Die Ambivalenz von Filter- und Abblock-Verfahren im Internet

Ambivalence of filter and blocking software in the Internet

Rainer Kuhlen
Fachbereich Informatik und Informationswissenschaft - Universität Konstanz
Institut für Bibliothekswissenschaft, Humboldt-Universität zu Berlin

(Vortrag auf dem Weltkongress Sicherheit moderner technischer Systeme.
Saarbrücken. 12.-14. September 2001)

I.

Zusammenfassung/Abstract - Die grundlegenden Konzepte von *Rating*, Filtern und Abblocken werden diskutiert. Die Positionen und Interessen beim Einsatz und bei der Verhinderung von Filter- und Abblock-Verfahren werden herausgearbeitet, wobei diese in den weiteren politischen Kontext gestellt werden. Einige Anwendungen von Filter- und Abblock-Verfahren – Schulen, Bibliotheken, Unternehmen, Überwachung, *Service Provider* – werden exemplarisch vorgestellt. Die Ambivalenz von Softwarelösungen allgemein – verwertbar für disparate Zwecke – wird im Blick auf Filter- und Abblock-Verfahren diskutiert, und schließlich wird ein Raster für die Einschätzung des Einsatzes von Filter- und Abblock-Verfahren vorgeschlagen.

The basic concepts of Rating, filtering and blocking are discussed. The divergent interests in filter and blocking software and corresponding anti-software are positioned in their political context. Prototypical applications of filter and blocking software (in schools, libraries, enterprises, service providers, state surveillance control) are presented. The ambivalence of software in general and with respect to filter and blocking software is discussed and, finally, a catalogue for the evaluation of filter and blocking software is proposed.

Index terms – Ad-Blocking, Anti-Filter, Blocking, Carnivore, Cryptography, Echelon, Filtering, Free flow of information, Hacker, Information interests, Information politics, Parental control, PeekaBooty, PICS, *Rating*, Stealth blocking, Surveillance, TestFinder

II. Die Verfahren

In diesem Beitrag geht es primär um die politischen und sozialen Aspekte und Konsequenzen von Filter-/Abblock- und *Rating*-Verfahren. Auf die zentralen Begriffe wird hier zu Beginn nur kurz eingegangen (entsprechend [1], [2], [3]).

Rating ist die Einschätzung und Bewertung von Informationsobjekten bezüglich der Qualität ihrer Inhalte und somit die Basis für Filtern und Blocken. Im *Rating*, sei es intellektuell oder maschinell durchgeführt, liegt der Sprengstoff, da die zum Einsatz kommenden Bewertungsverfahren zwangsläufig, implizit oder explizit, subjektive

Interessenlagen oder bestimmte Wertesysteme widerspiegeln, die kaum intersubjektiv gültig sein können, zumal nicht in interkultureller Perspektive. Was positiv, was negativ ist, muss auf der Basis eines *Rating*-Verfahrens entschieden werden. Die Filter- und Abblock-Programme führen nur das aus, was durch *Rating* festgelegt wurde. Im wesentlichen kommen beim *Rating* drei Verfahren zum Einsatz:

- Verwendung von Listen von als positiv oder negativ eingeschätzten Internet-Objekten. Dadurch wird z.B. bei positiv eingestuften Internet-Anwendungen der Zugang nur über die ihnen zugeordneten URLs, IP-Adressen oder IRC *Chat Lines* bzw. *Newsgroups* ermöglicht, alles andere wird abgeblockt. Solche Verfahren verursachen hohen intellektuellen Einschätzungsaufwand. Die entsprechenden Listen werden in der Regel von den Anbietern kommerzieller Filter-/Abblock-Software geheimgehalten, sind aber entsprechend beliebte Zielobjekte der Entschlüsselung in der Hacker-Szene.
- Verwendung von positiven oder negativen *Keyword*-Listen (*white/black lists*), durch die die Internet-Objekte gefiltert oder abgeblockt werden, bei denen es eine (zu definierende) Übereinstimmung ihrer Wortvorkommen mit den Einträgen der *Keyword*-Listen gibt. Etwas elaboriertere Verfahren versuchen, den Kontext des Vorkommens der guten oder schlechten Wörter mitzuberücksichtigen, z.B. könnten Sex-Wörter in Umgebungen der Kunst oder Medizin nicht als negativ bewertet werden. Einfache Matching-Verfahren – sind einmal die Listen aufgebaut - sind unaufwendig, da voll automatisierbar zu betreiben. Ein gewisser laufender Pflegeaufwand ist jedoch zu leisten, um aktuell in der Listenterminologie bleiben zu können. Auch hier gelten die Listen als Betriebsgeheimnis der meisten Anbieter (mit den entsprechenden Entschlüsselungsanreizen und -anstrengungen). Angesichts der in der Vergangenheit geäußerten Kritik an der Intransparenz der *Rating*-Verfahren und –Inhalte, werden Listen heute immer häufiger offengelegt bzw. wird es den Nutzern ermöglicht, ihre eigenen Listen zu entwickeln und für Filtern und Blocken zu verwenden.
- Anwendung von expliziten *Rating*-Verfahren, nach denen Internet-Objekte nach vorgegebenen semantisch definierten Bewertungsskalen innerhalb festgelegter Gegenstandsbereiche (Sex, Gewalt, politischer Radikalismus etc.) meist intellektuell bewertet werden, so dass bei der Suche oder der Navigation in den Internet-Diensten nur die zugestellt werden, die direkt einem mit Hilfe des *Rating*-Systems ermittelten Profil entsprechen, bzw. die abgeblockt werden, die durch die *Rating*-Verfahren als negativ eingeschätzt wurden.
-

Rating-Verfahren stützen sich überwiegend auf den PICS-Standard (*Platform for Internet Content Selection*). PICS wurde entwickelt und gefördert vom *World Wide Web Consortium* (W3C) und ist im wesentlichen eine Sprache zur Formulierung von Filterregeln (Profilen), durch die der Zugriff oder das Abblocken von URLs (und damit der entsprechenden Web-Seiten) möglich wird, die durch PICS-Labels (sogenannte *rating tags*) im HTML-Code beschrieben werden. Einmal über PICS formulierte Profile könnten leicht von Personen und Institutionen übernommen bzw. auch modifiziert werden, um den

Aufwand der Eigenentwicklung gering zu halten und um verschiedene Anwendungen kompatibel zu halten. PICS ist also selber keine Filter-/Abblock- oder *Rating*-Software, sondern gibt technische Spezifikationen vor, auf deren Grundlage Bewertungsschemata, reale *Rating*-Software/-systeme entwickelt werden können[1].

