Future of Privacy

Zukunft von Netz und Gesellschaft

Ralf Bendrath*

"Die Zukunft ist bereits da,
sie ist nur noch nicht gleichmäßig verteilt."
William Gibson

"Der beste Weg, die Zukunft vorherzusagen,
ist, sie zu erfinden."
Alan Kay

Ich bin gebeten worden, in die Zukunft des Datenschutzes zu schauen. Leider verfüge ich nicht über prophetische Fähigkeiten, und die technischen Hilfsmittel dazu, wie etwa eine Kristallkugel, habe ich auch nicht. Was also tun?

1. Experten fragen

Ein erster Schritt wäre, nachzuschauen, was denn andere zur Zukunft der Privatsphäre sagen. Die Delphi-Methode der Expertenbefragung ist ja ein gängiges Mittel der Futurologie, vor allem um Szenarien zu erhalten und mögliche Zukünfte von unwahrscheinlichen abzugrenzen. Recht verbreitet scheint hier auf den ersten

* Ralf Bendrath, Dipl.Pol., ist wissenschaftlicher Mitarbeiter am Sonderforschungsbereich "Staatlichkeit im Wandel" der Universität Bremen. Er ist außerdem aktiv im Arbeitskreis Vorratsdatenspeicherung und verschiedenen anderen Datenschutz-Zusammenhängen und ist "hard bloggin' scientist" bei bendrath.blogspot.com und www.netzpolitik.org.

Blick die Ansicht, dass die Privatsphäre ohnehin verloren sei. Bereits 1999, also lange vor dem Web 2.0, wurde Scott McNealy, der damalige Chef von Sun Microsystems, bekannt mit dem Zitat: "You have zero privacy anyway. Get over it".[1] Er hat diese Ansicht mittlerweile überdenken müssen und sie öffentlich zurückgezogen, als ein Laptop von Sun gestohlen wurde, auf dem Mitarbeiterdaten lagen – unter anderem auch die von McNealy selber.[2] Aber die These vom Ende der Privatheit steht weiterhin im Raum. Die Ars Electronica 2007 in Linz hatte den Titel "Goodbye Privacy", und die Kuratoren feierten dies sogar mit dem Slogan "welcome publicity!"[3]

Andere sind optimistischer. Sie glauben nicht nur zu wissen, dass der Schutz der Privatsphäre eine Zukunft hat, sondern auch, welche neuen Instrumente sich dafür durchsetzen werden. Der Datenschutzbeauftragte von Schleswig-Holstein, Thilo Weichert, sagte etwa auf der Jahrestagung 2007 der Deutschen Vereinigung für Datenschutz voraus: "2008 wird ein Auditjahr."[4] Hier ist allerdings oft auch der Wunsch Vater des Gedankens, und manche Prophezeiung wird in der Hoffnung geäußert, dass sie sich damit auch erfüllen möge. Das Unabhängige Landeszentrum für Datenschutz (ULD) in Kiel hat sich in den letzten Jahren als Vorreiter von Datenschutz-Audits einen Namen gemacht und arbeitet derzeit daran, dieses Instrument europaweit zu etablieren.[5] Insofern stimmt die Prognose auf jeden Fall für Thilo Weichert und seine Mitarbeiter.

Aus Kiel kamen aber bereits andere wertvolle Hinweise auf die Zukunft des Datenschutzes. Das ULD hat bereits 2004 seine Sommerakademie unter das Thema gestellt "Der Datenschutz der Zukunft". Wiederum fragt sich der geneigte Leser, wie sie denn nun aussehen soll, diese Zukunft. Interessant war daher der Untertitel

---

[1] Polly Sprenger: Sun on Privacy: 'Get Over It', in: Wired News, 26.01.1999, http://www.wired.com/politics/law/news/1999/01/17538.

[2] Ashlee Vance: Ernst & Young fails to disclose high-profile data loss. Sun CEO's social security number exposed, in: The Register, 25.02.2006, http://www.theregister.co.uk/2006/02/25/ernst_young_mcnealy.

[3] Armin Medosch / Ina Zwerger: Goodbye Privacy! Welcome Publicity? in: Gerfried Stocker / Christine Schöpf (Hrsg.): Goodbye Privacy. Ars Electronica 2007, Ostfildern: Hatje Cantz, 2007, 21-25.

[4] Detlef Borchers: Bielefelder Impressionen von Daten- und Menschenschutz, in: heise News, 14.10.2007, http://www.heise.de/newsticker/meldung/97345.

[5] European Privacy Seal, http://www.european-privacy-seal.eu.

der Veranstaltung: "realisiert mit Identitätsmanagern!"[6] In der Tat ist das Verwalten der eigenen Online-Identität ein immer wichtiger werdendes Feld. Unter anderem zeigt sich dies daran, dass die Debatte um die "nutzer-zentrierte Identität" mittlerweile zum Kern konzeptioneller Überlegungen rund um das Web 2.0 geworden ist. Microsofts "Infocards"-Konzept für Internet-Ausweise und der URL-basierte Standard "OpenID" erlauben es immer mehr Netizens, ihre Online-Identitäten konsistent über viele Seiten hinweg zu verwalten. Damit soll perspektivisch eine bessere Durchsetzung des Rechts auf informationelle Selbstbestimmung möglich werden, so die Protagonisten dieser Technologien. Was kommt also im Bereich digitales Identitätsmanagement auf uns zu?

