aufreger_aid_770108.html

Friedman, M. (1975). *There's no such thing as free lunch*. Chicago: Open Court Publishing.

Fröhlich, C. (2011). *Warum Google+ nicht scheitern darf.* In stern.de:

http://www.stern.de/digital/online/facebook-vs-google-warum-google-nicht-scheitern-darf-1703667.html

FTD Online (2012). *Facebook verliert großen Werbekunden.*

In ftd.de:

http://www.ftd.de/it-medien/medien-internet/:rueckzug-von-gm-facebook-verliert-grossen-werbekunden/70037679.html

Goldgraber A. / Henselmans B. (2012). *Europe versus Facebook.* In. WDR-Bericht aus Brüssel:

http://www.youtube.com/watch?v=buzW8eMCjHw&t=8s

Härting, N. (2012), *Kommunikationsfreiheit im Netz „Internet Freedom" im Lichte des Art. 5 GG.* In: K+R Magazin für Kommunikation + Recht. Frankfurt am Main. Deutscher Fachverlag GmbH. S. 265 ff.

Hardin, G. (1968). The Tragedy of the Commons, in: Science, Vol. 162, No. 3859, S. 1243-1248.

http://www.sciencemag.org/cgi/content/full/162/3859/1243 (Stand: Dezember 2011)

Hardin, G. (2003): *The Free Rider Problem*. Standford Encyclopedia of Philosophy

http://plato.stanford.edu/entries/free-rider/ (Stand: Dezember 2011)

Harvard Online Factbook (Fall 2004-2005):

http://www.provost.harvard.edu/institutional_research/archive/2005OnlineFactBook.pdf

Hess C. und Ostrom E. (2003). Ideas, Artifacts, and Facilities: Information as a Common-Pool Resource in: Law & Contemporary Problems 66. S. 111-147. http://www.law.duke.edu/shell/cite.pl?66+Law+&+Contemp.+Probs.+111+(WinterSpring+20%2003)

Hedemann, F. (2010). *Datenschutz: Facebooks Instant Personalization mit erster Sicherheitslücke.*

In t3n.de: http://t3n.de/news/datenschutz-facebooks-instant-personalization-erster-272366/

Heise Online (2011). *Like-Button: Facebook erklärt Details zur Speicherpraxis.*

http://www.heise.de/newsticker/meldung/Like-Button-Facebook-erklaert-Details-zur-Speicherpraxis-1339079.html

Heise Online (2011 A). *"Digitaler Radiergummi" ist gestartet.*

http://www.heise.de/newsticker/meldung/Digitaler-Radiergummi-ist-gestartet-1175979.html

Höver, P. (2011). *Weichert fordert mehr Schutz im Netz durch Politik.*

In: Schleswig-Holsteiner Zeitungsverlag: Flensburg.

http://www.shz.de/artikel/article//weichert-fordert-von-politik-mehr-verantwortung-im-netz.html

Horchert J. / Reißmann O. / Stöcker C. (2012). *Schnüffel-Plan der Schufa: Was Facebook über*

sie verrät. In Spiegel Online:

http://www.spiegel.de/netzwelt/netzpolitik/facebook-was-ein-profil-der-schufa-verraten-kann-a-837531.html

InsideFacebook (2012). http://www.insidefacebook.com/

Jentzsch, N. (2012). *Privatsphäre: Verhaltensexperimente zur persönlichen Privatsphäre erfordern neue Standards.* Deutsches Institut für Wirtschaftsförderung: Berlin:
http://www.diw.de/documents/publikationen/73/diw_01.c.393931.de/12-9-3.pdf

Katz, I. (2012). *Web freedom faces greatest threat ever, warns Google's Sergey Brin.* In guardian.co.uk:

http://www.guardian.co.uk/technology/2012/apr/15/web-freedom-threat-google-brin

Kallus, M. (2012). *PwC-Studie zum Datenschutz: Facebook Like Button behindert Social Media.* In: www.cio.de.
http://www.cio.de/facebook/2880379/

Katz, E. / Foulkes D. (1962). *On the Use of Mass Media as „Escape“: Clarification of a Concept.* In: Public Opinion Quarterly. Nr. 26, S. 377ff.

Kempf, D. (2012). *Persönliche Daten im Internet – Nutzerverhalten und Schutz.* Hannover: Pressekonferenz zum „Safer Internet Day“ 7. Februar 2012.

http://www.bitkom.org/files/documents/bitkom_praesentation_datenschutz_prof_ke

mpf_07_02_2012(1).pdf

Küchemann, F. (2012). *Werbung im Internet - Wollten Sie nicht diesen Flug buchen?* In: Frankfurter Allgemeine Online. http://www.faz.net/aktuell/feuilleton/medien/werbung-im-internet-wollten-sie-nicht-diesen-flug-buchen-11785826.html

Kurz, C. / Rieger, F. (2011). *Die Datenfresser. Wie Internetfirmen sich unsere per sönlichen Daten einverleiben und wie wir die Kontrolle darüber zurück erlangen.* Frankfurt am Main: Verlag S. Fischer.

Landesdatenschutzgesetz Nordrhein-Westfalen (2003):

https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=2&gld_nr=2&ugl_nr=20061&bes_id=4908&aufgehoben=N&menu=1&sg=#det251223

Le Menestrel, M. (2001). *A process approach to the utility for gambling.* Barcelona: Universitat Pompeu Fabra Publicaciónes. http://www.econ.upf.edu/~lemenestrel/IMG/pdf/a_process_approach_to_the_utility_for_gambling.pdf

LfM Nordrhein-Westfalen (2009). *Heranwachsen mit dem Social Web -*

Zur Rolle von Web 2.0 -Angeboten im Alltag von Jugendlichen und jungen Erwachsenen.

http://www.lfm-nrw.de/fileadmin/lfm-nrw/Pressemeldungen/zusammenfassung_socialweb.pdf

Lorenz, S. (2012) *Persönliches Interview 05.07.2012.* Witten.

Lüdicke, M. K. (2006). *A Theory of Marketing.* Wiesbaden: DUV, Gabler Edition Wissenschaft.

Lüpken-Räder, G. (2012). *Datenschutz von A-Z.* Freiburg: Haufe-Lexware GmbH & Co. KG.

Luhmann, N. (2011). *Organisation und Entscheidung*. Wiesbaden. VS Verlag für Sozialwissenschaften. 3. Auflage.

Milgrom P. / Roberts J. (1992). *Economics, Organization and Management.* New Jersey: Prentice-Hall Inc.

Moore T. et al. (2010) *Economics of Information Security and Privacy*. New York – Dordrecht –Heidelberg-London: Springer Verlag.

Müller G. / Reichenbach M. (2001). *Sicherheitskonzepte für das Internet.* Berlin-Heidelberg: Springer Verlag.

n-tv.de/jga/dpa/rts/DJ (2012). *Ende des Turbo-Wachstums? Facebook boomt langsamer.*
In n-tv.de: http://www.n-tv.de/wirtschaft/Facebook-boomt-langsamer-article6096196.html

Nash, J. F. (1996) *Essays on Game Theory*. Massachusetts: Edward Elgar Publishing Inc.

Netzwertig, 2010
http://netzwertig.com/2010/04/08/wikipedia-und-wikileaks-auch-nonprofit-braucht-geld/

Olson, M. (1965) *The Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge- Massachusetts: Harvard University Press.

Ostrom, E. (1990 A). *Governing the commons: the evolution of institutions for collective action*. New York: Cambridge University Press.

Ostrom, E. (1990 B). *The Evolution of Institutions for Collective Action.* New York: Cambridge University Press.

Ostrom, E. (1999). *Die Verfassung der Allmende. Jenseits von Markt und Staat.* Tübingen: Mohr Siebeck.

Ostrom, E. (2005). *Understanding Institutional Diversity*. New Jersey: Princeton University Press.

Ostrom, E. (2011). *Was mehr wird wenn wir teilen*. München: Oekom Verlag.

Palfrey J. / Gasser U. (2008). *Born Digital: Understanding the First Generation of Digital Natives.* New York: Basic Books.

Pascal, B. (1670), *Pensées.* Paris: Port-Royal.