Unter Filtern wird die positive Leistung von entsprechender Software verstanden, das an Information bereitzustellen, was gewünscht ist. Beim Einsatz von Filtern werden den Nutzern von Internet-Diensten ausschließlich die einem vorab definierten Profil entsprechenden Informationen zugestellt. Diese Leistung ist nur möglich, wenn die Informationselemente des Profils (z.B. eine Menge von inhaltsbeschreibenden Ausdrücken) mit den inhaltsbeschreibenden Elementen der Informationsobjekte im Internet übereinstimmen oder wenn die Objekte vorab explizit qualifiziert worden sind. Filterverfahren sind entsprechend in der Methodik verwandt mit den im *Information Retrieval* und beim *Data Mining* zum Einsatz kommenden Such-/Selektionsverfahren. Ihre Leistung besteht vor allem in der schnellen Verarbeitung großer Mengen an Text, wie es das durch die Firma Paracel[2] vertriebene und auch wohl bei Echelon (S. Abschnitt III) für das Filtern zum Einsatz kommende *TextFinder*-Verfahren tut, bei dem fast 15.000 Parallelprozessoren verwendet werden[3]. Weitergehende intelligente Verfahren, wie mit ihnen in der Künstlichen Intelligenz oder in der Agententechnologie experimentiert wird, kommen kaum zum Einsatz, auch wenn die Rede davon ist, dass bei anspruchsvollen Aufgaben, wie sie bei Echelon anfallen, auch sogenannte Themenanalysen (*topic analysis*) angewendet werden („finde Dokumente oder Textstellen, die Thema xyz zum Gegenstand haben"), die auf Assoziations-/ und Inferenzleistungen bzw. Ähnlichkeitsanalysen beruhen, also nicht nur auf dem bloßen Vorkommen von Wörtern oder Phrasen. Die erwähnte Firma Paracel gehört zum Geschäftsbereich von Celera Genomics, so dass mächtige Filterverfahren auch zum Zwecke der automatischen Analyse von Genomsequenzen eingesetzt werden.

Abblocken ist das inverse Gegenstück zum Filtern, also die negative Leistung, das fernzuhalten, was nicht gewünscht ist. Durch Blocken wird der Zugriff auf definierte, durch ein *Rating*-Verfahren qualifizierte Information verweigert bzw. unmöglich gemacht. Man spricht von passivem Blocken, wenn die Initiative zum Abblocken nicht von den Betroffenen selber ausgeht, sondern von Dritten auferlegt wird, z.B. wenn Staaten oder *Service Provider* den Internet-Zugang für ihre Bürger/Kunden durch Ausgrenzen bestimmter Inhalte oder *Websites* insgesamt einschränken, wenn Unternehmen nicht

---

[1] Bekannte Anwendungen von PICS, also Entwicklungen von *Rating*-Verfahren in inhaltlicher Sicht, sind *Safe Surf* (http://www.safesurf.com); ESRB (*Entertainment Software Rating Board*; http://esrb.org/about.html); *Net Shepherd* (http:/www.netshepherd.com); *evaluWEB* (http://calvin.ptloma.edu/~spectre/evaluweb/); *Safe for Kids Web Rating System* (http://www.weburbia.com/safe/) und vor allem RSACi (*Recreational Software Advisory Committee*; http://www.rsac.org/homepage.asp; auch Entwickler von *Rating*-Verfahren für Video-Spiele). Ein Beispiel für Rating in der Medizin nach PICS unter http://www.imbi.uni-freiburg.de/medinf/lehre/kollws9900/eysenbach/sld082.htm (Folie 82).

[2] http://www.paracel.com/

[3] Aus der Firmenbeschreibung: „The largest TextFinder installation filters the equivalent of 1,000 times all the major newspapers and newswires in the world, in many different languages, against tens of thousands of complex interest profiles. It also searches the world's largest online text archive, currently more than 10 terabytes, for thousands of analysts" (http://www.paracel.com/main.html).

jobbezogene Informationen gegenüber ihren Angestellten abblocken oder Bibliotheken im Auftrag ihrer Geldgeber gegenüber bestimmten Nutzergruppen nicht als korrekt angesehene Informationen ausblenden[4].

Abgeblockt werden kann im Prinzip alles durch jeden gegenüber jedem. Abblocken kann verdeckt geschehen, wenn Benutzer gar nicht erfahren, dass eine als abgeblockt klassifizierte Information existiert oder wenn ihnen suggeriert wird, dass die angewählte *Website* nicht (mehr) existiert. Man spricht von aktivem Blocken, wenn die Entscheidung, zu bestimmten Internet-Inhalten keinen Zugang zu haben, von den Betroffenen selber getroffen wird, sei es, dass direkter Einfluss auf die Ausgestaltung der zugrundeliegenden *Rating*-Verfahren genommen wird, sei es, dass man sich in einer Art Selbstzensur oder Selbstbeschränkung den Verfahren angebotener Software anvertraut.

III. Positionen und Interessen

Über kaum etwas wurde (und wird) im Internet so erbittert und mit so divergenten Interessen gestritten wie über die Frage der Filter- und Abblock-Verfahren, die auf der Grundlage von *Rating*-Verfahren für Angebot und Nutzung von Internet-Diensten immer mehr zum Einsatz kommen, und zwar quer durch alle Anwendungsgebiete, nicht mehr, wie ursprünglich, auf die Möglichkeit der Elternkontrolle über die Webnutzung ihrer Kinder (*parental control*) beschränkt.

Für die eine Position mag die seit 1997 im Netz verankerte Website der *American Civil Liberties Union* stehen[5], die den dramatisch programmatischen, die Dystopie beschwörenden Titel trägt „Fahrenheit 451.2: Is Cyberspace Burning? How *Rating* and Blocking Proposals May Torch Free Speech on the Internet"[6]. ACLU sah und sieht in jeder Bewertung von Internet-Inhalten, die anderen aufgezwungen wird, reale Zensur oder zumindest den Einstieg in Zensur und sei es nur in die Selbstzensur[7], auch wenn die

---

[4] Vgl. dazu http://www.bluehighways.com/filters/filtersc/sld001.htm

[5] www.aclu.org/issues/cyber/burning.html; zur Frage von *Blocking*-Software mit Blick auf öffentliche Bibliotheken vgl. http://www.aclu.org/issues/cyber/box.html

[6] In der US-amerikanischen Kultur ist die Anspielung auf den 1953 erschienenen Roman „Fahrenheit 451" von Ray Bradbury jedermann verständlich. "It was a pleasure to burn" von Guy Montag, der den Auftrag hat, private Bibliotheken zu verbrennen, da Bücher und Bibliotheken in einem totalitären System subversiv sind, gehört zu den bekanntesten und meist zitierten Eingangssätzen der *Science-Fiction*-Literatur.