Die Identity Futures Working Group hat vor kurzem einen Workshop veranstaltet, um Szenarien für das ID-Management zu erarbeiten. Die Ergebnisse sind allerdings nicht so positiv, wie es sich die Kollegen aus Kiel vorstellen. Hier nur zwei Beispiele:

> *Um 2014 ist in den USA, Europa und China anonymer Netzzugang verboten. WLAN-Hotspots müssen die Nutzer authentifizieren, und sie verlassen sich dafür auf T-Mobile, AT&T, et cetera. WLAN ist nicht mehr "frei".*
>
> *"Um 2011 ist die Anonymität in öffentlichen Räumen wie Cafes zerstört durch billige und zuverlässige Gesichtserkennungs-Tools. Jeder mit Laptop, Kamera und Internet-Zugang kann dann fast alle Gäste identifizieren."* [7]

Das Beispiel Identitätsmanagement zeigt also schon im Kleinen, was für den Datenschutz auch generell gilt: Bislang gibt es unter den Experten keine eindeutige Prognose, sondern nur widersprüchliche Szenarien.

---

[6] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Sommerakademie 2004: Der Datenschutz der Zukunft - Informationelle Selbstbestimmung durch Identitätsmanagement, Pressemitteilung, 30.08.2004, https://www.datenschutzzentrum.de/material/themen/presse/20040830-sommerakademie.htm.

[7] Identity Futures Working Group: Identity Futures, 2007, http://wiki.idcommons.net/index.php/Identity_Futures.

2. Trendanalysen

Wenn die Szenarien also nicht weiter helfen, könnte man auf die Trendforschung zurückgreifen. Man könnte also einige Tendenzen aufzählen, die alle mehr oder weniger bekannt sind. Technisch scheint die Entwicklung klar zu sein. Moore's Law, nach dem sich die Zahl der Transistoren in einem Schaltkreis alle zwei Jahre verdoppelt, kennt heute jeder. Ein ähnliches Gesetz gilt auch für Speicherbausteine und Festplatten. Die Zahl der Internetanschlüsse steigt ebenfalls, in vielen Gebieten der Welt wird sie bald 100% pro Kopf der Bevölkerung betragen. Gleichzeitig steigt die Zahl der Überwachungsmaßnahmen in ähnlichem Maße an. Gab es 1998 in Deutschland noch knapp über 10.000 durch die Strafverfolger abgehörte Telefonanschlüsse, so waren es im Jahr 2006 bereits mehr als 40.000.[8]

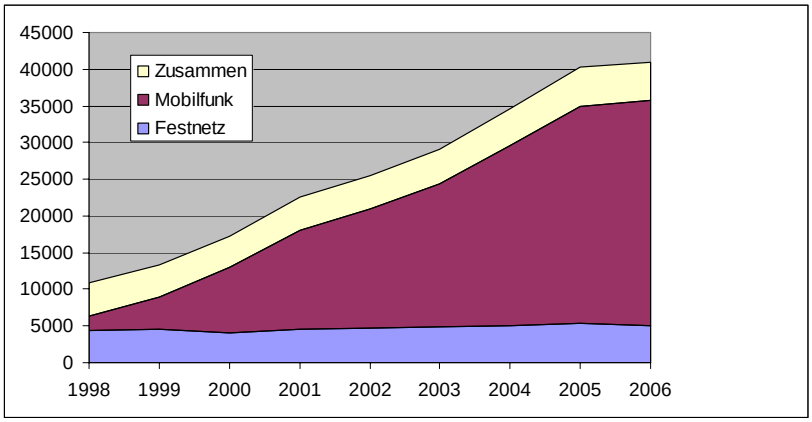

Abbildung 1: Abgehörte Rufnummern in Deutschland, 1998-2006
Quelle: Bundesnetzagentur, Grafik: LDI NRW

[8] Stefan Krempl: Telekommunikationsüberwachung steigt weiter stark an, in: heise News, 27.04.2006, http://www.heise.de/newsticker/meldung/72439.

In den USA verlangt der Geheimdienstkoordinator Michael McConnell bereits offen, alle E-Mails, Dateiübertragungen oder Web-Suchanfragen auswerten zu dürfen.[9] Diese Forderung kam schon auf den Markt, bevor der Kongress sich mit dem Präsidenten darüber geeinigt hatte, ob die Telekommunikationsanbieter nachträgliche Immunität für ihre Mithilfe beim bisher illegalen flächendeckenden Telefonabhören erhalten sollten - eine Veranstaltung, die eines Rechtsstaates eigentlich nicht würdig ist. Auch in der Europäischen Union werden demnächst alle Verbindungsdaten von Telefon, Internetzugang und E-Mail verdachtsunabhängig auf Vorrat gespeichert, sofern nicht das Bundesverfassungsgericht oder der Europäische Gerichtshof dem noch Einhalt gebieten.[10] Sind wir also auf dem geraden Weg in den von massiver Rechenpower und Speicherkapazität und schrumpfenden rechtlichen Schutzmechanismen ermöglichten Überwachungsstaat?