Pareto, V. (1906). *Manuale di economia politica.* Mailand: Carocci Editore.

Pariser, E. (2011). *The Filter Bubble – What The Internet Is Hiding From You"*.

New York. The Viking Press.

Pariser, E. (2012). *Filter bubbles, meet Upworthy.*
Im Blog: Thefilterbubble.com. http://www.thefilterbubble.com/

Pariser, E. / Kamin, J. (2012). *Yahoo's man+machine algorithm: the numbers are in.* Im Blog: Thefilterbubble.com. http://www.thefilterbubble.com/

Plessner, H. (2000). *Mit anderen Augen – Aspekte einer philosophischen Anthropologie.*
Stuttgart: Reclam Verlag.

Pluta, W. (2012). *Datenschutz: Neue EU-Regeln zu Cookies treten in Kraft.*
In Golem-News:
http://www.golem.de/news/datenschutz-neue-eu-regeln-zu-cookies-treten-in-kraft-1205-92094.html

Priddat B. P. (2008). *moral hybrids - Skizze zu einer Theorie moralischen Konsums.* Zeitschrift für Wirtschaft und Unternehmensethik. Kassel.
http://www.zfwu.de/fileadmin/pdf/2_2000/Birger_Priddat.pdf

Prummer J. (2012). *Datenschutz-Aktivist Schrems - Der Mann, der Facebook nervt.*
In: Süddeutsche Online: http://www.sueddeutsche.de/digital/datenschutz-aktivist-schrems-der-mann-der-facebook-nervt-1.1337259

Rorty, Richard. (1991). *Kontingenz, Ironie, Solidarität.* Frankfurt am Main: Suhrkamp Verlag.

Reißmann O. (2012). *Änderung der Richtlinien: Facebook-Nutzer haben keine Wahl.* Spiegel Online: http://www.spiegel.de/netzwelt/netzpolitik/neue-regeln-facebook-laesst-seinen-nutzern-keine-wahl-a-837015.html

Sawall, A. (2012). *Facebook vs. Thilo Weichert. Neues Fenster für die Zukunft auf Gestoßen.* In: Golem.de.

http://www.golem.de/news/facebook-vs-thilo-weichert-neues-fenster-fuer-die-zukunft-aufgestossen-1207-93410.html

Say, J.-P. (1803). *Traité d'economie politique.* Paris. Imprimerie de Casimer.

Schaar, P. (2007). *Das Ende der Privatsphäre – der Weg in die Überwachungsgesellschaft.* München: Wilhelm Goldmann Verlag.

Schaar, P. (2012 A). *Mein Pseudonym und ich.* Datenschutz-Forum:

https://www.bfdi.bund.de/bfdi_forum/showthread.php?3231-Mein-Pseudonym-und-ich

Schaar, P. (2012 B) *Persönliches Interview 27.04.2012.* Berlin

Schmitt, S. (2011). *ALGORITHMEN - Automatisch vorsortiert.* In: DIE ZEIT. http://www.zeit.de/2011/26/Internet-Surfverhalten-Filter

Schneider, K. (2007) *StudiVZ, Xing & Co.: Die freiwillige Entblößung.* In: Neue Gegenwart – Magazin für Medienjournalimus. Ausgabe 53 vom 07. Oktober 2007.

http://www.neuegegenwart.de/ausgabe53/entbloessung.htm

Schröder, O. (2012). *EU-Datenschutzreform.* Rede vor dem Deutschen Bundestag. http://www.bmi.bund.de/SharedDocs/Reden/DE/2012/03/psts_bt.html

Smith, A. (1976). *An Inquiry into the Nature and Causes of the Wealth of Nations. Vol. I/ Vol. II.* München: IDION-Verlag (als Vorlage diente eine sich in der Universitätsbibliothek Heidelberg befindende Originalausgabe).

Sobiraj L. (2012). *Thilo Weichert: "Facebook nervt".* In:

http://www.gulli.com/news/18823-thilo-weichert-facebook-nervt-2012-05-16

Sorge, P. (2012). *Wahl zwischen Pest und Cholera – Interview mit Thilo Weichert.* In Cicero: http://www.cicero.de/kapital/datenschutz-thilo-weichert-facebook-google-wahl-zwischen-pest-cholera/48881?seite=1

Spence M. (1973). *Job Market Signalling*. Massachusetts: The Quarterly Journal of Economics, Vol. 87, No. 3. (Aug., 1973), pp. 355-374

Spiegel (2012 A). *Geballte Ladung –Bundestagspräsident Norbert Lammert kritisiert die anonymen Beleidigungen im Netz.* S. 23. Hamburg: Der Spiegel 13/2012 vom 26. März 2012.

Spiegel Online. (2012)**.** *Bürger verlangen immer häufiger Informationen von Behörden.* http://www.spiegel.de/politik/deutschland/der-bundesdatenschutzbeauftragte-peter-schaar-stellt-jahresbericht-vor-a-829487.html

Stern. (2012). Eigenes Facebook-Benutzerkonto löschen.

http://www.stern.de/digital/eigenes-facebook-benutzerkonto-loeschen-1843266.html

Steiner, P. (2006). *Effektiv arbeiten mit dem Internet.*

Darmstadt: Wissenschaftliche Buchgesellschaft

Stiftung Warentest (2010). *Ungeschützt.* In: test 4/2010.

Sueddeutsche (2012 A). *Ariane Friedrich schließt ihre Facebook-Seite.*

In sueddeutsche.de:

http://www.sueddeutsche.de/digital/nach-stalking-kontroverse-ariane-friedrich-schliesst-ihre-facebook-seite-1.1344111

Sueddeutsche (2012 B). *General Motors zweifelt an Facebook-Anzeigen.*

In sueddeutsche.de:

http://www.sueddeutsche.de/wirtschaft/2.220/schlechte-nachrichten-vor-dem-boersengang-facebook-verliert-anzeigenkunden-general-motors-1.1358760

Sueddeutsche (2012 C). *Facebook kündigt neue Funktion an - Ändern statt löschen.*
In sueddeutsche.de:

http://www.sueddeutsche.de/digital/2.220/facebook-kuendigt-neue-funktion-an-aendern-statt-loeschen-1.1391546

Talbot, D. (2012) *Mit Crowdsourcing zu mehr Privatsphäre.* In: Heise Technology Review. http://www.heise.de/tr/artikel/Mit-Crowdsourcing-zu-mehr-Privatsphaere-1517104.html

Tangens R. (2011). *Laudatio: Der BigBrotherAward 2011 in der Kategorie „Kommunikation"- eine „Gated Community".* In: http://www.bigbrotherawards.de/2011/.comm1

Tangens R. (2012) *Persönliches Interview 21. Juni 2012.* Bielefeld.

Tamir D. L. / Mitchell J. P. (2012). *Disclosing information about the self is intrinsically rewarding.*

Harvard University, Cambridge: PNAS Early Edition.

Taucis (2006). *Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung - Studie im Auftrag des Bundesministeriums für Bildung und Forschung.* Kiel - Berlin: Landeszentren für Datenschutz.

Thiel, P. A. (2009). *The Education of a libertarian – reaction essay.*

Washington D.C.: Cato Unbound.

http://www.cato-unbound.org/2009/04/13/peter-thiel/the-education-of-a-libertarian/

Tomasello, M. (2002). *Die kulturelle Entwicklung des menschlichen*

Denkens: Zur Evolution der Kognition. Frankfurt am Main:

Suhrkamp Verlag.

VPRT Verband Privater Rundfunk und Telemedien e.V. (2011). *Stellungnahme des VPRT zur Mitteilung der Kommission Gesamtkonzept für den Datenschutz in der EU.*
http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/vprt_de.pdf

Vukovic M. (2011). *Neue Nähe.* Berlin: Axel Springer Akademie.

http://www.youtube.com/watch?v=vK2_3WRRqgQ

Weichert T. (2012) *Social Media Chancen und Risiken.* Flensburg: AK Medien auf dem Campus.

www.datenschutzzentrum.de

Weiser M. (1991). *The Computer for the 21st Century*. Scientific American.