[7] Ähnlich viele anderen Institutionen aus der amerikanischen Bürgerrechtsbewegung, z.B. *The Censorware Project:* „We at the Censorware Project believe that this type of software [filter, blocking] is the greatest single threat to free speech as we know it on the internet over the next decade. We are committed to exposing the flaws of this misunderstood software and working to encourage alternatives to censorship" (http://censorware.net/about.shtml); *Global Internet Liberty Campaign*: "Originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering and Rating systems have been shown to pose their own significant threats to free expression. When closely scrutinized, these systems should be viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could" (http://www.gilc.org/speech/Ratings/gilc-munich.html); *Internet Free Expression Alliance (IFEA):* "content <filtering> techniques already have been implemented in ways inconsistent with free speech principles, impeding the ability of Internet users to publish and receive constitutionally protected expression" (http://www.ifea.net/). Ähnliche Positionen beziehen Organisationen professioneller Informationsarbeit, z. B. *American Library Association* (ALA)

Berechtigung, sich vor unerwünschten Internet-Inhalten selber schützen zu wollen, nicht bestritten wird. Gemeinsam mit den meisten kommerziellen Vertretern der Informationswirtschaft distanziert sich die amerikanische *Human Rights*-Bewegung von jeder staatlichen Kontrolle von Internet-Inhalten bzw. von Informationsflüssen allgemein. Das hat verschiedentlich zu zunächst unverträglich scheinenden, aber erfolgreichen Koalitionen geführt – mit Blick auf unser Thema, z.B. bei der Abwehr von staatlicher Kryptographie-Kontrolle[8] oder der Kampagne gegen das *Communications Decency Act* von1996[9]. *Free speech principles* müssen nicht inkompatibel mit dem Interesse der Wirtschaft sein, von staatlichen, zumal folgekostenrelevanten Auflagen verschont zu bleiben[10].

Die krass andere Position, die auf der Grundlage z.B. eines autoritären Politikverständnisses (die Politik wisse besser als die Bürger, was für sie gut ist) den Bürger eines Staates den Zugriff zum Internet durch Verwendung von Filter- und Abblock-Verfahren einschränkt, wird offen kaum vertreten, auch wenn Staaten wie Irak, Singapore oder China immer wieder verdächtigt und beschuldigt werden, solche Verfahren anzuwenden[11]. Möglicherweise handeln verschiedene Staaten so, machen ihre Handlungen aber natürlich nicht explizit im Internet öffentlich[12].

In Ermangelung einer offenen Zensurposition verwenden wir als Gegenposition zu den Vertretern eines uneingeschränkt freien Zugriffs auf die Internet-Inhalte die *Self-Regulation*-Bewegung, die, bevorzugt als Initiative der Wirtschaft, durch entsprechende

---

- Resolution on the Use of Filtering Software in Libraries: „the American Library Association affirms that the use of filtering software by libraries to block access to constitutionally protected speech violates the Library Bill of Rights" (http://www.ala.org/alaorg/oif/filt_res.html). Eine Resolution mit dem Titel "Coalition statement against <stealth blocking>" ist von den wichtigsten *Internet civil liberties organizations* unterzeichnet worden (http://www.peacefire.org/stealth/group-statement.5-17-2001.html)

[8] Vgl. dazu [3], 331ff. Kryptographie ist für die Durchsetzung von Filterverfahren bzw. ebenso für die Abwehr von Filterverfahren ein entscheidender Faktor, da ja nicht entschlüsselbare Information auch nicht gefiltert bzw. abgeblockt werden kann..

[9] Dies ist als "The Battle..." (Reno vs. ACLU) in die Internet-Geschichte eingegangen

[10] Ein aktuelles Beispiel ist derzeit der Widerstand der Wirtschaft, federführend vertreten durch den Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (www.bitkom.org), gegen einen Regierungsentwurf (von 7/01), nach dem die Informationswirtschaft die Kosten für eine weitgehende und nach Möglichkeit lückenlose Überwachung des Internet-Verkehrs zum größten Teil selber tragen soll (was im Prinzip schon jetzt durch entsprechende Gesetze, IuKDG bzw. im Telekommunikationsgesetz (TKG, §88), geregelt ist).

[11] Vgl. J. Schauble (Herald Correspondent in Beijing): China tries to weave tighter Web (http://www.smh.com.au/news/0004/24/world/world03.html); M. Pottinger: China enacts Internet crackdown (http://www.zdnet.com/zdnn/stories/news/0%2C4586%2C2636407%2C00.html).

[12] In einer Pressemitteilung von Reporters Sans Frontières vom 9 August 1999 werden 20 Staaten als Internet-Feinde ausgemacht, „because they control access totally or partially, have censored web sites or taken action against users. They are: the countries of Central Asia and the Caucasus (Azerbaijan, Kazakhstan, Kirghizia, Tajikistan, Turkmenistan and Uzbekistan), Belarus, Burma, China, Cuba, Iran, Iraq, Libya, North Korea, Saudi Arabia, Sierra Leone, Sudan, Syria, Tunisia and Vietnam (http://members.tripod.com/luotsong/internet.htm). Darüberhinaus werden insgesamt 45 Staaten ausgemacht, die den Zugriff ihrer Bürger auf das Netz einschränken, vor allem dadurch, dass sie gezwungen sind oder werden, staatlich kontrollierte Internet Provider zu verwenden.

Filter- und Abblockmaßnahmen dafür sorgen will, dass zum einen der Staat sich aus der Regulierung der Internet-Inhalte heraushält, zum andern bei den Nutzern der Angebote der Informationswirtschaft ein vertrauensvolles Klima „sauberer Webnutzung“ erzeugt wird. *Self-Regulation*-Ansätze werden in der Regel auch von der Politik unterstützt, da sie dadurch von der unpopulären Notwendigkeit befreit wird, durch gesetzgeberische Maßnahmen Kontrolle über Internet-Inhalte auszuüben. Man kann dies als delegierte interventionistische oder delegierte liberale Politik bezeichnen, indem Regulierung nicht selber vorgenommen wird, aber Regulierung von Dritten gefordert wird, mit der „Androhung“, es doch selber zu machen, wenn diese Dritten es nicht oder nicht ausreichend oder gegenüber staatlichen Organen nicht kooperativ genug realisieren.