Es gibt aber auch gegenläufige Tendenzen. Das Datenschutzrecht breiten sich kontinuierlich auf dem Globus aus. Seit dem ersten Datenschutzgesetz der Welt, das 1971 in Hessen verabschiedet wurde, gab es eine fast lineare Vermehrung dieser Regulierung in aller Welt.

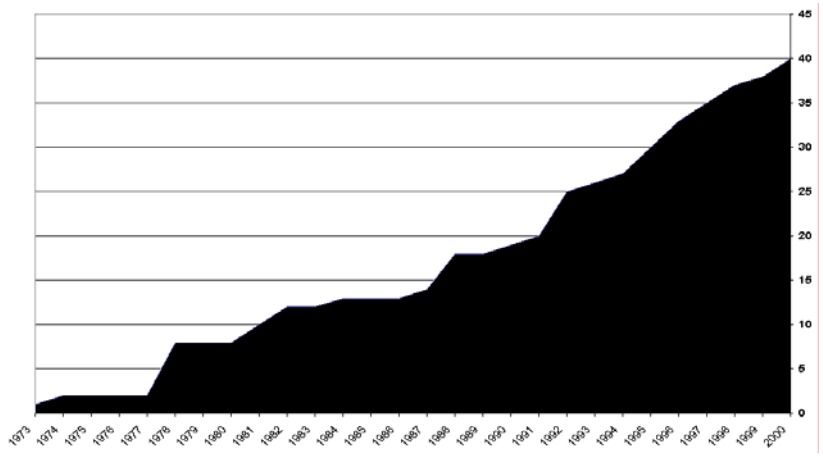

Abbildung 2: Staaten mit Datenschutzgesetzen 1973-2000
Quelle: Colin J. Bennett / Charles D. Raab: The Governance of Privacy, Aldershot: Ashgate, 2003; eigene Darstellung

[9] Lawrence Wright: The Spymaster, in: The New Yorker, 21.01.2008, http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright
[10] Ausführliche Informationen: http://www.vorratsdatenspeicherung.de.

Heute verfügen mehr als 40 Staaten über Datenschutzgesetze; dazu kommen eine Anzahl internationaler Regelungen, Standards und *Codes of Conduct*.

Auch der politische Widerstand gegen die Überwachung wächst in letzter Zeit wieder rapide. Digitale Bürgerrechtsgruppen wie der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. (FoeBuD), der Chaos Computer Club e. V. (CCC) oder der europäische Dachverband European Digital Rights (EDRi) verzeichnen seit Jahren kontinuierliche Mitgliederzuwächse. In Deutschland am dynamischsten ist derzeit der Arbeitskreis Vorratsdatenspeicherung, der Ende 2005 mit einer Handvoll Aktivisten gestartet ist und mittlerweile über mehr als 1600 Mitglieder sowie an die 60 Ortsgruppen hat. Er hat auch das Thema Datenschutz und Privatsphäre erstmals seit 20 Jahren wieder auf die Straße gebracht. Der Höhepunkt war bislang die Demonstration "Freiheit statt Angst - Stoppt den Überwachungswahn" im September 2007 in Berlin, die 15.000 Teilnehmer mobilisieren konnte. Auch das Demonstrationsbündnis zeigt, wie breit das Thema wieder im politischen Spektrum verankert ist: Neben klassischen Datenschutzverbänden demonstrierten Ärzteverbände, kirchliche Seelsorger, Journalisten, Handwerker, Autonome und Liberale sowie die gesamte in Parteien organisierte Opposition.

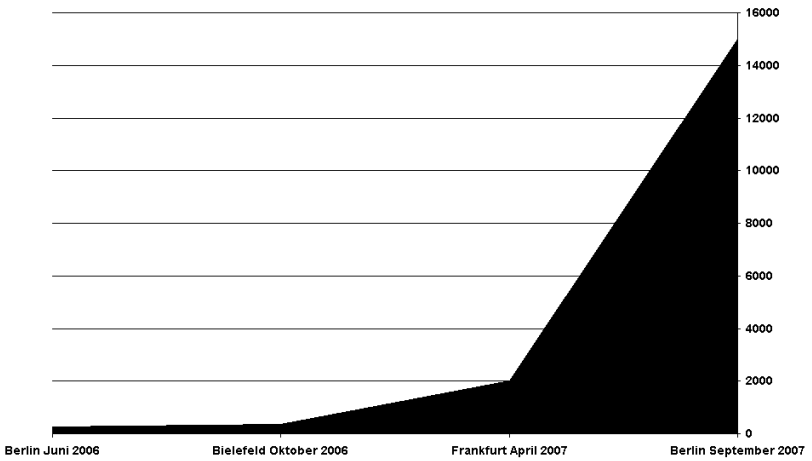

Abbildung 3: Demonstrationsteilnehmer "Freiheit statt Angst - Stoppt den Überwachungswahn"
Quelle: Veranstalter (AK Vorratsdatenspeicherung); eigene Darstellung

Mehr Überwachung, mehr Datenschutzgesetze, mehr politische Mobilisierung für die Privatsphäre, und das auch noch alles gleichzeitig - auch anhand der Trendanalysen ist also keine eindeutige Tendenz zu erkennen. Interessant ist aber schon die Erkenntnis, dass es widersprechende Bewegungen und Kräfte gibt. Auch im Bereich Überwachung und Datenschutz sind die Verhältnisse nicht linear, sondern dialektisch. Und die Widersprüche haben sich offenbar in letzter Zeit zugespitzt.

