Die Mythen von Transparenz und Sicherheit im Internet

Günter Müller

Herr Präsident, Herr Dekan, liebe Kollegen, Mitarbeiter, Freunde und Familie,

die Nachricht von der Verleihung der Ehrenpromotion durch die TU Darmstadt an einer so großen und traditionsreichen Fakultät, wie es die Informatik ist, hat schon die Frage aufkommen lassen, ob ich das auch verdiene. Mir ist der Hobbit Bilbo Beutlin aus Tolkiens Herr der Ringe eingefallen, der – wie nun auch ich im Besitz etwas sehr Wertvollen, sagen könnte: **Wenn ich so gut wäre, wie ich mich heute geehrt fühle, dann hätte ich halb so viel Freude, denn ich wäre 10 mal mehr der Überzeugung ich verdiene das.** Ich vertraue der Fakultät für Informatik und der Universität, dass sie eine gute Entscheidung getroffen haben und bedanke mich sehr. Ich freue mich sehr und bin auch stolz Ihren Ansprüchen gerecht geworden zu sein.

Mein Thema heute ist das Verhältnis von Öffentlichkeit und Sicherheit, insbesondere jedoch der Privatsphäre. Da es im deutschen Rechtssystem das Konstrukt der „Privacy“ im Gegensatz zum amerikanischen Rechtssystem nicht gibt, will ich mit dem Begriff „Privatheit“ das ausgeübte Recht der informationellen Selbstbestimmung beschreiben. Wir können dabei zwei Pole unterscheiden: Während Datenschützer jeglichen fremdbestimmten Gebrauch persönlicher Daten verhindern wollen, sehen andere das Heil in der völligen Transparenz und im Internet das dazu notwendige Werkzeug. Sehr häufig stellt man fest, dass gerade die Jüngeren die gewonnene Freiheit über die Gefahren stellen. Die Erfolge der Piratenpartei in Berlin sind ein Ausdruck dieses technisch begründeten Generationenunterschiedes.

Die Piratenpartei und ihre Ideen sind nun keineswegs neu. Sie haben einen geistigen Anwalt, auf den die heutige Interpretation der Privatheit in der US-Verfassung zurückgeht. Lois Brandeis wurde 1856 in Kentucky geboren und 1901 in das oberste Gericht gewählt, was auf konservativer Seite zu heftigen Kampagnen mit Argumenten führte, die schon die Sorgen vor einem Kontrollverlust wie auch beim heutigen Internet andeuten: **„Brandeis ist ein militanter Kreuzritter für die Wahrheit. Er ist gefährlich nicht wegen seiner intellektuellen Brillanz, seiner logischen Fähigkeit und seines Mutes, sondern**

weil er nicht korrumpiert werden kann". Ich werde in meinen Vortrag **vier berühmt gewordene** Sätze von ihm nutzen, um trotz aller herstellbaren Transparenz die Notwendigkeit der Sicherheit und Privatheit zu begründen.

Von 1890 stammt das erste „Klischee" Brandeischer Rhetorik: **„Sunlight is the best of all desinfectants".** Die Metapher ist universell. Chamisso nutzte sie schon 100 Jahre vorher in der Ballade „die Sonne bringt es an den Tag". Nun hat die Piratenpartei gerade in den letzten Wochen in entlarvender Weise erfahren, dass es so einfach mit dem „Sonnenlicht" nicht ist. Zwei ihrer in den Berliner Senat gewählte Abgeordnete hatten verschwiegen, dass sie vor den Piraten bei der NPD waren. Die Ironie ist es nun nicht, dass seltsame Zeitgenossen bei den Piraten Unterschlupf suchen, sondern dass es dort Leute gibt, die nun eine differenziertere Meinung zur Transparenz vertreten. Privatheit gilt solange, bis man ein Amt hat. Klingt nach preußischem Dreiklassenwahlrecht aus dem 19. Jahrhundert. Damals durften nur die Besitzenden wählen - heute hätte nur Amtsferne ein Recht auf Privatheit.

Besser hätte man folgendermaßen argumentiert: Hätte es bereits zuvor Transparenz gegeben, wären die Kandidaten nicht aufgestellt worden. Dazu nun wieder Brandeis: **"If there is time to expose falsehood and fallacies, the remedy is speech not silence?".** Sein Kalkül lautet, dass Transparenz die Kosten der Geheimhaltung enorm erhöhe und man diese gegen den Schaden abwägen müsse, den eine Entdeckung mit sich bringt.