Für die Politik in den USA war „*Self-Regulation*“ nach dem Scheitern des *Communications Decency Act* von 1996/97, durch den die Politik versucht hatte, direkt auf *Internet-Inhalte* Einfluss zu nehmen, offizielle Regierungspolitik. Möglicherweise zeichnet sich aber in der jetzigen Bush- Administration, entgegen der ansonsten bei republikanischer Politik vorherrschenden Liberalisierung, eine stärkere Tendenz zu staatlicher Regulierung ab, wenn es um im Internet zu verteidigenden bzw. anzugreifenden Werte geht, vor allem um die Sicherung von *Privacy* oder auch das Abblocken illegaler und vor allem für Kinder als schädlich angesehene *Internet-Inhalte*[13]. Auch in der EU dominiert mit Blick auf Filter- und Abblock-Politik der Selbst-Regulierungsansatz[14], ebenso in Deutschland, wo sich z.B. die Justizministerin Herta Däubler-Gmelin jüngst positiv zustimmend zu der Filter-Selbstregulierung durch die von Bertelsmann unterstützte ICRA-Filter-/*Rating*-Initiative geäußert hat[15]. Schließlich ist der *Self-Regulation*-Ansatz für Filtern und Blocken auch bei den Basis-Bewegungen im Internet populär, z.B. bei Eltern-Organisationen, Anonymisierungs-, *Anti-Spam*- oder *Web-of-trust*-Bewegungen, zumal dann, wenn sie als Realisierung des Prinzips der informationellen Selbstbestimmung verstanden werden können.

Für dieses von der Politik und großen Teilen der Informationswirtschaft gleichermaßen favorisierte Selbstregulierungsprinzip mag die *Internet Content Rating Association* (ICRA)[16] stehen, eine Vereinigung[17] zur Klassifizierung von Internet-Inhalten mit dem

---

[13] Vgl. Brian Krebs, Newsbytes, White House Urged To Use Internet As Human-Rights Soapbox (9.2.2001), wo darauf hingewiesen, dass das Internet als Mittel zur Demokratisierung (wie zu Zeiten des Kalten Krieges Radio Free Europe und Voice of America) angesehen werden sollte und enormes Potenzial habe „in exporting American values and democratization in many repressive nations that restrict media and the press“ (http://www.newsbytes.com/news/01/161789.html) (vgl. die entsprechende Studie des Lawyers Committee for Human Rights, auf die sich die aktuelle USA-Politik bezieht, unter http://www.lchr.org/home.htm).

[14] Vgl. EU -Action Plan on promoting safer use of the Internet (http://europa.eu.int/ISPO/iap/decision/en_print.html)

[15] http://www.heise.de/newsticker/data/jk-06.04.01-003/

[16] www.icra.org

[17] ICRA wird neben der Bertelsmann-Stiftung u.a. getragen von AOL Europe, British Telecommunications, Cable & Wireless, Demon Internet, EuroISPA, IBM, Internet Watch Foundation, Microsoft, T-Online sowie die Software & Industry Association. Die Entwicklung der Filtersoftware wurde im Rahmen der „Action Plan on promoting safer use of the Internet“ der EU (http://europa.eu.int/ISPO/iap/decision/en_print.html) mit mehreren hunderttausend ECU ebenso wie

wesentlichen Ziel, Kinder vor potenziell schädlichem Material zu schützen, ohne das Recht der Anbieter von Inhalten auf Meinungsfreiheit zu beeinträchtigen. ICRA hat das früher von RSACi aufgestellte Inhaltskennzeichnungssystem übernommen und (über ein internationales Beratergremium) weiterentwickelt, wobei es den Nutzern anheimgestellt wird, neben dem angebotenen, das Ausfiltern und Abblocken leistende Basisvokabular frei wählbare nationale, kulturell divergierende und weltanschaulich geprägte Zusatzfilter zu verwenden. Damit sind wir bei den Anwendungen.

IV. ANWENDUNGEN

Filter- und Abblock-Verfahren sind als Software-Lösungen unabhängig von dem Zweck des Verfahrens; sie können für ordnungs-, sicherheitspolitische, militärische Zwecke genauso eingesetzt werden wie als Mittel der Kontrolle von Eltern über das Netzverhalten ihrer Kinder (*parental control*) oder als Mittel von Unternehmen, ihre Mitarbeiter davon abzuhalten, während der Arbeitszeit in nicht job-relevanten *Websites* zu navigieren. Die Entwickler von WebWasher z.B. weisen explizit unter dem allgemeinen Ziel "Keep Your Web Clean" auf die Vielzahl möglicher Anwender hin – "companies, schools, public-sector agencies and home users"[18] -, die durch die Software in die Lage versetzt werden sollen „to use the Internet more productively, efficiently and confidently". In der Regel legen heutzutage die Anbieter von Filter- und Abblock-Software darauf Wert, dass Nutzer ihrer Produkte selbstbestimmt damit umgehen können - so WebWasher, aber auch das erwähnte, von der Bertelsmann-Stiftung favorisierte ICRA-Verfahren.

Filter- und Abblock-Verfahren werden zunehmend in öffentlich finanzierten Institutionen wie *Bibliotheken und Schulen* (freiwillig oder durch Verordnung, experimentell oder routinemäßig) eingesetzt. Ein neueres Beispiel aus Deutschland ist die Hamburger Pan Amp AG[19], die im Monat Juli 2001 mit Unterstützung des Bayerischen Staatsministeriums für Unterricht und Kultus und im Rahmen der Bundesinitiative "Schulen ans Netz" den 4300 netzangeschlossenen Schulen des Freistaates Bayern die für die Internet-Filterung erforderliche Filter-Technologie für Testzwecke zur Verfügung stellte[20]. Die Begründung: „Durch Internet-Filterung können bestehende Gefahren minimiert und den Schülern ein jugend- und ausbildungsgerechter Zugang zum Internet ermöglicht werden."

---

das Siemens-Ableger Filterprogramm „WebWasher" unterstützt. Ziel dieses *Action Plan* ist es, alle Formen der Selbstregulierung des Internet durch die Informationswirtschaft selber zu unterstützen.