3. Qualitative Sprünge

Was heißt das nun? Das Entscheidende sind meines Erachtens nicht quantitative Entwicklungen, sondern qualitative Sprünge. Ohne eine Einschätzung solcher Sprünge, ohne das Gefühl dafür, wann Quantität in Qualität umschlägt, verstehen wir die Veränderungen nämlich nicht. Und die Veränderungen haben oft mit qualitativen Sprüngen in der Technologie zu tun.

Um das zu illustrieren, erlauben Sie mir einen Blick in die Vergangenheit. Im Jahr 1890 erschien im Harvard Law Review ein Artikel unter dem Titel "The Right to Privacy".[11] Er gilt bis heute als juristischer Gründungsakt für den Schutz der Privatsphäre. Geschrieben haben ihn zwei angesehene Juristen aus Boston, der Anwalt Samuel Warren und der spätere Verfassungsrichter Louis Brandeis. Wie kamen sie dazu, diesen Artikel zu schreiben? Den Anstoß gaben zwei technische Entwicklungen.

Kurz zuvor hatte die Eastman Dry Plate Company unter dem Produktnamen "Kodak" die ersten Handkameras mit Rollenfilm auf den Markt gebracht. Während Kameras vorher umständlich aufgebaut werden mussten, eine lange Belichtungszeit hatten und man nach jedem Foto die Filmplatte wechseln musste, erlaubten diese neuen Geräte erstmals so etwas wie Schnappschüsse. Das wiederum führte zu einem Problem für die gesellschaftliche Elite, zu der Warren und Brandeis damals in Boston gehörten. Findige Reporter schossen mit diesen Kameras nämlich heimlich Fotos von den Partys der Upperclass.

Die andere Entwicklung war die Entstehung der modernen Tageszeitungen. 1812 war die Schnellpresse erfunden worden, 1845 die

[11] Louis Brandeis / Samuel Warren: The Right to Privacy, in: Harvard Law Review 4 (1890), 193-220.

Rotationsmaschine, und 1884 kam die Linotype-Setzmaschine auf den Markt. Anzahl und Auflagenstärke der Tageszeitungen stiegen daher gegen Ende des 19. Jahrhunderts rasant an. Dieses neue Massenmedium sorgte für die schnelle und großflächige Verbreitung von Informationen - und auch von Fotos. Also erschienen die Fotos von den privaten Feiern der High Society, zu der auch Brandeis und Warren gehörten, in den Zeitungen in Boston.

Das hatte zwei Effekte: Aus den Mitgliedern der abgeschotteten gesellschaftlichen Elite wurden damit erstmals, wie man heute sagen würde, "Promis". Zum anderen waren Warren und Brandeis gar nicht erfreut über diese Entwicklung, und als Reaktion entwickelten sie die bereits erwähnte juristische Fundierung von Privatheit und Privatsphäre, die die berühmte Formel enthält vom "right to be let alone".[12]

Dieser kurze Blick zurück auf die Ursprünge des Rechtes auf Privatheit zeigt bereits zweierlei: Erstens: Privatheit und Technologie waren schon immer eng verwoben, nicht erst seit der Erfindung von Computern und Datennetzen. Zweitens: Schon die 1890 verwendeten Geräte illustrieren sehr treffend den Kern der technischen Bedrohungen für die Privatsphäre. Die Kamera steht für die Mittel des Beobachtens und Aufzeichnens, während die Druckerpresse die Mittel des Transports, der Verbreitung und der Veröffentlichung symbolisiert.

Wie sieht es heute aus, mehr als einhundert Jahre später, mit Computern, Internet und einer Durchdringung von Alltag und Berufsleben mit Informationstechnologie? Man könnte sagen, dass die Eastman-Kodak-Kamera von Handy-Kameras abgelöst wurde, während die Druckerpresse ihre Rolle an das Internet und Dienste wie Flickr und YouTube abgeben musste. Die Mittel des Aufzeichnens und Überwachens sind ebenso moderner geworden wie die Mittel der Verbreitung, aber im Kern gibt es nichts Neues. Oder?

Es ist eine Technologie dazu gekommen, die Warren und Brandeis noch nicht vorhersehen konnten: Der Computer als symbolverarbeitende Maschine, die automatisch Entscheidungen fällen kann. Er ermöglicht neben dem Aufzeichnen und dem Verbreiten nun auch das automatische Sortieren von Informationen. Da so auch Daten über Personen sortiert werden können, und damit reale Personen

[12] William L. Prosser: Privacy, in: California Law Review 48:3 (1960), 383-423.

von vom Computer gefällten Entscheidungen betroffen sind, besteht die Gefahr der "digitalen Diskriminierung", wie David Lyon es ausgedrückt hat.[13]

Auf dieser Basis und als Reaktion darauf sind eigentlich alle Datenschutzgesetze entstanden. Sie sollten vermeiden, dass Menschen von Daten, die in Maschinen über sie gespeichert sind, kontrolliert, sortiert und diskriminiert werden. Die EU-Datenschutzrichtlinie von 1995 als letzter großer Akt dieser Tradition kam gerade zu früh, um einen weiteren qualitativen Sprung aufgreifen zu können.