Reprint: http://cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf

Welt-Online. (2012). *Facebook und das Geld - Wie das Netzwerk überleben will.* In: Welt Online.
http://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article106768984/Wie-das-Netzwerk-ueberleben-will.html

ZDF heute. (2012). *Sendung vom 01. Juni 2012: USB-Sticks werden ab Juli teurer.*

http://www.zdf.de/ZDFmediathek/beitrag/video/1654478/ZDF-heute-Sendung-vom-01.Juni-2012

Anhang

7.5 Interview mit Dr. Gunnar Bender, Director Public Policy Facebook Germany

Interview mit Dr. Gunnar Bender, Director Public Policy Facebook Germany, am 11.07.2012 in Berlin. Das Interview führte Nina Forkefeld.

N. Forkefeld: Was ist die Aufgabe des Director Public Policy bei Facebook?

G. Bender: Im Wesentlichen geht es darum Aufklärung über Facebook zu betreiben. Das bedeutet ich werde dann kontaktiert, wenn irgendwo mal wieder eine öffentliche Facebook-Party stattfindet oder wenn es darum geht der Politik Hintergründe zu Facebooks Anwendungen zu erläutern.

N. Forkefeld: Wie wichtig ist Facebook die Interaktion mit den Nutzern?

G. Bender: Meine Position gibt es unter anderem deswegen, weil Facebook verstanden hat, dass es eine Schieflage in der Kommunikation gibt. Auch bei den Abstimmungen zu den neuen Nutzungsbedingungen hat Facebook versucht sich stark am Feedback der Nutzer zu orientieren. Facebook arbeitet derzeit verstärkt daran, die Nutzerwünsche zu verstehen und zu berücksichtigen.

N. Forkefeld: In letzter Zeit gab es u.a. wegen dem Börsengang viel negative Presse über Facebook. Besteht nicht die Gefahr, dass die Bedürfnisse der Aktionäre in den Vordergrund treten?

G. Bender: Facebooks größtes Anliegen ist nach wie vor die Zufriedenheit der Nutzer. Natürlich geht es Facebook auch um den unternehmerischen Erfolg, aber Facebook bemüht sich um mehr Transparenz, was das Agieren am Datenmarkt angeht. Meine Rolle ist es u.a. auch die Lücke zwischen Amerikanischem Handeln und Deutschem Handeln zu füllen. In Deutschland herrschen eben ganz andere Vorgaben als in den USA. Ich denke, dass Facebook zeigt, in dem es Leute wie mich einstellt, dass es die Schieflage verstanden hat.

N. Forkefeld: Wie sieht die Zukunft bei Facebook aus?

G. Bender: Facebook ist ein besonderes Unternehmen und das wird es auch bleiben. Das Unternehmen ist rasant gewachsen und mit Mark Zuckerberg, der ein sehr innovativer und außergewöhnlicher Unternehmer ist, wird das Unternehmen Schritt für Schritt weiter wachsen. Das Netzwerk hat schon jetzt ein enormes Potential und die Nutzerzahlen steigen noch immer. Ich denke die Erfolgsgeschichte Facebooks wird sich zweifellos fortsetzen.

7.6 Interview Axel Fischer (Vorsitzender Enquete Komission „Internet und Digitale Gesellschaft)

Interview Axel Fischer (Berlin, 26.04.2012) - Thema Datenschutz in Sozialen Netzwerken. Das Interview führte Nina Forkefeld.

1.) Wie würden Sie das heutige Internet und die Digitalgesellschaft charakterisieren? Welches sind Chancen? Welches Risiken der Digital-Gesellschaft?

Vereinfachte Kommunikation, schnellerer Zugang zu Information, neue Dienstleistungen sind nur einige Aspekte, die unsere derzeitige Entwicklung in das digitale Zeitalter kennzeichnen. Wie jedes Ding haben auch die vielfältigen Neuerungen in diesem Zusammenhang zwei Seiten: einfacherer Zugang zu digitalisierten Musikwerken erfreut jeden Einzelnen. Wenn damit jedoch im Rahmen einer Kostenloskultur z.B. durch illegale Kopien die Entlohnung von Kreativen in unserem Land nicht mehr in rechtlich vorgesehenem und gesellschaftlich erwünschtem Umfang sichergestellt ist, so müssen wir uns der Gefahr einer drohenden kulturelle Verarmung stellen. Das Hauptrisiko besteht aus meiner Sicht darin, dass wir unsere gesellschaftlichen Rahmen - auch den Rechtsrahmen - zu langsam bzw. nicht in geeigneter Weise an die durch das Internet induzierten ubiquitären Veränderungen anpassen. Im Mittelpunkt steht die Frage: Wie wollen wir unsere Gesellschaft von morgen gestalten, auf welchem freiheitlichen und nachhaltigen Weg in das Zeitalter der Digitalisierung überwiegen die Vorteile die Nachteile besonders, und wie beschreiten wir diesen Weg so, dass wir möglichst alle Menschen in unserem Land dabei mitnehmen?

2.) Wie würden Sie die zwei Arten von Öffentlichkeit (die virtuelle und die reale)

charakterisieren?

Handelnde Akteure, geltende Normen und andere Formen der Interaktion unterscheiden die virtuelle von der realen Öffentlichkeit. Eine verändert wahrgenommene Umgebung ändert die Verhaltensweisen der Nutzer im Internet. Virtuelle und reale Öffentlichkeit beeinflussen sich gegenseitig und wirken auf die Nutzer ein.

3.) Was gewichten Sie höher den Freiheitsanspruch von Individuen oder die individuelle Erhaltung der Menschenwürde?

Wie auch aus unserem Grundgesetz hervorgeht, findet die Freiheit jedes Menschen in unserer Gesellschaft ihre Grenze in den Rechten und besonders der Würde Anderer.

3.) Man sagt, Social Media Plattformen im Internet hätten eine demokratische Wächterfunktion. Ist diese These Ihrer Meinung nach haltbar?

Die Ereignisse in Nordafrika haben gezeigt, dass Social Media Plattformen erfolgreich als Kommunikationsinstrument zur Unterstützung demokratischer Bewegungen genutzt werden können.

4.) Wieso halten sie internationale Regelungen für das Internet für sinnvoll?

International einheitliche technische Standards ermöglichen den Datenaustausch über das Internet. Mit der weltweiten Vernetzung treten Akteure aus unterschiedlichen Kulturräumen mit jeweils anderen Sitten und Gebräuchen und unterschiedlichen Rechtssystemen in direkten Kontakt miteinander. Für eine dauerhaft zukunftsverträgliche weitere Entwicklung des Netzes als Kommunikations- und Austauschmedium wünsche ich mir - ähnlich dem physischen Handelsbereich - Rahmenbedingungen, die einen fruchtbaren Austausch aller Beteiligter auch unter Berücksichtigung kultureller Aspekte nachhaltig sichern.

5.) Warum ein Ausschuss für Internet und digitale Gesellschaft? Und was wären seine primären Aufgaben?

Siehe hierzu: http://blogfraktion.de/2012/02/08/wir-brauchen-einen-ausschuss-fur-internet-und-digitale-gesellschaft-im-deutschen-bundestag/

6.) Welches sind die wichtigsten Ziele, die sie beim Einsatz eines Internet-Ausschusses verfolgen möchten? Was müsste sich ändern?

Siehe hierzu: http://blogfraktion.de/2012/02/08/wir-brauchen-einen-ausschuss-fur-internet-und-digitale-gesellschaft-im-deutschen-bundestag/

7.) Haben Sie selbst das Gefühl die Kontrolle über die von Ihnen im Internet freigegebenen Informationen und Daten zu haben? Wie wichtig finden Sie in diesem Zusammenhang ein Radiergummi?

Die Kontrolle über die weitere Verbreitung einmal freigegebener Informationen bzw. Daten im Internet entzieht sich weitgehend dem eigenen Einfluss. Ein "digitaler Radiergummi" zur allgemeinen Beförderung eines "Vergessens" im Internet würde aus heutiger Sicht Manches vereinfachen. Er kann jedoch im Zweifelsfall z.B. juristisches Vorgehen gegen unrechtmäßige Nutzung von Daten im Zweifel nicht ersetzen. Im Mittelpunkt der Bestrebungen muss daher die Erlangung bzw. Gewährung eines funktionierenden Ordnungsrahmens für das Netz stehen.