[18] http://www.webwasher.com/en/company/vision.htm

[19] http://www.panamp.de/

[20] Aus der Web-Beschreibung: „Die Internet-Filterung erfolgt durch Negativ-Filter, die Webseiten mit jugendgefährdenden Inhalten sperren und somit politisch extreme, sexistische und gewaltverherrlichende Inhalte für die Schüler unzugänglich machen. Die PAN AMP AG setzt hierfür das Filter Administration System (FAS) ein. Zur Sperrung werden die NotList, einer der umfangreichsten deutschsprachigen Negativ-Filter, CyberNot, einer der größten internationalen Negativ-Filter und eine semantische Keyword-Filterung der PAN AMP AG verwendet." Das *Filter Administration System* (FAS) ist bereits seit Mitte 2000 in allen Bremer Schulen mit Internet-Zugang im Einsatz (http://www.heise.de/newsticker/data/jo-02.07.01-000/).

Unter Namen wie *Internet Access Management* versuchen *Unternehmen*, ihre Mitarbeiter davon abzuhalten, während ihrer Arbeitszeiten sich mit Web-Inhalten zu beschäftigen, die nichts mit der Arbeit zu tun haben und die so von eigentlicher Produktivität abhalten. In Deutschland ist hier vor allem das Produkt WebWasher zu nennen, das innerhalb von Siemens, Paderborn, entwickelt wurde[21].

Software wird ebenfalls zum automatischen Abblocken von Werbeinformation und anderen unerwünschten kommerziellen Informationen eingesetzt. Solche *Ad-Blocking*-Software überprüft in einfachen Versionen auf einem *Proxy-Server*, ob und welche Information von einem bekannten *Ad-Server* z.B. als Werbebanner eingespielt werden soll[22] und weist diese bei entsprechender Einstellung zurück, d.h. transportiert diese nicht zum Client weiter. Fortgeschrittenere Verfahren greifen real in den HTML-Code ein und entfernen so werberelevante Information für den Benutzer. Ähnlich funktioniert *Anti-Spam*- oder *Anti-Cookie-Software*. Beispiele für solche *(Ad-)Blocking-Software* sind JUNKBUSTERS[23] zur Kontrolle jeder Art von kommerzieller Kommunikation, WebFree für Macintosh-Rechner[24], Tumbleweed Messaging Management System (MMSTM)[25] AdSubtract software von interMute[26] oder AtGuard von WRQ, die eine Art persönliche *Firewall* für ihre Kunden installieren[27]. Das sind nur einige wenige Beispiele aus einem offensichtlich wachsenden Markt, der über Stichworte wie *Anti-Spam Software* oder *Anti-Ad Software* etc. erschlossen werden kann. Auch bieten die führenden *Browser*-Hersteller und *Service Provider* direkt oder vermittelt Hilfestellung für solche *Blocking-Assistenz-Software* an.

Wie nicht anders zu erwarten, hat solche *Blocking-Software* wieder Anti-Maßnahmen unter der Frage „Will Banner Blocking Software Kill Internet Marketing?“ provoziert[28], z.B. Initiativen wie des Verlages „Mind's Eye Fiction“. Aus diesem Interesse wird betont, dass durch Bannerwerbung und andere Werbeformen erst das gebührenfreie Angebot an Web-Inhalten möglich wird, so dass *Ad-Blocking-Software* nur vordergründig das Prinzip der informationellen Selbstbestimmung fördere, in Wirklichkeit aber den Umfang und die Freiheit des Informationsangebotes und damit den freien Fluss der Information behindere. Manche Anbieter gehen dabei so weit, Benutzer von *Ad-Blocking-Software* vom Zugang zu ihren Website auszuschließen. Man verwendet also Filter-Software, um die Benutzung von anderer Filtersoftware festzustellen und deren Benutzer dann von der Benutzung abzublocken. Möglicherweise erfolgversprechender ist der Ansatz von *Mind's Eye Fiction*, als Belohnung für den Verzicht auf *Ad-Blocking-Software* die kostenlose Lektüre ihrer Produkte anzubieten[29] - ein Ansatz, der unter dem Stichwort *Banner Rewards Software* auch sonst erprobtes Marketing-Mittel ist.

---

[21] Seit 10/99 als Siemens-Spin-off, webwasher.com AG, selbständig.

[22] Vgl. Bill Dimm: How Ad-Blocking Software Works. April 23, 2001 (http://SaveTheFreeWeb.com/articles/how_blockers_work/)

[23] http://www.junkbusters.com/summary.html

[24] http://www.falken.net/webfree/

[25] http://www.tumbleweed.com/en/solutions/products/mms_products/index.html?source=goto

[26] http://www.adsubtract.com/im/

[27] http://home.pages.at/atguard/Wrq/getstart.htm

[28] http://www.iboost.com/promote/advertising/banner_advertising/articles/00604.htm

[29] Vgl. http://www.internetnews.com/IAR/article/0,,12_157841,00.html

Die klassische Anwendung von Filter- und Abblock-Verfahren zielt auf die Überwachung des Telekommunikationsverkehrs durch staatliche Organe ab. In den letzten Jahren ist einige Transparenz in die Aktivitäten des Echelon-Systems gekommen[30], durch das, 1947 zu Zeiten des Kalten Krieges eingesetzt, weltweit Kommunikation aufgezeichnet und ausgewertet wird[31]. Neben den USA beteiligen sich daran Großbritannien, Kanada, Australien und Neuseeland. Für dieses Abhörsystem ist in den USA die *National Security Agency* (NSA) zuständig. Man geht aus, dass durch Überwachung der Satellitenkommunikation (ob Unterseekabel ebenfalls „angezapft" werden, wird vermutet, ist aber nicht als sicher bekannt) etwa eine Milliarde Nachrichten (weitgehend Emails, Telefonanrufe, Faxe) pro halbe Stunde aufgezeichnet und dann ausgefiltert werden können[32]. Eine öffentliche Kontrolle findet nicht statt. Entsprechend wird Spekulationen über Reichweite und Durchdringungsrate von Echelon Tor und Tür geöffnet. So vermutet man, dass der Schwerpunkt der Echelon-Aktivitäten sich seit geraumer Zeit von der politischen Spionage zur Wirtschaftsspionage verlagert hat (dies wird von der offiziellen USA-Politik bestritten – Daten würden nicht an private Firmen weitergegeben[33]). Ebenfalls wird immer wieder der Verdacht geäußert, dass die Computerindustrie teilweise mit NSA zusammenarbeite und Email-Programme mit entsprechenden NSA-Schlüsseln so präpariere, dass Emails leichter „abhörbar" werden.