4. Das Internet

Eine viel debattierte Frage ist, ob diese Datenschutzregelungen noch zukunftstauglich sind, ob sie also den qualitativen Sprung, der mit dem Internet verbunden ist, richtig erfassen können. Das Internet hat ja vor allem dazu beigetragen, dass die Daten über uns nun nicht mehr nur bei Versandhausbestellungen, Steuererklärungen oder Arztbesuchen anfallen. Weil wir uns als Internetnutzer in einem sozialen Interaktionsraum bewegen, der vollständig auf Code basiert, finden *alle* unsere Aktivitäten hier in Computern und in dem virtuellen Raum der Datenleitungen statt. Das muss nicht die Dystopie der Science-Fiction-Filme á la "Matrix" bedeuten, sondern bringt auch unglaubliche Freiheiten und neue Möglichkeiten, sich auszudrücken, zu experimentieren und zu kommunizieren - Second Life ist hierfür nur ein bekanntes Beispiel. Was aber bleibt, ist die Tatsache, dass alles durch Computer und in Computern geschieht und damit von Computern gespeichert und von Computern ausgewertet werden kann. Es kann dadurch aber auch manipuliert und kontrolliert werden, was wir im Internet tun können und was nicht. Lawrence Lessig hat darauf in seinem Buch "Code and other Laws of Cyberspace" eindrücklich hingewiesen.[14]

Ich sage bewusst: Es *kann*. Vorratsdatenspeicherung, Internet-Filter, das Sperren von Ports, die überwiegend von Tauschbörsen benutzt werden - all dies kommt natürlich vor. Es ist aber nicht zwangsläufig so, sondern immer das Ergebnis von politischen Aus-

[13] David Lyon (Hrsg.): Surveillance as Social Sorting. Privacy, Risk, and Digital Discrimination, London / New York: Routledge, 2003.

[14] Lawrence Lessig: Code and other Laws of Cyberspace, New York: Basic Books, 1999.

einandersetzungen, ökonomischen Interessen, gesellschaftlichen Normen und kulturellen Praktiken.

Sie merken schon: Ich drücke mich bisher davor, etwas über die Zukunft des Privaten auszusagen. Ich will es nun doch noch wagen, indem ich auf *einen* speziellen qualitativen Sprung hinweise, der mit dem Internet verbunden ist, sich aber erst in den letzten Jahren deutlich herauskristallisiert hat.

5. Die Zukunft ist schon da?

Ich behaupte, dass die Zukunft zugespitzt so aussehen wird wie die Spezies der "Borg" in der Science-Fiction-Serie "Star Trek". Die Borg sind dort bedrohliche Mensch-Machine-Wesen, die in riesigen würfelförmigen Raumschiffen durchs All fliegen und eigentlich nur darauf aus sind, andere Planeten zu erobern, um sich deren Lebensformen und vor allem Technologien anzueignen. Ich will zeigen, dass diese Zukunft schon da ist. Warum? Aus zwei Gründen.

Erstens, weil die Verschmelzung von Mensch und Maschine immer enger wird. Wir tragen heute bereits fast alle ein Handy mit uns herum, dazu kommen computergesteuerte Hörgeräte und Prothesen, Autos nehmen uns Entscheidungen beim Einparken und bald auch beim Fahren ab, und dass unsere Festplatte heute ein intimerer Bereich ist als unser Schlafzimmer ist in der Debatte um die Online-Durchsuchung[15] deutlich geworden. Andreas Pfitzmann hat bei der diesbezüglichen Anhörung des Bundesverfassungsgerichtes in Karlsruhe im Oktober 2007 das überzeugende Argument gebracht, dass unsere Laptops und Festplatten uns immer mehr Gehirnfunktionen abnehmen und damit ein Teil des erweiterten Körpers und Nervensystems sind.[16] Natürlich werden wir friedlicher sein als die Borg. Vor allem werden wir auch nicht aussehen wie sie, weil die Technologien heute zum Teil schon viel kleiner sind, als es sich die Macher der Fernsehserie in den achtziger Jahren haben vorstellen können. Steve Mann, der "erste Cyborg", der ständig einen Computer mit sich herumtrug und seine Umgebung

[15] Dies hat sich auch in der inzwischen getroffenen Entscheidung des Bundesverfassungsgerichts manifestiert, BVerfG 1 BvR 370/07 vom 27.02.2008, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

[16] Der "Sprechzettel" findet sich unter http://dud.inf.tu-dresden.de/literatur/BVG2007-10-10.pdf.

aufzeichnete, fiel früher als Freak sofort auf. Heute sieht man seine Elektronik gar nicht mehr, weil die Kamera in die Sonnenbrille eingebaut ist und der Computer in Form von PDA oder Smartphone mittlerweile ein Massenprodukt ist.