8.) Erachten Sie das Erlangen individueller Kontrolle über personenbezogene Daten und Einforderung von Nutzerdatentransparenz als staatliche oder gesellschaftliche Aufgabe?

?

9.) Wie stehen Sie heute zur aktuellen Datenschutz-Debatte? Halten Sie ein "Vermummungsverbot" im Internet noch immer für sinnvoll?

Ein ubiquitäres Vermummungsverbot im Internet hatte ich nie gefordert - es kann im Netz durchaus Rückzugsorte für anonyme Alkoholiker etc. geben.

Das Bewusstsein von Anonymität und damit der Verlust sozialer Kontrolle verleitet jedoch Menschen vielfältig zu Aggression und Beleidigungen. Sicherlich empfinde nicht nur ich die weitgehend sachlichen politischen Diskussionen bei fehlender Anonymität z.B. auf Facebook angenehmer als von Unterstellungen, Beschimpfungen, Beleidigungen und Verleumdungen geprägten Meinungsäußerungen auf manch anonymisierter Plattform. Mittels "Cyber-Mobbing" werden junge Menschen in den Selbstmord getrieben. Erfahrungen mit Junk-Mails, Schadprogrammen, Betrugsversuchen, Abmahnungen, Datendiebstahl

usw. lassen bei Vielen die Angst mit surfen. Wir müssen Wege finden und durchsetzbare Regeln einführen, die das Leben mit dem Internet für alle Gesellschaftsmitglieder erträglich machen, und nicht nur wirtschaftlichen Interessen bzw. den Ansprüchen einer vergleichsweise kleinen Gruppe sog. "Nerds" genügt. Geltendes deutsches Recht muss in Deutschland durchsetzbar sein.

10.) Sollte es Ihrer Meinung nach Gesetze gegen Internet-Beschimpfungen geben?

s.o.

11.) Wieviel Anonymität in sozialen Netzwerken ist Ihrer Meinung nach tragbar?

Jeder Anbieter sollte selbst darüber entscheiden, wie er sein Angebot gestaltet. Wichtig ist, dass geltendes Recht durchsetzbar sein muss, so dass auch für andere Beteiligte zunächst anonyme Nutzer für ihr Handeln gegebenenfalls zur Verantwortung gezogen werden können.

Bezogen auf die Klarnamen-Nennung im Internet:

12.) Was müssten Social Media Betreiber ändern? s.o.

13.) Was müssten Social Media Nutzer ändern? s.o.

14.) Welche Aufgaben hätte der Staat? s.o.

15.) Inwiefern hängt das durch das Internet veränderte

Informationsverhalten mit dem gesellschaftlichen Urteilsvermögen zusammen?

Dem Vorteil, über mehr Informationen aus mehr Quellen verfügen zu können, steht eine fehlende Filterfunktion teilweise unbekannter Medien gegenüber. Nutzer brauchen daher eine höhere Medienkompetenz, d.h. erhöhte Leistungen bei Themenfilterung, Wahrheits- und Relevanzbeurteilung.

16.)Welche Daten und Informationen sind schützenswert? Von wem? Gegen wen?

Datenschutz und Datensicherheit sind wichtige Themen.

17.) Welche Maßnahmen sind gegen Bildungen von Monopolen im Internet Ihrer Meinung nach erforderlich?

Welche Maßnahmen zur Sicherung eines funktionierenden Wettbewerbs von Marktteilnehmern zum Wohle deren Kunden mit Blick auf das Internet sinnvoll sein können, hängt vom konkreten Fall ab.

18.) Bedeutet für Sie persönlich die Nutzung von Social Media einen Gewinn an Sozialen Kontakten oder eher die Schwächung bestehender.

Der erhöhte Austausch mit anderen Menschen via Social Media hat für mich nicht nur zum Kennenlernen vieler neuer Menschen, sondern auch zur Intensivierung von bereits bestehenden Beziehungen geführt. Ich glaube nicht, dass dadurch bestehende Beziehungen übermäßig belastet bzw. geschwächt worden wären.

7.7 Interview Stefan Lorenz, IT-Spezialist der Backes SRT GmbH

Interview mit Stefan Lorenz, IT-Spezialist der Backes SRT[16] GmbH, am 05. Juli 2012. Mit-Entwickler der Software X-Pire! (Datensicherheits-Software).

1.)N. Forkefeld: Gibt es überhaupt ein digitales Radiergummi?

S. Lorenz: Ein Digitales Radiergummi im Internet kann es nicht geben. Das ist technisch nicht möglich. Das hat folgenden Grund. In dem Moment, in dem ich ein Bild oder irgendwelche persönlichen Daten veröffentliche gebe ich sie aus meinem Kontrollbereich ab, in den Kontrollbereich von Anderen. Sie können sich beispielsweise mein Bild herunter laden auf Ihren Rechner. Wollte ich jetzt sicherstellen, dass ich dieses Bild löschen kann, bräuchte ich Zugriff auf Ihren Rechner. Das wiederum kann nicht in Ihrem Sinne sein. Was wir mit unserer Software X-Pire! versucht haben ist zu testen, wie weit man gehen kann. Technisch wurden Schlüssel auf Server hochgeladen und das Bild wurde verschlüsselt und in einem anderen Bild untergebracht.

2.)N. Forkefeld: Funktioniert dieses Verfahren nur mit Bildern, oder auch mit anderen Daten?

S. Lorenz: Das X-Pire!-Verfahren ist ohne weiteres auf andere Dateien ausweitbar. Was wir durch die Verschlüsselungs-Mechanik erreicht haben ist, dass nach zeitlichem Verfall des Schlüssels das Bild oder die Datei nachträglich nicht mehr verfügbar ist oder eingesehen werden kann. Hätten Sie Ihre Fotos also mit einem

[16] SRT = Security research & technologies

Schlüssel geschützt, könnte ich heute nicht mehr sehen, was Sie früher in Sozialen Netzwerken getan haben. Ich könnte mir aber durchaus heute all Ihre ungeschützten Bilder und Dateien kopieren und sichern und könnte über eine Dauer die mir beliebt darüber verfügen. Die Kritik ist aus diesem Grund, dass die Software nur einen unzureichenden Datenschutz bietet.

3.)N. Forkefeld: Wie schätzen Sie die Rolle der Politik beim Thema Datenschutz ein?

S. Lorenz: Es muss Grenzen geben, die die Politik vorschreibt. Es muss vor allem Grenzen für die Betreiber Sozialer Netzwerke geben. Es kann kein keinen technischen Schutz geben, also sollte die Politik auf Datenschutzthemen einwirken. Das wichtigste was sie Politik tun kann, ist über Gefahren aufzuklären, den Benutzer dazu zu bringen eine Haltung einzunehmen, bei der er selbst umsichtig und vorsichtig ist mit seinen Daten umgeht. Es geht darum, dass der Nutzer realisiert, dass einmal preisgegebene Daten weg sind – das haben die meisten nämlich noch nicht realisiert. Es gibt sehr viele die haben das noch nicht verstanden und an diesem Punkt wäre Aufklärungsarbeit angebracht.

4.)N. Forkefeld: Sollte die Politik den Betreibern Sozialer Netzwerke X-Pire verordnen?

S. Lorenz: Ich weiß nicht ob die Politik das kann, da ich nicht weiß ob ein solcher Eingriff juristisch möglich wäre. Das Kapital von z.B. Facebook ist die Menge an Daten, die Menge an Nutzern und auch die Qualität dieser Daten. In diesem Fall diesen Zugriff zu gestatten wäre wirklich ein Zugriff auf das Kernpotential des Unternehmens. Ich glaube nicht, dass irgendein Unternehmen der Welt sich gerne auf seine Kernkompetenz zugreifen lassen wollen würde. Zudem würde die Qualität der Daten darunter leiden, denn auf einmal könnte jeder Nutzer zu jeder Zeit seine Daten ändern oder löschen. Das widerspricht zutiefst dem Gedanken und den Geschäftsinteressen von Facebook. Aber X-Pire! wäre mit Sicherheit eine Möglichkeit den Nutzern wieder etwas Kontrolle zurück zu geben.