Etwas mehr Kontrolle und Transparenz ist bei dem in der Wirkung vergleichbaren *Carnivore-System* gegeben, für das das amerikanische FBI (also die Bundespolizei) zuständig ist und das Aufzeichnungs- und Filtersoftware direkt auf den Servern von Internet-Providern einrichtet, so dass eine umfassende, nicht nur auf einzelne Personen bezogene „Rasterfahndung" durchgeführt werden kann. Für die Überwachung und Auswertung muss eine richterliche Genehmigung vorliegen. In Deutschland wird ebenfalls die Debatte darüber geführt, inwieweit polizeiliche Ermittlungsverfahren stärker überwachend und ausfilternd in die Internet-Kommunikation eingreifen sollen und dürfen. Im Teledienste-Datenschutzgesetz ist es den *Internet Service Providern* (ISP) bislang nur dann gestattet, persönliche Daten aufzuzeichnen, wenn die Zustimmung der Betroffenen vorliegt. Um schnell reagieren zu können, wird erwogen, dass die Polizei, sozusagen vorbeugend und auf Vorrat, den Providern die Order zur Aufzeichnung geben darf, dass aber die spätere filternde Auswertung erst nach richterlichem Beschluss geschehen darf (die Daten sind immerhin dann schon aufgezeichnet und nicht unwiederbringbar verloren).

Insgesamt ist die Rolle der *Internet Service Provider* bezüglich Filtern und Blocken ambivalent. Dass ISP ihren Kunden die Benutzung von Filter- und Abblock-Software anbieten, gehört zum heute nachverlangten Service. Inwieweit ISP selber von sich aus

---

[30] Durch eine Website, die an der George-Washington-Universität gepflegt wird, ist eine umfassende Dokumentation zu Echelon bzw. zur NSA allgemein zugänglich (http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html).

[31] Vgl. D. Campbell (24.07.2000): Inside Echelon. Zur Geschichte, Technik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems (http://www.heise.de/tp/deutsch/special/ech/6928/1.html).

[32] In Deutschland darf der Bundesnachrichtendienst entsprechend einem Urteil des Bundesverfassungsgerichts ebenfalls Kommunikation über Satelliten auswerten.

[33] Vgl. http://w3.zdf.msnbc.de/news/49745.asp

Inhalte abblocken sollen oder dürfen, ist in Deutschland längere Zeit im Zusammenhang des CompuServe-Urteils des Münchener Landgerichts[34] diskutiert worden. Dahinter steht das allgemeine Problem, inwieweit *Provider* verpflichtet sind, rechtswidrige Inhalte selber zu sperren. Die Lösung in der jetzigen Version des TDG (30.6.2000) besteht darin, dass Diensteanbieter natürlich für eigene Inhalte verantwortlich sind (§5, Abs. 1), aber für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann, „wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern“ (§5, Abs. 2). Ansonsten sind sie entsprechend Abs. 3 für fremde Inhalte, die sie zur Nutzung bereithalten, nicht verantwortlich. Diskutiert wird, ob aufgrund der Formulierung in Abs. 4 nicht ein Konflikt zu Art. 5 I 1 GG bzw. Art. 5 I 3 GG (Informationsfreiheit und Zensurverbot) besteht.

In letzter Zeit ist das Verhalten verschiedener ISP, aus vorauseilendem Gehorsam oder aus welchen Gründen auch immer, *Blocking*-Verfahren einzusetzen, ohne ihre Kunden darüber zu informieren, unter der Bezeichnung *stealth blocking* diskutiert bzw. kritisiert worden. *Stealth blocking* ist dadurch definiert, dass den Kunden (oder sogar dem Verkaufs- und technischen Personal) der jeweiligen ISP nicht bewusst wird, dass bestimmte Website abgeblockt werden und ihnen suggeriert wird, dass die angewählte Zieladresse nicht mehr im Netz aktiv sei. Mit einer Resolution von 5/2001 haben sich führende amerikanische Internet-Bürgerrechtsbewegungen, unter dem Dach von *Global Internet Liberty Campaign* (GILC) und *Internet Free Expression Alliance* (IFEA, in einem „Coalition statement against <stealth blocking>“ zusammengefunden, mit der zentralen Aussage: „We believe that ISPs that practice "stealth blocking" are violating consumer protection principles and restricting user choice and freedom in cyberspace“[35].

V. Ambivalenz von Softwarelösungen

Filter- und Abblock-Verfahren sind Software, und Software kann durch andere Software modifiziert (verstärkt, vermindert) oder unterlaufen werden. In der Auseinandersetzung zwischen der *Human Rights*-Bewegung, die prinzipiell jede Inhaltskontrolle im Internet ablehnt, den Selbstregulierungsvertretern, in der Regel aus der Informationswirtschaft, und den politisch motivierten Regulierungsinstitutionen spielt Software eine (mit)entscheidende Rolle. Man kann das sogar so weitgehend interpretieren, wie es Lawrence Lessig [5] tut, dass Software (*Code* bei Lessig) in ihrer Reichweite die Mächtigkeit von gesetzgeberischen Maßnahmen unterläuft oder sogar ersetzt. Das kann, ergänzend zu den Filterverfahren, am Beispiel der Urheberrechts-/Copyright-Kontrolle durch Verfahren des *Digital Rights Management* gezeigt werden. Nicht zuletzt wegen der Effizienz von Software setzen heute, wie erwähnt, die meisten staatlichen oder überstaatlichen Institutionen bevorzugt auf softwaremäßig abgesicherte Selbstregulierungsansätze für Internet-Inhaltskontrolle, zumal gesetzes-/verordnungs-basierte Regulierungen ohnehin durch gravierende Implementierungs-/Durchsetzungsdefizite beeinträchtigt sind oder gar, wie das *Communications Decency Act*, vor höherer Gerichtssprechung oft nicht Bestand haben. Software – so die Kritik und

[34] http://www.beck.de/mmr/Archiv/mmr03_2000/Rechtsprechung/seite171.htm
[35] http://www.peacefire.org/stealth/group-statement.5-17-2001.html

die Befürchtung – löst tendenziell gesetzgeberische Gestaltung und damit tendenziell staatliche Autonomie und Autorität auf, zumal wenn sie wie bislang territorial verortet ist.