Abbildung 4: Steve Mann und seine tragbaren Computer
Quelle: http://wearcam.org/pictures.html

Der *zweite* Grund, warum wir den Borg immer ähnlicher werden, folgt aus den sozialen Nutzungen dieser Mensch-Maschine-Kopplung. Weil Computer heute nicht mehr als Stand-Alone-Systeme fungieren, sondern als Teil von Netzwerken ausgelegt sind, können wir sie eben auch dazu nutzen, um ständig mit anderen in Kontakt zu bleiben. Und genau das macht bei Star Trek die Borg als Gesellschaftsmodell aus: Jede Drohne ist ständig im Kontakt mit den anderen, hört deren Gedanken und weiß, was sie tun. Das ist wiederum auch keine Science-Fiction mehr. Ähnliche Phänomene kennen wir von Jugendlichen mit der quasi ständigen Ko-Präsenz der Clique durch SMS. Man weiß, was die anderen machen, auch wenn sie räumlich weit weg sein mögen. Im Internet hat diese Funktion in letzter Zeit Twitter übernommen, ein Web 2.0-Dienst, mit dem man ständig über seine Webseite oder seinen RSS-Feed mitteilt, was man gerade tut. Mit Twitter macht man dies allerdings komplett öffentlich. Eine privatere Variante ist Chat und Instant Messaging. Auch hier ist nicht nur das Verschicken von Nachrichten selber wichtig, sondern auch die Information darüber, wer aus dem sozialen Umfeld gerade online ist, wer über seinen Status angibt, dass er Zeit zum Chatten hat und wer auf "busy"

geschaltet ist. Nicht vernetzt sein ist auf jeden Fall "out". Wer sich zum Beispiel beim Social-Networking-Dienst "studiVZ" anmeldet, dann aber das Vernetzen versäumt, erhält bei jedem Einloggen die unschöne Meldung "Du hast keine Freunde". Das klingt nun gar nicht erstrebenswert.

Interessanterweise sind die Borg als Gesellschaft nicht-hierarchisch strukturiert. Auch hier sind sie ein Modell für die kommende Netz-Gesellschaft. Auch im professionellen Bereich deutet sich ja seit einiger Zeit ein Ende des "organizational man" an, der durch feste hierarchische Institutionen wie Firma, Familie, Kirche und Verein geprägt wurde und in ihnen seine Identität erhielt und fixierte. Das neue Paradigma kann als "vernetzter Individualismus" bezeichnet werden: Ein ständiges Arbeiten an der eigenen Identität, wobei die Selbstdarstellung eine Rolle spielt, aber auch die relationale Positionierung in unterschiedlichen sozialen Kontexten.[17] Bei diesen sozialen Nutzungsformen der technischen Vernetzung ist es kein Zwang durch staatliche Behörden oder mächtige Konzerne, der die Leute dazu bringt, ihr Innerstes nach außen zu kehren und anderen mitzuteilen. Sie machen das freiwillig. Sie wollen sich präsentieren. Sie wollen in Kontakt bleiben. Der Mensch ist eben ein soziales Wesen.

Zum Glück unterscheiden wir uns aber auch von den Borg. Während diese als aggressive Raumfahrer-Spezies mit dem einzigen Ziel, andere Kulturen zu assimilieren, zur Homogenität neigen, haben wir die Freiheit, unsere Sozialbeziehungen und deren technisches Management zum großen Teil selber zu wählen. Die Vielfalt dieser Angebote für das internetgestützte Identitäts- und Beziehungsmanagement ist ja mittlerweile immens.

Das Interessante und Gute bei vielen dieser Vernetzungsdienste ist, dass nur genehmigte Kontakte der Empfängerkreis für verschickte Nachrichten sind. In diesen Plattformen bilden wir also bewusst abgegrenzte Teilöffentlichkeiten - oder sollte man besser sagen: private Runden? Auch SMS stehen in dieser Grauzone zwischen ganz öffentlich und ganz privat.

Eine Klarstellung ist an dieser Stelle angebracht, da meine Ausführungen unter Umständen bisher den Eindruck hinterlassen haben, ich würde einer technikdeterministischen Lesart der Geschichte

[17] Vgl. Manuel Castells: Die Internet-Galaxie: Internet, Wirtschaft und Gesellschaft, Wiesbaden: VS Verlag, 2005.

anhängen. Das ist keineswegs so. Im gesellschaftlichen Prozess des Aushandelns und Praktizierens der Grenzlinie zwischen "öffentlich" und "privat" ist viel Varianz möglich und auch vorhanden, sowohl über Raum als auch über Zeit. Zeitungen in anderen Ländern als den USA sind etwa bis heute viel zurückhaltender in der Berichterstattung über das Privatleben von Personen des öffentlichen Lebens als es die Bostoner Zeitungen Ende des 19. Jahrhunderts waren. Die staatliche Überwachung wird in Deutschland regelmäßig vom Verfassungsgericht gestoppt, während es in anderen Teilen der Welt keine solchen Grenzen gibt. Social-Networking Plattformen wie Facebook, Xing oder studiVZ haben völlig unterschiedliche Datenschutz-Richtlinien, obwohl sie im Wesentlichen die gleichen Angebote machen. Hier sieht man ja auch bereits, wie es einen Trend zu mehr Datenschutz gibt. StudiVZ hat am Anfang ordentlich öffentliche Prügel aus der Blogosphäre und dann auch den Massenmedien bezogen, unter anderem wegen Datenlecks und Stalker-Gruppen. Inzwischen bemüht sich der Dienst, wie man hört, um ein Datenschutz-Audit.