5.)N. Forkefeld: Was sollten die Betreiber tun?

S. Lorenz: Es muss Grenzen für die Spielregeln geben, die Betreiber bekommen. Die Politik muss sagen, ihr müsst prinzipiell, wenn eine Nutzeranfrage vorliegt die

Daten zu löschen, diese Daten tatsächlich löschen. Das wäre ein wichtiger Schritt, dass sich Betreiber an die politischen Spielregeln halten und diese ausführen. Als Nutzer hat man jederzeit das Recht die eigenen Daten einzusehen und die Frage zu stellen, welche Daten von einem selbst gespeichert sind. Der Nutzer hat zudem ein Anrecht darauf, dass diese Daten (sollten sie nicht aus rechtlichen Gründen vorgehalten werden müssen) gelöscht werden. Nur halten sich die Betreiber nicht daran, das muss auch umgesetzt werden. Das muss seitens der Politik forciert werden.

6.)N. Forkefeld: Wie könnte ein solches Einwirken konkret aussehen?

S. Lorenz: Betreiber könnten beispielsweise gezwungen werden diese Löschung für den Nutzer bequem zu gestalten. Über Formulare auf der Website könnte der Nutzer die Löschung der eigenen Daten beantragen. Es wäre ein minimaler Eingriff seitens der Politik, den Nutzern die Möglichkeit zu geben Daten löschen zu lassen. Dennoch ist eine solche Löschung bei Sozialen Netzwerken technisch nicht ganz leicht. Problematisch ist das z.B. bei Facebook, die Daten werden in drei Way-Back-Maschinen nachgehalten, auch wenn Facebook diese bereits gelöscht hat. Dieser Prozess führt dazu, dass das Internet nichts vergisst.

7.)N. Forkefeld: Was kann ich heute als Nutzer tun um meine eigenen Daten zu schützen, wie kann Ihre Software helfen?

S. Lorenz: Was jetzt schon im Netz ist, ist drin. Die Kontrolle darüber haben Sie verloren. Nachträglich etwas zurückzuholen, wie der Begriff „Digitales Radiergummi“ nahelegt, ist leider unmöglich. Was man machen kann ist, wenn Sie ein neues Bild einstellen möchten, dann könnten Sie das Bild mit dem Programm bearbeiten und schützen und dann dieses geschützte Bild einstellen. Das ist insofern ein Schutz, als dass wenn später jemand dieses Bild sucht, nachdem es schon verfallen ist, dieses Bild dann nicht mehr ansehen kann. Problematisch ist aber, dass das Bild auch eine Gültigkeit hat. In den nächsten Wochen soll z.B. jeder dieses Bild sehen können. Wenn aber in dieser Zeit in der das Bild gültig ist, jemand eine Kopie anfertigt, dann hat er das Bild trotzdem. Das lässt sich nicht verhindern. Denn alles was ich sehen kann, das kann ich auch kopieren. Die Möglichkeiten seine Daten technisch zu schützen sind deshalb extrem eingeschränkt. Etwas gar nicht erst Online zu stellen ist bislang der beste Schutz, den Sie haben.

8.)N. Forkefeld: Wie sieht es mit geschützten Strukturen, wie Intranet aus?

S. Lorenz: Das ist etwas anders in diesem Szenario, da ich ja weiß wer auf die Daten zugreifen wird, kann ich diese Teile verschlüsseln. Dann kann ich nur den ausgewählten Leuten, die Zugriff haben sollen, diesen Schlüssel geben. Ich bin dann immer noch darauf angewiesen, dass diejenigen die Zugriff auf die Daten haben keinen Missbrauch betreiben.

9.)N. Forkefeld: Wie funktioniert X-Pire!?

S. Lorenz: Sie geben eine Datei z.B. ein Bild in das X-Pire!-Programm. Dort wird die Datei verschlüsselt. Dieser Schlüssel wird auf einen Schlüsselserver hochgeladen. Dieser Schlüsselserver gehört Ihnen entweder selbst oder einer Instanz der sie vertrauen. Dann wird in diese Datei die Information eingebettet, wo dieser Schlüssel sich befindet. Geht nun jemand mit seinem Browser auf das Bild und möchte es betrachten, fragt das Plugin automatisch beim Schlüsselserver an, ob er dieses Bild freigeben kann. Ist das Bild abgelaufen, kann es nicht mehr betrachtet werden.

7.8 Interview Peter Schaar Bundesdatenschutzbeauftragter

Interview mit Peter Schaar Bundesdatenschutzbeauftragter am 27.04.2012 in Berlin. Das Interview führte Nina Forkefeld.

1) Gibt es ein Datentransparenzoptimum?

Die Frage ist ob es überhaupt ein Optimum der Transparenz gibt, genauso wie ein Optimum des Datenschutzes schwierig auszumachen ist. Wir kommen ja von einer grundrechtsorientierten Sichtweise, dass es so etwas gibt, wie ein Grundrecht auf Privatsphäre oder einen Schutz von personenbezogenen Daten, oder wie das Bundesverfassungsgericht sagt, ein informationelles Selbstbestimmungsrecht.

Jetzt muss gefragt werden, was sind die entgegenstehenden Interessen? Und in dem Moment in dem der Betroffene selbst entscheidet seine Daten transparent zu machen, also zu veröffentlichen oder in ein solches Netzwerk einzustellen, ist es sicherlich

nicht Aufgabe des Datenschutzes den Einzelnen daran zu hindern. Insofern gibt es keine Probleme damit, dass man Informationen über sich selber preisgibt. Wenn man jetzt aber Informationen über Dritte preisgibt, dann ist das natürlich eine Beeinträchtigung von deren Interessen und rein rechtlich gesehen bedeutet das, dass man deren Einwilligung braucht oder eben einen Rechtfertigungsgrund. Das ist die juristische Betrachtungsweise. Im Hinblick auf das Verhältnis Kunde – Unternehmen, also Facebook vs. Facebook-Nutzer ist es so, dass ja nicht nur die Informationen preisgegeben werden, die man dem Unternehmen bewusst gibt, sondern durch sein Verhalten im Netzwerk - ich melde mich an, ich gehe auf irgendwelche Seiten, ich interessiere mich für jemanden anders – werden Informationen auch über das Nutzungsverhalten offenbart.

Ein weiterer Punkt ist, gerade bei sozialen Netzwerken haben Sie eine Verknüpfung von Nutzer-Profilen, im Sinne von Mitglieder-Profilen, die Einblicke gestatten, die der Einzelne gar nicht steuern kann. Also derjenige der ein bestimmtes Hobby hat, dieses Hobby aber aus irgendeinem Grund nicht preisgeben möchte, steht vor der Problematik, dass seine Freunde aber dieses Hobby auch alle haben. Sobald die Freunde des Betroffenen dieses Hobby aber in ihrem Nutzerprofil mit eingestellt haben, gibt es eine gewisse Wahrscheinlichkeit, den Schluss zu ziehen, dass diese Person auch dieses Hobbys teilt. Das kann für Leseinteressen, politische Meinungen, sexuelle Orientierung, religiöse Anschauung, usw. gelten. Die Frage ist, kann man dort Optimalitätsüberlegungen anstellen.

2) Sollte es eine gesetzliche Rahmenregelung geben, oder wäre ein Bildungs- beziehungsweise Aufklärungs-Ansatz sinnvoller?

Das ist nur ein Ansatz unter verschiedenen, den Nutzer zu einem mündigen Nutzer zu machen, was A) Transparenz und B) Entscheidungsfreiheit voraussetzt. Und Entscheidungsfreiheit setzt wiederum voraus, dass der Dienst so konstruiert ist, dass diese Entscheidungsfreiheit tatsächlich gewährleistet ist. Es geht dabei nicht nur um das Stichwort „Privacy-by-design“ sondern auch darum, was sind die richtigen Voreinstellungen und das ist dann der „Privacy-by-default“-Ansatz. Da muss man den Faulheitsfaktor mit einbeziehen, d.h. erfahrungsgemäß - und das ist bei sozialen Netzwerken nicht anders als bei anderen Verhaltensweisen, egal ob es um eine

Kundenkarte geht oder um sonstige Angebote - die Voreinstellungen entscheiden in minimal 80% der Fälle darüber, welche Settings letztlich Bestand haben. Und vom Unternehmen her, dass auf diese Vernetzung und Preisgabe von Daten setzt – und das ist ja die Geschäftsidee von Facebook- ist der „Privacy-by-default“ –Ansatz etwas, dass im Grundsatz gegen die Geschäftsinteressen von Facebook gerichtet ist.