Möglicherweise liegt in der Verletzung dieses Kalküls der Fall Guttenberg und seiner kleineren Epigonen begründet. Die Sonne „Internet" brachte es an den Tag. Die Veröffentlichungen von Wikileaks haben u.a. nicht nur in der amerikanischen, sondern auch in der deutschen Wirtschaft zu sogenannten „War Rooms" geführt, die sich fragten, wie man auf unvermeidbare Transparenz reagieren solle. Letztlich war das Ergebnis einfach, „**tue aus Gefahr vor Konsequenzen nichts, wofür du dich später schämen musst**".

Brandeis, wäre zufrieden. Wer könnte gegen Transparenz sein? Doch so einfach ist der Fall nicht immer. Hier nun ein weiterer Fall aus den USA, der von Larry Lessig in seinem Artikel „Against Transparency" in der Zeitschrift „New Republic" vom Oktober 2009 bekanntgemacht wurde. Unter dem Titel **„ How Money watered down the Climate Bill"** publiziert die Webpage MAPLIGHT.org, dass die Abgeordneten, die für die Annahme der Ablehnung gestimmt hatten,

ein Spendenaufkommen von durchschnittlich $ 37.000 aus der Energie, Öl- und Gasindustrie erhielten, während die Befürworter es auf ganze $ 2.541 brachten. Die Faktenlage scheint eindeutig. Geld kauft Resultate und Einfluss und das Internet bringt es an den Tag.

Ich möchte dazu zwei Aspekte nennen. Der Erste ist das Verständnis von „Fairness“. Darunter werden Kriterien verstanden, die das Verständnis des Entstehens einer Entscheidung scheinbar nachvollziehbar erklären und bei denen das Verständnis der Umstände sicher scheint: So könnte man etwa erkennen, dass z.B. der Abgeordnete oder Firmenchef zu dumm war, um eine Sache zu verstehen. Eventuell waren sie auch zu faul und haben nie an Sitzungen teilgenommen? Vielleicht war jemand zu liberal, zu konservativ oder schlankweg zu gierig? Nun, ist sowas dann fair? Wenn man „Fair“ mit „Vertrauen“ vergleicht, bemerkt man, dass Fair ein statischer Begriff ist und keinen Fortschritt zulässt, während Vertrauen Fehler zwar nicht vermeidet, aber dynamische Veränderungen und Fortschritt beinhaltet. Wenn die Sorge vor Fehlern vorherrscht und Vertrauen fehlt, dann wird jede Öffentlichkeit zur Inszenierung, dient eher der Verschleierung und verkommt zum „Transparenztheater“.

Der zweite Aspekt ist, dass Fakten nicht mit Wahrheit verwechselt werden dürfen, sondern sehr schnell basierend auf einen vorhandenen Wertesystem und einer Urteilsneigung interpretiert werden. Hierzu wieder Brandeis und ein Fall, den Larry Lessig schildert. Die Website Sunlight.org schreibt, dass 2001 ein Gesetz diskutiert wurde, welches für die Kreditkartenindustrie den Nachteil gehabt hätte bei Insolvenz der Kunden selbst leer auszugehen. Mrs. Clinton hat nun 2001 und 2003 gegen dieses Gesetz gestimmt, um dann 2005 als New Yorker Senatorin doch für das Gesetz abzustimmen. Dazwischen lag eine Spende über $ 140.000 aus der Kreditkartenindustrie. Der Fall scheint klar. Sie war in der Zwischenzeit New Yorker Senatorin geworden und ihrer Wählerschaft verantwortlich. Die Meldung erhielt ihren **Sensation**saspekt, weil es sich um Mrs. Clinton handelte und die Berichterstatter waren sich sicher, dass die Leser so viel **Aufmerksamkeit** investieren würden, um die Gründe für die Neupriorisierung selbst nachvollziehen zu können, um zum „richtigen“ Schluss zu kommen.

Dieser „Schluss“ beruht ja dann auf Fakten und da, so glauben die Anhänger von Transparenz sei die Wahrheit eineindeutig ableitbar. Fakten können aber nur in Zusammenhang mit den Interessen, Wünschen, kognitiven Fähigkeiten und den sozialen Kontexten der Akteure richtig interpretiert werden. Wir können also über Wirkungen von Informationen nur dann etwas sagen, wenn man auch erfährt, welche Ketten von Ereignissen zu dieser Entscheidung geführt haben. Dies erfordert aber einen erheblichen Aufwand. Hier gebietet es sich geradezu auf den Rückgang der Auflagen der Zeitungen zu verweisen. In Deutschland hatten Zeitungen bis weit in die 90er Jahre eine Kapitalrendite von 27,3 %. Jetzt sind es im Durchschnitt noch 2,8%. Die Logik der Leser ist: Warum eine Zeitung kaufen, wenn man die Geschichte doch umsonst im Internet bekommen kann. Dieses Verhalten ignoriert den Aufwand verantwortlicher Redakteure bei der Auswahl und der Reduktion der Informationsflut. In diesem Zusammenhang gewinnt die Sensation, da die aufzubringende Aufmerksamkeit mit der Zunahme an Informationen zu teuer wird.