6. Die Zukunft gestalten

Bei Prognosen über die Zukunft stehen wir immer vor der Herausforderung, qualitative Sprünge in komplexen dynamischen Systemen frühzeitig zu erkennen. Und das globale Zusammenspiel von Technologie, Wirtschaft, Staat, Gesellschaft und Kultur ist sicherlich ein komplexes dynamisches System. Was heißt das für unser Verständnis von Privatheit, Öffentlichkeit, Überwachung? Meine These ist, dass ganz viele dieser Entwicklungen noch offen sind. Wir können sie beeinflussen, indem wir Visionen entwerfen und diese in handlungsleitenden Modellen spezifizieren. Dazu brauchen wir aber Theorien, die uns erklären, was hier vor sich geht, und für Theorien braucht es zuallererst die richtigen Begriffe, die uns beim Begreifen helfen. Meine weitere These ist an dieser Stelle, dass unsere alten Begriffe nicht mehr passen, um adäquat auf diese neuen Entwicklungen zu antworten.

Was meinen wir denn mit "Privatheit" oder "Privacy"? Hier zeigt sich ja schon anhand der verschiedenen Begriffe und Formeln, die im Laufe der Zeit dafür geprägt wurden, dass es keine einheitliche Definition gibt: "the right to be let alone", "fair information practises", "Datenschutz", "informationelle Selbstbestimmung", "Vertraulichkeit", und so weiter.

Gemeinsam war diesen Begriffen und Verständnissen, dass Privatheit bislang immer als das Gute, als Gegenmodell zur Veröffentlichung und damit Observierbarkeit, gedacht wurde.

	Belohnung	**Strafe**
Privat	**X**	
Öffentlich		**X**

Abbildung 5: Das "klassische" Modell von Privatheit[18]

Im Kern war Privatheit aber auch immer negativ definiert, als Gegenbegriff zu "Überwachung". Leider ist auch das Überwachungsmodell unscharf geworden. Das Benthamsche Panoptikum mit dem allwissenden Big Brother im Zentrum und den vereinzelten, quasi monadischen Objekten der Kontrolle an den Rändern trifft heute nicht mehr zu. Daniel Solove hat bereits vor einiger Zeit die Debatte angestoßen, ob statt Bentham und Orwell nicht eher Kafka der paradigmatische Autor der Überwachung ist: Nicht ein alles kontrollierender Akteur, sondern eine unkontrollierbare, unverantwortliche und nicht mehr verstehbare Maschinerie steht dem Individuum gegenüber - heute nicht mehr wie bei Kafka als Bürokratie, sondern als Computeralgorithmen gedacht.[19] Das Modell ist hilfreich, um Flugverbotslisten, Kredit-Ratings und andere in Technik gegossene Mechanismen gesellschaftlichen Sortierens und Diskriminierens zu verstehen. Aber es erfasst die angesprochenen Mechanismen des sozialen Vernetzens und der freiwilligen, begrenzten Veröffentlichung nicht. Ich meine, dass uns spätestens mit dem Web 2.0 klar geworden sein sollte, dass Privatheit nicht immer gut und Veröffentlichung nicht immer schlecht ist.

[18] Die Idee für diese Matrix stammt von Ralf Klamma.
[19] Daniel Solove: The Digital Person. Technology and Privacy in the Information Age, New York: NYU Press, 2004

	Belohnung	Strafe
Privat	**Ruhe**	**Einsamkeit**
Öffentlich	**Aufmerksamkeit**	**Pranger**

Abbildung 6: Das "Web 2.0"-Modell von Privatheit

Wie ich bereits angemerkt habe, ist allerdings auch die Grenze zwischen "öffentlich" und "privat" nicht mehr klar. Und eigentlich war sie es nie. Auch die Dinnerpartys und Bälle der Upperclass im Boston von Samuel Warren und Louis Brandeis waren nicht abgeschottet und ganz privat. Sie waren natürlich gesellschaftliche Ereignisse, die eben in einem spezifischen sozialen Kontext stattfanden. Und natürlich wollten die Gastgeber, dass in der gesellschaftlichen Elite von Boston anschließend über diese grandiosen Festivitäten geredet wurde. Sie wollten nur, dass es innerhalb dieses spezifischen Kontextes bleibt.

Auf diese gesellschaftliche Funktion von Wissen und Nichtwissen als Inklusions- und Exklusionsmechanismus hat Georg Simmel bereits vor 100 Jahren in seinen Studien zum Geheimnis hingewiesen.[20] Das Geheimnis ist gesellschaftlich nur relevant, wenn es geteilt wird. Die Tatsache, dass Gerüchte und Tratsch sozial hoch verregelt sind, zeigt uns aber, dass es wichtig ist, dass ein Geheimnis nicht beliebig verbreitet wird, sondern in seinem Kontext bleibt. Ganz banal gesprochen: Mein Chef weiß andere Sachen von mir als mein Bankberater, meine Partnerin weiß anderes als die Mitglieder des Chaos Computer Clubs. Nur so wird es uns möglich, verschiedene gesellschaftliche Rollen einzunehmen, nur so wird gesellschaftliche Differenzierung möglich. Anstatt an der Unterscheidung privat-öffentlich festzuhalten, sollten wir daher besser zwischen verschiedenen Kontexten unterscheiden. Diese haben jeweils spezifische Normen, die die Weitergabe persönlicher Infor-

[20] Georg Simmel: Das Geheimnis und die geheime Gesellschaft (1. Teil), in: Soziologie. Untersuchungen über die Formen der Vergesellschaftung. Berlin: Duncker & Humblot Verlag 1908 (1. Auflage), 256-304, verfügbar unter http://socio.ch/sim/unt5a.htm.

mationen regeln. Nur wenn diese Normen eingehalten werden, ist die Integrität des Kontextes und der darin organisierten Sozialbeziehungen gewährleistet.