Während der Nutzer prinzipiell sicherlich eher diesen Privatsphären-Ansatz - je nachdem wie er sich einem solchen Dienst nähert, und ob er nur bereit ist sich mit Freunden auszutauschen – im Vordergrund sieht. Als Datenschützer trete ich für diesen „Privacy-by-default“ –Ansatz ein.

3) Sie setzen sich stark für eine europaweite Datentransparenz ein. Was halten Sie im Zuge der aktuellen Datenvorratsspeicherung-Debatte für sinnvoll? Wie lange sollte man auf Daten zugreifen können?

Also grundsätzlich gilt im Datenschutz, dass die Daten nur so lange und auch nur insoweit gespeichert werden sollten, wie es wirklich erforderlich ist.

4) Sie meinen den Grundsatz der Datensparsamkeit?

Nein das ist nochmal vorgelagert, aus diesem Grundsatz die Datenverarbeitung nicht völlig frei zu geben, sondern da eben einen Interessenausgleich hinzubekommen, wird da eben differenziert zwischen einem Kaufvertrag, wo bestimmte Daten wie z.B. die Kontonummer, Lieferadresse erforderlich sind und einer Verarbeitung für Werbezwecke, die ja einseitig im Sinne des Unternehmens oder des Werbetreibenden sind. Bei diesen Interessen, die durchaus berechtigt sind – da sind Sie dann bei einem Trade Off irgendwo, da können Sie dann wohlfahrtsökonomische Überlegungen anstellen – muss man dann fragen, wie groß ist das Interesse des Unternehmens an der Verwendung der Daten für Werbezwecke oder zum Zuspielen von bestimmten Informationen, also Targeting vs. dem Interesse des Einzelnen alleine gelassen und nicht gestört zu werden, nicht Objekt der Datenverarbeitung Dritter zu sein. Davon hängen dann rechtliche Konstruktionen ab, wo man dann sagt, naja also wenn jetzt eine Vollregistrierung aller meiner Interessen statt findet, ist das unverhältnismäßig. Wenn dann die Daten aber anonym gespeichert werden, und der Werbetreibende gar nicht weiß wessen Daten es sind und um welche Person es sich handelt und ihn das eigentlich gar nicht interessiert, dann ist die Beeinträchtigung

möglicherweise doch nicht so groß. Man muss fragen, welche Daten werden verarbeitet, für welchen Zweck sind sie ursprünglich erhoben worden, wie intensiv ist die Verarbeitung. In einem sozialen Netzwerk ist die Erwartung dass die Daten geschützt sind geringer, als wenn es sich um die Daten einer privaten Krankenversicherung handelt. Das sind die Rahmenaspekte, die berücksichtigt werden müssen und die dann auch zu unterschiedlichen Gewichtungen führen bei solchen Interessenausgleichen.

5) Wie unterscheidet sich der Datenmarkt von anderen Märkten?

Nun, der Datenmarkt unterscheidet sich natürlich in erster Linie dadurch von anderen Märkten, dass es sich um einen Markt mit virtuellen Produkten handelt. Insofern ist es so, dass die Daten nicht verschwinden, wenn Sie gedoppelt werden. Der Datengebrauch ist (das ist auch der Kern der Urheberrechtsdebatte) sofern keine Regulierung stattfindet, prinzipiell mit keinen Grenzkosten verbunden. Das ist natürlich der entscheidende Unterschied. Man kann jetzt über rechtliche Begrenzungen, siehe Urheberrecht, siehe Datenschutz, den Markt versuchen in ein konventionelles Raster einzufügen, was natürlich nicht immer so ganz einfach ist.

6) Wie kann man Anreize für mehr Transparenz und mehr Strukturierung setzen (sowohl bei Betreibern als auch beim Staat)? Wie kann mehr Übersichtlichkeit für den Endnutzer bzw. den Bürger geschaffen werden?

Da gibt es verschiedene Ansätze. Das eine ist die Möglichkeit diese sehr komplexen Strukturen öffentlich zu machen, das führt aber zu dem Problem, dass der Rezipient dieser Information sehr hohen Aufwand betreiben muss, um diese Information überhaupt zu verstehen und zu bewerten. Ob er das überhaupt kann ist fraglich, weil die Komplexität riesig ist. Die zweite Möglichkeit wäre zu differenzieren zwischen Kern-Informationen und Informationen die in extenso die Hintergründe noch einmal beleuchten: Wir bearbeiten das und das Datum, für den und den Zweck und die Daten werden dort verarbeitet. Vielleicht drei Kerninformationen, Art der Daten, verantwortliche Stelle, Zweck der Datenverarbeitung, und dann könnte man natürlich in einem gestuften System dem Interessierten mehr Informationen zur Verfügung stellen. Das ist das Prinzip der sogenannten „layered notices“, ein Ansatz der auch schon seit längerem im Datenschutz diskutiert wird. Eine andere Möglichkeit ist eine Art von Standardisierung vorzunehmen anhand von Kriterien-Katalogen zu sagen,

das entspricht einer Vorgabe z.B. dem Datenschutzrecht oder einem bestimmten Qualitätsanspruch. Dann würde man durch z.B. Zertifikate oder Gütesiegel oder vergleichbare Instrumente das Nutzervertrauen befriedigen. Das kann man dann auch noch stufen nach unterschiedlichen Klassen, aber im Grundsatz läuft dieser Ansatz stets nach dem gleichen Muster ab.

7) Wie ist Deutschland datenschutzrechtlich gegenüber anderen europäischen Ländern aufgestellt?

Das ist ganz schwer zu sagen. Gerade im Datenschutzrecht haben wir schon seit 1995 eine europäische Richtlinie. Gerade wird darüber diskutiert diese Richtlinie durch eine Verordnung zu ersetzen. Das ist gerade das aktuellste Thema mit dem wir täglich zu tun haben. Insofern haben wir im großen und ganzen ein vergleichbares Schutzniveau, aber ich kann nicht Deutschland im Vergleich zu anderen Ländern z.B. Italien, Spanien, usw. hervorheben. Es gibt Bereiche in denen Deutschland besonders gute Regelungen hat und andere in denen Deutschland hinterher hinkt. Insofern tue ich mich schwer mit so einem Ranking. Es gibt verschiedene Versuche zu so einem Ranking und das können Sie auch nachlesen. Die sind aber immer auch zu hinterfragen, was sind eigentlich die Kriterien die da angelegt worden sind. Danach schnitt Deutschland noch relativ gut ab, auch im europäischen Vergleich und bei privacy international.

8) Halten Sie Deutschland für überreguliert?

Nein, aber ich denke dass der Datenschutz in seiner Grundstruktur schon etwas bejahrt ist und auf anderen Datenverarbeitungsmodellen beruhte, als sie heute in der Netzwerkökonomie alltäglich sind. Insofern ist eine Überarbeitung und Modernisierung dringend erforderlich, aber nicht nur in Deutschland. Ich glaube auch überhaupt nicht daran, dass Datenschutz durch nationales Recht, jedenfalls im Bereich der Netzwerkökonomie, regeln kann. Da brauchen wir mindestens einen europäischen Ansatz und das hat die Europäische Kommission ja auch verstanden und deshalb auch ein Datenschutzpaket vorgelegt.

9) Welches ist die größte Herausforderung vor der Sie in Ihrem Amt momentan stehen?

Das zentrale Problem ist die fortschreitende technologische Entwicklung mit immer intensiverer Vernetzung, Stichwort: Ubiquitous Computing. Wobei das Internet als Schiene für diese Vernetzung verwendet wird. Es geht um Integration von IT in Alltagsgegenstände verknüpft mit dem Internet.