Für und wider Filter- und Abblock-Verfahren kann mit ethischen, programmatischen und politischen Argumenten gestritten werden, aber eben auch mit Software. Solange es Filter- und Abblocksoftware gibt, gibt es auch Anti-Filter- und Anti-Abblock-Software. Mit dem Spruch "How to disable your blocking software. It's not a crime to be smarter than your parents" und dem Motto "Open Access for the Net Generation" bietet z. B. *Peacefire* eine gleichnamige Software an, durch die unter Windows (98) weit verbreitete Filter-/Abblocksoftware (SurfWatch, Cyber Patrol, Net Nanny, CYBERsitter, X-Stop, PureSight and Cyber Snoop) einfach umgangen werden kann. *Peacefire* verstehe sich auch als Reaktion auf ein USA-Bundesgesetz, das von öffentlich finanzierten Bibliotheken den Einsatz von wirkungsvoller Filter-Software verlangt, um nicht-gesetzeskonforme Informationen abblocken zu können [7]. Aktuelles und spektakuläres Beispiel (Mitte 2001) für solche Anti-Software mit konstruktiven Eigenlösungen für uneingeschränkte Kommunikation ist die von der Hacker-Gruppe *Cult of the Dead Cow* entwickelte Software *PeekaBooty*, durch die der Zugriff auf *Websites* wieder „freigeräumt" wird, die durch *Rating*-basierte Verfahren an sich abgeblockt werden sollen. Ohne dass bislang Details der Software bekannt sind, kann man davon ausgehen, dass sie als *Open-Source* freigegeben wird, so dass sie im großen Stil in der Internet-Welt der *Human-Rights*- und Hacker-Bewegung weiterentwickelt werden und vermutlich als Anti-Software mächtiger als jede entwickelte Abblock-Software sein wird.

PeekaBooty steht in der Tradition von *Web-of-trust*- und kryptographie-basierten Anonymisierungsverfahren, so dass in verteilten Netzen Navigation und Kommunikation frei möglich wird/bleibt. Auf die zentrale Rolle von Kryptographie dabei wurde schon hingewiesen. Wenn *Internet-Inhalte* so verschlüsselt werden, dass sie auf keinen Fall für unbefugte Dritte entschlüsselt werden können, können diese Inhalte nicht mehr ausgefiltert oder abgeblockt werden, es sei denn von denen, die autorisierte Empfänger der verschlüsselt übertragenen Informationen sind und die der Einsicht in die dann entschlüsselten Informationen Filterverfahren vorschalten können. Diese Position einer durchgängigen Verschlüsselung – darauf weist Brin [6] hin – kann aber im Gegensatz zum Prinzip einer offenen (transparenten) Gesellschaft stehen, in der Informationen nicht in Nutzungs- und Berechtigungszonen eingeteilt werden sollen.

Unentschieden, wie auf Dauer die Auseinandersetzung zwischen *Blocking* und *Anti-Blocking* ausgehen wird. Bislang sieht es so aus, dass es zu jeder Filter- und Abblocksoftware entsprechende Anti-Software geben wird, genauso wie bislang jede Copyright-Sicherungssoftware, also jedes *Digital Rights Management*, eine De-Copyright-Software provoziert hat. Dies ist auf Dauer ein volkswirtschaftlich gesehen unsinniges „Spiel", so dass nach anderen Lösungen für die selbstbestimmte Kontrolle von *Internet-Inhalte*n auf der Grundlage eines gesellschaftlichen Konsenses gefunden werden muss. Schließlich muss auch auf die Ambivalenz im Nutzen und in der Nutzung von Anti-Software hingewiesen werden. Die Hacker-Gruppe *Cult of the Dead Cow* hatte schon früher Software öffentlich gemacht, durch die auf Sicherheitslücken in Microsoft-Betriebssystemen hingewiesen werden sollte. Was allerdings Cracker nicht daran hinderte, eben diese Software zu verwenden, um sich in krimineller Absicht illegalen Zugriff zu *Windows*-Rechnern zu verschaffen. Genau das gleiche kann mit Software wie

PeekaBooty geschehen, durch die kriminelle Akteure sich einen nicht kontrollierbaren Freiraum sichern können.

VI. FAZIT

Vielleicht muss man die Reichweite von Filter- und Abblock-Verfahren nicht überbewerten. Alle bislang durchgeführten Studien (z.B. nachgewiesen in [1], [2], [7], auch im TIFAP-Projekt[36]) weisen klar nach, dass die Leistungen von Filter- und Abblock-Verfahren auf dem gegenwärtigen Stand der Technik (sprachoberflächen-/listenorientiert) unzureichend sind, dass also einerseits zu viel abgeblockt wird – also durchaus harmlose oder nicht-abblockungswürdige Seiten abgeblockt werden – andererseits kaum all das abblocken, was sie abblocken sollten. *Recall* und *Precision* – um die im Information üblichen Bewertungsparameter hier anzuwenden (vgl. die Daten in [1]) – sind bislang unakzeptabel gering. Das ist aber sicher nur ein Zwischenergebnis. Die vor allem im Kontext der staatlichen Überwachung entwickelten themenbasierten und in Zukunft auch wissensbasierten Verfahren werden weitaus mächtiger sein. Semantisch stimmige Überwachung und Abblocken werden methodisch machbar werden, auch wenn zur Zeit die Barriere (oder der Schutzwall) einer durchgängigen, starken Kryptographie als theoretisch unüberwindbar erscheint (faktisch wird Kryptographie aber nur peripher eingesetzt).

Wie können Filter- und Abblock-Verfahren – gesetzt sie sind so effizient, wie sie es heute nur zu sein behaupten – eingeschätzt werden? Offensichtlich ist, dass Verfahren des Filterns und Blockens für sich wertneutral sind, jedoch auf einem meist subjektiven oder interessegeleiteten *Rating* basieren. Sie können gleichermaßen für das positive Ziel der Zustellung nur erwünschter Information und für das negative Ziel der Verhinderung unerwünschter Information eingesetzt werden. Sie können aus polizeilichen Ermittlungs- bzw. nachrichtendienstlichen Interessen ebenso verwendet werden, wie zur Kontrolle des Navigationsverhaltens von Angestellten einer Firma, zur Entlastung von Eltern, die ihren Erziehungsauftrag wegen Überlastung an Software abgeben wollen, zum Schutz vor belästigender Werbeinformation oder sonstiger störender, beleidigender oder verletzender Information, zur zielgerechten, interessenadaptiven Selektion von ansonsten nicht mehr überschaubarer Medieninformation, ...