	Norm 1	**Norm 2**	**...**
Kontext 1			
Kontext 2			
...			

Abbildung 7: Das "Kontext"-Modell von Privatheit

Helen Nissenbaum hat versucht, dies in einer allgemeinen Theorie von Privatheit als kontextueller Integrität zusammenzufassen.[21] Dieser Ansatz wird momentan an der Theorie-Front breit diskutiert, und hier scheint sich durchaus ein neues Verständnis von Privacy durchzusetzen.

7. Zeit, Zukunft und Vergessen

Beim Thema "Zukunft" spielt die zeitliche Dimension eine entscheidende Rolle. Und genau diese Dimension ist in der Debatte um Privatheit als kontextuelle Integrität bislang unterbelichtet. Sowohl in der normativen Theorie von Nissenbaum, als auch in den verschiedenen technischen Ansätzen zum nutzer-kontrollierten Identitätsmanagement wird nur in der Sozialdimension differenziert. Man unterscheidet also, dass man in verschiedenen Kontexten unterschiedliche Rollen annehmen kann. Was bislang nicht breit diskutiert wurde, ist die zeitliche Dimension. Was genau auf den Partys von Samuel Warren und Louis Brandeis in Boston vor

[21] Helen Nissenbaum: Privacy as Contextual Integrity, in: Washington Law Review, 79:1 (2004), 119-157, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=534622.

mehr als 100 Jahren passiert ist, weiß heute niemand mehr. Und auch die damals Beteiligten konnten sich wahrscheinlich schon wenige Monate später nur noch an die Highlights erinnern oder im Familienkreis Fotos herumzeigen.

Bei heutigen gesellschaftlichen Events gibt es in der Regel sofort Flickr-Fotos, Blog-Posts und Twitter-Mitteilungen von Gästen und Angehörigen. Was passiert nun, wenn es etwa eine Hochzeitsfeier war, aber die Ehe nach ein paar Jahren scheitert? Die Betroffenen haben dann unter Umständen kein Interesse mehr daran, dass diese Informationen überhaupt verfügbar sind, und sei es auch nur für einen ausgewählten Kreis von Personen, also in einem definierten Kontext. Viktor Mayer-Schönberger hat daher kürzlich vorgeschlagen, dass man personenbezogene Daten mit einem Verfallsdatum versehen sollte.[22] Eine ähnliche Idee gab es auch bei dem anfangs erwähnten Workshop der Identity Futures Working Group:

> *"2010 werden Usenet-Nachrichten von vor 20 Jahren beim Betrachten Altersflecken und Risse haben. Myspace-Einträge von vor zwei Jahren sind vergilbt."* [23]

Computer sollten also das Vergessen wenn schon nicht lernen, so doch zumindest symbolisch darstellen können. An dieser zeitlichen Dimension wird sich meines Erachtens die nächste große Debatte um Datenschutz, Privatheit und informationelle Selbstbestimmung entzünden.[24]

Ein deutliches Zeichen dafür ist übrigens auch, dass sich ausgerechnet um das sperrige Thema "Vorratsdatenspeicherung" der politische Protest gegen die zunehmende Überwachung kristallisiert und organisiert hat. Die Vorratsdatenspeicherung hebt nämlich nicht nur die kontextuelle Integrität auf, indem sie pauschal alles

---

[22] Viktor Mayer-Schönberger: Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing, Research Working Paper 07-022, Cambridge/Mass.: John F. Kennedy School of Government, 2007, http://ksgnotes1.harvard.edu/Research/wpaper.nsf/rwp/RWP07-022.

[23] Identity Futures Working Group: Identity Futures, 2007, http://wiki.idcommons.net/index.php/Identity_Futures.

[24] Die Ideen des Vergessens und des Verfallsdatums gehen über die zeitliche Beschränkung der Datenspeicherung durch die rechtlich bereits vorgesehene Zweckbindung hinaus. Im Gegensatz zu Daten, die zur Erfüllung eines Geschäftes oder anderer Transaktionen bei Dritten anfallen, werden nämlich auf den Plattformen des "Social Web" die Daten von den Betroffenen selber veröffentlicht, ohne dass ein bestimmter Zweck ihrer Nutzung festgelegt wäre.

Kommunikationsverhalten von allen speichern lässt, sondern sie hebt auch das Vergessen auf und zwingt die Betreiber von Internet- und Telefondiensten zum Erinnern - gegen ihr eigenes Geschäftsmodell und gegen die gesellschaftlichen Normen der Kommunikation.

Privacy bleibt also weiterhin ein spannendes Feld, in dem es gerade konzeptionell noch viele Innovationen, aber auch viele Kämpfe geben wird. Das lässt sich mit Gewissheit sagen, auch wenn ansonsten die Zukunft naturgemäß unbestimmt ist.