10) Welches ist der Schwerpunkt Ihrer Arbeit? Sind Sie der Meinung, dass es besonders schützenswerte Daten gibt?

Das ist eine Möglichkeit einen Sensitivitätsansatz der Daten zu wählen. Für mich ist aber das zentrale Problem die Profilbildung. Unabhängig von der Sensitivität des Einzeldatums kann die Verknüpfung unterschiedlichster Informationen dazu führen, über diesen Umweg möglicherweise sehr, sehr sensible Informationen über diese Person zu gewinnen: Wenn man das Surfverhalten auswertet, wenn man den Klickstream erfassen kann, wenn man den Inhalt von E-Mails erfassen kann, wenn man den Terminkalender heranzieht. Ich spreche hier jetzt nicht explizit von Google, aber Google folgt ja genau diesem Modell. Und Facebook sozusagen von der anderen Seite auch. Das man alles Mögliche in die Welt einer Infrastruktur integriert und dabei alle möglichen Informationen, die an unterschiedlicher Stelle angefallen sind zusammenführt, ob das nun in der Timeline ist, oder ob das nun ein Google-Profil ist.

11) Wie kann man es hinbekommen, dass es das Recht des „Vergessen-werdens" oder ein Radiergummi gibt?

Das ist eine relativ neue Diskussion zu einem alten Thema. Grundsätzlich gibt es schon Löschungsansprüche, seit es das Datenschutzrecht gibt, müssen bestimmte Daten wieder gelöscht werden. Das Problem ist, dass im Internet einmal veröffentlichte Informationen wieder schwer zurückholbar sind. Und die bisher vorgeschlagenen technischen Verfahren führen auch nur zu einer teilweisen Zurückholung von Daten. So dass man wahrscheinlich damit leben muss, dass technisch eine hundertprozentige Löschung einmal veröffentlichter Daten nicht gelingen wird. Andererseits ist es durchaus denkbar dass man, wie es auch schon vorgeschlagen wird in der Literatur, über ein Verfallsdatum nachdenkt. Das einer Information ein Datum angeheftet wird, also dass der Einzelne selber, wenn er eine bestimmte Information öffentlich macht, sagt diese Information sollte nach 5 Jahren nicht mehr recherchierbar sein. Das wäre technisch nicht hundertprozentig

durchführbar, aber es könnte im Hinblick auf die Legitimität und möglicherweise auch auf die Legalität der Datennutzung dann bedeutsam sein, wenn man sagt, diese Daten sollen dann nicht mehr verwendet werden und sollten möglichst gelöscht werden. Und wer das missachtet wird vielleicht auch andere Vorgaben missachten. Insofern sind Regeln so gut wie niemals derart, dass sie sich selbst exekutieren und zu hundertprozentigen Lösungen führen.

12) Wie schlimm steht es um die Datensammlungen wirklich? Muss die Allgemeinheit befürchten, dass im Facebook – Vorstand CIA-Mitarbeiter sitzen?

Das ist natürlich Quatsch. Es ist generell Quatsch einem verschwörungstheoretischen Ansatz zu folgen. Dem folge ich nicht. Der entscheidende Punkt ist, dass die Datenmacht von so großen Unternehmen, die ihre Geschäftsmodelle auf dem Sammeln persönlicher Daten aufbauen, außergewöhnlich groß ist. Insofern ist es so, dass ein echter Markt gar nicht mehr besteht und dass durch diese Datenkonzentration genau diese Profilbildung erfolgt, die den Einzelnen letztlich nicht mehr frei lässt. Das ist das zentrale Problem, dass damit möglicherweise Schindluder getrieben wird, dass da irgendwelche bösen Menschen sitzen wie überall auf der Welt - es kann einem auch die Gelbörse geklaut werden, das kommt vor – das will ich hier aber nicht unterstellen. Problematisch ist dieses strukturelle Ungleichgewicht zwischen Nutzer und Unternehmen.

13) Was kann man gegen diese Monopolbildung im Internet tun?

Es gibt Ansätze die ähnlich sind wie im Kartell-Recht. Das heißt, dass man durchaus nicht nur bei verkauften Gütern, sondern auch bei solchen Datendiensten den Markt beobachtet und gegebenenfalls zu Entflechtungen beiträgt.

Ein Anbieter der E-Mail und andere Kommunikationsmöglichkeiten anbietet kann dann in Zukunft nicht mehr zusätzlich auch noch ein soziales Netzwerk betreiben. Das wäre ja eine Form von Entflechtung, die denkbar wäre. Eine regionale Entflechtung ist heute im Internetzeitalter nicht mehr zweckmäßig.

14) Welches ist Ihrer Meinung nach die gefährlichere Datenkrake, eher Google oder eher Facebook?

Ich will da jetzt gar keine Bewertung vornehmen. Ich denke beide Unternehmen haben ungeheure Datensammlungen angehäuft und beide Unternehmen haben mit differierenden Geschäftsmodellen jeweils das Interesse die Kunden in ihren Strukturen zu halten und die Daten aus den verschiedenen Bereichen zu verknüpfen. Wobei mein Eindruck ist, dass Google im Hinblick auf die Datenmengen doch noch sehr weit vorne ist, ohne dass ich das jetzt zahlenmäßig belegen kann, im Vergleich zu Facebook. Allerdings holt Facebook schon auf. Aber ich will hier keine moralischen Kategorien einführen. Google hat ein bisschen früher begonnen, also haben sie auch ein bisschen früher von Datenschutz gehört. Insofern haben sie auch da einen gewissen Vorsprung, ohne das ich jetzt Google übermäßig loben würde.

15) Sie sagten Eingang der „privacy-by-default"-Ansatz sei der spannendere. Dieser setzt aber auch wieder eine Nutzersensibilisierung voraus?

Er setzt voraus, dass der nicht sensible Nutzer eine Art Grundschutz genießt. Das heißt ich werde Kunde bei einem Dienst und kann mir sicher sein, dass in der Umgebung in der ich mich bewege, meine Daten angemessen gesichert sind.

7.9 Studie Diana Tamir

7.10 Interview Rena Tangens, FoeBuD e.V.

Interview Frau Rena Tangens am 21. Juni 2012 in Bielefeld. Das Interview führte Nina Forkefeld.

1.) Welche Parallelen hat Facebook heute zu George Orwell's Roman 1984?

Die viel interessantere Parallele gibt es bei Aldous Huxleys "Brave New World". Denn in 1984 geht es um einen totalitären Staat, bei Huxley um den unbegrenzten Konsum und die freiwillige Normierung, die unfrei machen. Unbedingte Leseempfehlung!

2.)Halten Sie die aktuellen Veränderungen in den Facebook- Datenschutzbstimmungen für sinnvoll?

Natürlich nicht. Die alten und die neuen Datenschutzbestimmungen bei Facebook sind eine Farce.

3.) Wie lange sollte Ihrer Meinung nach eine Vorratsdatenspeicherung gewährleistet sein?

Der FoeBuD ist Teil des AK Vorrat, der die Vorratsdatenspeicherung aus guten Gründen ablehnt.
5-Minuten-Info:
http://www.vorratsdatenspeicherung.de/
Video
http://www.stop-vds.de/blog/

Aber: Was hat die Vorratsdatenspeicherung mit Facebook oder anderen sozialen Netzwerken zu tun?

4.) Wie denken Sie über einen privacy-by-default-Ansatz, also Datenschutz durch Nutzervoreinstellungen?

Privacy by default – also datenschutzgerechte Standardeinstellungen fordern wir schon seit langem. Wir haben dazu auch gemeinsam mit dem vzbv (Verbraucherzentrale Bundesverband) eine Unterschriftensammlung gemacht.
Privacy by default wird Facebook allerdings wohl kaum einführen, da es ihrem Geschäftsmodell (Pseudo-gratis gegen persönliche Daten und Beziehungen) zuwiderläuft.

5.) Wer profitiert noch von den Datensammlungen der Social Networks?

An allererster Stelle Facebook selbst. Denn was den meisten Nutzer/innen offenbar nicht klar ist: Egal, wie restriktiv sie ihre Datenschutzeinstellungen getrimmt haben: Facebook kann alles lesen.