Filter- und Abblocktechniken wie auch allgemeinere Überwachungstechniken kommen ordnungspolitischen Interessen entgegen und scheinen auch den Moralvorstellungen gegenwärtiger bürgerlicher Gesellschaften zu entsprechen. Ist es durchaus noch unentschieden, inwieweit Staaten der Versuchung erliegen werden, Filter- und Abblock-Verfahren für eine perfektionierte Überwachung einzusetzen, scheint Einvernehmen darüber zu bestehen, dass auf den allgemeinen Informationsmärkten lediglich Formen der Selbstkontrolle bzw. Selbstregulierung konsensfähig sind, sei es durch die Institutionen der Informationswirtschaft, sei es durch Maßnahmen der Ersteller von *Websites* direkt oder sei es durch Institutionen, vor allem aus der Bürgerrechtsbewegung, die damit weitergehenden staatlichen Maßnahmen einen Riegel vorschieben wollen. In Anlehnung an [1] können die folgenden Forderungen an Filter- und Abblock-Verfahren aufgestellt:

[36] http://www.bluehighways.com/tifap/

- Zensur soll grundsätzlich in elektronischen Netzen verboten sein; Meinungsfreiheit darf weder über direkte (gesetzgeberische) noch indirekte (verstärkte Kontrollen) Maßnahmen, sei es von Seiten des Staates oder der Wirtschaft, eingeschränkt werden (Postulat des Zensurverbots bzw. der uneingeschränkten Meinungsfreiheit)
- jede Art diskriminierender Information (z.B. mit Bezug auf Geschlecht, Rasse, Religion, politische Überzeugungen) muss von den Netzen ferngehalten werden (Postulat der Nicht-Diskriminierung)
- die Netzbenutzer selber sind die kompetentesten Beurteiler der Validität und Sozialverträglichkeit von Information (Postulat der Autonomie bzw. Prinzip des aktiven, d.h. selbstbestimmten Blockens)
- Filter- und Abblock-Verfahren dürfen nicht ohne Wissen der Betroffenen eingesetzt werden (passives Blocken ist in der Regel unakzeptabel), d.h. die *Rating*-Basis von Filter- und Abblock-Verfahren muss transparent und individuell definierbar sein (Prinzip der Transparenz)
- die den *Rating*-Verfahren zugrundeliegenden Wertesysteme dürfen nicht auf Länder mit ganz anderen kulturellen Hintergründen übertragen werden (Prinzip der kulturellen Autonomie)
- Filter- und Abblockverfahren sollten nicht fest „verdrahtete“ Bestandteile von Internet-Software, wie Browser oder Suchmaschinen, werden, sondern sollen individuell und kontrolliert eingesetzt werden können (Prinzip der individuellen Kontrolle)
- *Rating*-Verfahren dürfen als Form der Selbsteinschätzung bzw. ersatzweise der Delegation der Einschätzung an Dritte nicht verbindlich werden bzw. dürfen Internet-Browser bzw. Internet-Suchmaschinen *Websites* nicht automatisch abblocken, die sich nicht einem (standardisierten) *Rating*-Verfahren aus welchen Gründen auch immer unterworfen haben (Prinzip der freiwilligen Anwendung)
- (öffentlich finanzierte) Schulen, Universitäten, Bibliotheken, Informationsvermittlungseinrichtungen jeder Art sollten nicht verpflichtet werden, *Rating*- bzw. Filter-/Abblock-Verfahren gegen ihren Willen oder gegen den Willen ihrer Klientel einzusetzen (Prinzip der informationellen Freiheit)

VII. REFERENCES

[1] R. Kuhlen, Ambivalenz von Filter-, Abblock- und *Rating*-Verfahren. In: H. Kubicek et al. (ed.),Telekommunikationsjahrbuch 2000. Global @home. Heidelberg, Hüthig-Verlag, 2000, 371-384

[2] C. D. Hunter, Filtering the future? Software filters, porn, pics, and the Internet content conundrum. Ph.D. dissertation, Faculty of The Annenberg School for Communication, University of Pennsylvania, 1999

[3] EPIC (ed.), Filters and freedom 2.0: Free speech perspectives on Internet content controls. Washington, D.C., Electronic Privacy Information Center, 2001

[4] R. Kuhlen, Die Konsequenzen von Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden? Frankfurt a. Main, Suhrkamp,1999

[5] L. Lessig: Code and other laws of cyberspace. New York, NY, Basic Books (Perseus Books Group), 1999

[6] D. Brin: The transparent society. Will Technology force us to choose between privacy and freedom? Reading, MA, Addison-Wesley, 1998

[7] B. Haselton: Study of Average Error Rates for Censorware Programs (Studie von Peacefire vom 23.10.2000: http://www.peacefire.org/error-rates/)

Rainer Kuhlen born. 01/07/1944; married to Prof. Elizabeth Couper-Kuhlen, 2 children; living in Konstanz, Germany. Study of philosophy, German literature and sociology at the University of Muenster (1964-1969); Assistant professor for philosophy at the University of Muenster (1969-1972); Postgraduate training in information science at the Center for Machine Documentation (ZMD) in Frankfurt (1972-1974); Lecturer at the Teaching Institute for Documentation in Frankfurt (1974-1979); PhD 1976 at the University of Regensburg; since 1980 Professor for Information Science at the University of Constance

Co-editor of the following journals: Journal of Information science, Nachrichten fuer Dokumentation, Information Processing & Management, Library Management; Chief editor of the book series Schriften zur Informationswissenschaft (currently more than 30 vols.); Member of the Board of the Hochschulverband Informationswissenschaft (German Society of Information Science – HI); Director of the Steinbeis Transfer Center for Information/Electronic Markets and Information Engineering (IMIE) at the University of Constance; Member of the German Commission for UNESCO, Chairperson of the German UNESCO Committee for Communications, Informatics and Information; German UNESCO Chair in Communications (ORBICOM); Director of NETHICS e.V. (Information Ethics in the Net); Member of numerous advisory boards for institutions in Information Politics and Information Economy.

Numerous publications (books and articles) in the fields of information retrieval, computational linguistics, information science theory, text condensation, hypertext, information/electronic markets, information ethics, electronic communication forums. Numerous projects (mainly third-party-financed – BMFT/BMBF, DFG, EU and partially through joint projects with industrial partners) have been carried out since 1980 in the fields of information retrieval, text condensation/automatic abstracting/automatic indexing, knowledge representation and management, visualization of knowledge structures, hypertext/-media, information/electronic markets, quality management, information ethics, media assistants, electronic communication forums.