Und Facebook kann bestimmen, wem sie was weitergeben. Erste Profiteure sind natürlich Werbekunden. Aber auch die us-amerikanischen Dienste. Und jeder andere, dem Facebook die Daten oder auch Erkenntnisse daraus zugänglich macht.

Durch die Auswertung der persönlichen Beziehungen, der Analyse wer im Freundeskreis

besonderes Vertrauen genießt sowie aller persönlichen Äußerungen ist aktiver Manipulation Tür und Tor geöffnet.

6.) Halten Sie die Einführung eines „Verfallsdatums“ für Informationen für sinnvoll? Oder die Einführung eines „Radiergummis“ für persönliche Daten?

Das Verfallsdatum wird wenig helfen. Denn wer weiß schon heute, was ihm oder ihr morgen peinlich oder schädlich sein könnte? Das vom Innenministerium sogenannte "Radiergummi" gibt es nicht. Es ist ein irreführender Begriff. Die vorgestellte Implementation war das Mitgeben eines Verfallsdatums bei Bildern. Und das ist a) aus oben genannten Gründen nicht praktikabel und b) kann es die Löschung nicht garantieren.

7.) Was müssten Facebook und Google in Deutschland ihrer Auffassung nach tun, um das Nutzer- und Kundenvertrauen zu stärken?

Facebook und Google sollen nicht das Kundenvertrauen "stärken", sondern
sie müssen es sich erst einmal verdienen. Und dazu müssten sie ihr Geschäftsmodell ändern. Denn: Wenn du für den Dienst eines Konzerns im Internet nichts bezahlst, bist du nicht Kunde oder Kundin, sondern das Produkt, das verkauft wird.

http://www.zeit.de/2011/40/Jon-Callas-ueber-Facebook/seite-1

8.) Welches ist Ihrer Einschätzung nach das problematischste Vergehen Facebooks? Die Presse erwähnt zur Zeit vor allem Ideenklau bei Patenten, die Intransparenz der Nutzungsbedingungen, sowie die Profilbildung und Auswertung von Klickraten?

Der systematische Verstoß gegen Datenschutzgesetze, die systematische Intransparenz, die dazu dient, die Nutzer/innen im Dunkeln zu lassen über diese Datenschutzverstöße, Profilbildung und Auswertung von Klickraten. Das größte Problem aber ist die Monopolbildung und die Ausweitung des Einflussbereichs von Facebook über Like-Buttons etc. – kurz gesagt, dass Facebook die zentrale Plattform für die Internet-Nutzer/innen werden will. Verschärfend kommt dazu, dass die öffentliche Hand, Städte und der Rundfunk so blauäugig sind, sich mit ihren Angeboten zu Facebook begeben,

anstatt ihre eigenen unabhängigen Webseiten zu pflegen. Sie liefern damit nicht nur sich selbst, sondern zugleich ihre Nutzer/innen der Willkür von Facebook aus.

Europe vs. Facebook
http://europe-v-facebook.org/DE/de.html

9.) Für wie intensiv schätzen Sie den zukünftigen Investoren-Einfluss auf Facebook ein?

Der steht im Gesetz: Aktiengesellschaften sind Treuhänder des Geldes ihrer Aktionäre. Das heißt, Facebooks oberste Aufgabe ist, das Geld der Aktionäre zu mehren. Und das heißt im Klartext, dass sie die Facebook-Nutzer/innen noch viel mehr ausquetschen müssen als bisher schon: noch mehr Auswertung von Daten, mehr Werbung, und Aneignung der Inhalte der Nutzer/innen (wie in den neuen Nutzungsbedingungen geschehen.)

10.) Wie gefährlich sind „Instant Personalization“ und die Textanalyse für den „Happiness Index“? Wozu verwenden die Betreiber diese Auswertungen?

Instant personalization ist gefährlich – sie weitet den Einflussbereich von Facebook auf andere Webseiten im Internet aus. Der "Happiness-Index" ist schnuppe. Es ist nur ein schönes Beispiel, das belegt, dass Facebook eben auch alle persönlichen Nachrichten – also die zwischen zwei Nutzer/innen ausgetauscht wurden – von Facebook gescannt und ausgewertet werden.
Facebook kann mit der Auswertung der persönlichen Nachrichten eben auch andere Stimmungen entdecken, auswerten und für sich einsetzen. So hat Facebook eine Analyse der persönlichen Nachrichten der Beliebtheit der republikanischen Präsidentenkandidaten gemacht und veröffentlicht. (Dazu gab es diverser Presseberichte). Damit kann Facebook Einfluss nehmen. Niemand kann überprüfen, ob die Auswertung korrekt ist.
Facebook zensiert übrigens auch Nachrichten, die Facebook nicht genehm sind. So geschehen mit Nachrichten zu occupy, zu Pirate Bay.

Leseempfehlung: "Filter Bubble" von Eli Pariser
http://www.thefilterbubble.com/
http://www.zeit.de/2011/26/Internet-Surfverhalten-Filter

11.) Wie/mit welchen Rahmenbedingungen kann der Staat Social Media-Betreiber hinsichtlich eines besseren Datenschutzes positiv unterstützen?

Mit der Durchsetzung geltendes Rechtes. Das heißt, die Aufsichtsbehörden mit den entsprechenden Mitteln ausstatten, unabhängige Kontrollen und Sanktionen durchsetzen.

Innenminister Friedrich muss aufhören, dem Verbraucherschutzministerium und allen Datenschutzbeauftragten, die ihren Job ernst nehmen, in den Rücken zu fallen. Der Innenminister lässt sich von Facebooks Lobbyisten instrumentalisieren, wenn er öffentlich sagt, dass eine Selbstverpflichtung ja schon ok sei. Nein, ist sie nicht. Auch Facebook muss sich an geltendes Gesetz halten.

Andere Social Networks, die sich ihrerseits bemühen, Datenschutz bei sich umzusetzen, müssen sich durch dieses Verhalten völlig verarscht vorkommen.

Bitte hier weiterlesen:
ULD Schleswig-Holstein zu Facebook:
https://www.datenschutzzentrum.de/facebook/index.html

12.) Was kann gegen die Monopolbildung im Internet unternommen werden?

Eine gesetzliche Regulierung. Siehe Bundeskartellamt.
Um Wettbewerb zu ermöglichen, muss Datenportabilität durchgesetzt werden. Damit wäre es Nutzer/innen möglich, über die Grenzen einer Plattform hinaus mit anderen in Kontakt zu treten. So wie es bei eMail auch möglich ist, unabhängig von der Wahl des Mailproviders. Sobald diese plattformunabhängige Vernetzung durchgesetzt ist, können die Nutzer/innen sich endlich frei für eine Plattform entscheiden, etwa auch eine, die Datenschutz, Privatsphäre und europäische Gesetze achtet.

13.) Für wie brisant halten Sie die Verbindung des Facebook-Vorstandes zu amerikanischen Geheimdiensten?

Durch den Patriot Act (das Heimatschutzgesetz in den USA) haben die Geheimdienste

Zugriff auf alle Kommunikations-, Reise- und sonstigen Verkehrsdaten. Bei Facebook waren die Nutzungsbedingungen schon immer so formuliert, dass es allein in Facebooks Ermessen gestellt war, was sie an entsprechende Stellen weitergeben.
Mit den guten persönlichen Beziehungen wird hier wohl kaum noch ein richterlicher Beschluss eingeholt werden, um Daten weiter zu geben.
Zur politischen Einstellung von Peter Thiel lesen Sie bitte die angegebenen Links unter der BigBrotherAward-Laudatio. Zitat Peter Thiel " Most importantly, I no longer believe that freedom and democracy are compatible." (...) " The 1920s were the last decade in American history during which one could be genuinely optimistic about politics. Since 1920, the vast increase in welfare beneficiaries and the extension of the franchise to women — two constituencies that are notoriously tough for libertarians — have rendered the notion of “capitalist democracy” into an oxymoron."
http://www.cato-unbound.org/2009/04/13/peter-thiel/the-education-of-a-libertarian/