Zu dieser Neigung zur Sensation nun mein dritter Verweis auf Brandeis mit einem überaus aktuellen Thema. Er hat in seinem Buch „**other people’s money**“ geschrieben: **Bankers, when issuing security, must make public the commissions or profits they are receiving“**. Wir haben nun zwei Finanzkrisen erlebt. Im Jahre 2008 ging sie von den USA aus, jetzt sind es die Schulden der Eurostaaten. Alle Forderungen von Brandeis sind erfüllt gewesen und doch konnte das Unheil nicht vermieden werden. Wir erfahren das „Waterloo“ der Ökonomen, da zwar viele Lösungsvorschläge vorhanden sind, aber durch den Begriff „Systemrelevanz“ eine rationale Entscheidung im Sinne der Kalkulation der Risiken nicht mehr möglich ist.

Das tägliche Entscheidungsproblem zwischen „Sensation“ und „Aufmerksamkeit“ ist nun nicht mit zusätzlicher Belehrung zu lösen. Es ist keineswegs „irrational“, wenn man der Mehrheit der Themen im Internet „ignorant“ gegenüber steht. Vielmehr entscheidet man sich zuerst über den Grad an Aufmerksamkeit, den man investieren will oder ob man sich unter Aufbringen eines Minimums an Aufmerksamkeit mit der zuvor durch Dritte gefilterten „Sensation“ zufrieden gibt.

Davor schützt die Sicherheit und Privatheit.

Der vierte Spruch von Brandeis leitet die Diskussion um die Frage wie viel Sicherheit und Privatheit und vor allem: Was kann die Technik dazu beitragen. Für Brandeis gilt: **„Privacy is the right to be let alone".** Nun - Internet ist kein privater Raum. Wer im Internet ist, will nicht alleine sein, nur er will auch nicht ausspioniert werden. Die Frage nach der Privatheit reduziert sich also darauf, ob das Internet ein öffentlicher Raum und Privatheit daher per se ausgeschlossen ist. In den USA ist es nun so, dass man im Internet erst dann einen privaten Raum erzeugt, wenn man ein entsprechendes Bedürfnis explizit äußert, also eine „opt-out" Variante zur Interaktion wählt. In Europa hingegen bleibt man solange im privaten Bereich, bis man explizit ausdrückt, dass man an der Interaktion teilnehmen möchte, also eine „Opt-in" Variante wählt. Dieser einfache Unterschied im Verständnis erzeugt viele Missverständnisse und trägt der Sicherheitsforschung in Europa oft den Ruf ein, den technischen Fortschritt zu behindern. Als Beleg wird oft herangezogen, dass wenige der neuen Dienste in Europa erfunden worden seien. Dies ließe sich auf ein falsches Verständnis von Privatheit zurückzuführen.

Sicherheit wird jedoch dann kein Fortschrittshemmer, wenn man m. E. die folgenden vier Mythen der Sicherheitsforschung als teilweise falsch begreift und sie durch Ziele ersetzt, die der heutigen Zeit und ihrem technischen Stand entsprechen.

1. **Die größte Gefahr für die Privatheit kommt von einem unautorisierten Zugang zu Informationen.**

Die Krypotologie als die Königsdisziplin der Sicherheit hält Informationen vor Unberechtigten geheim. Hierzu müssen sich die Kommunizierenden aber vertrauen, während im Kontext der Privatheit lediglich selbstbestimmt Informationen preisgegeben werden und somit kein Vertrauen notwendig ist.

Es stehen zwei Strategien zur Verfügung. Zum einen die **Datensparsamkeit** und zum anderen automatisierte Werkzeuge, sogenannte „Privacy Enhancing Technologies" (**PET)**. Die Datensparsamkeit erfordert, dass man nichts an Daten freigibt, wenn es die Sache nicht erfordert. Die PET-Technologien versetzen den Nutzer theoretisch in die Lage, seine Wünsche zu formulieren und auch durchzusetzen. Die Annahme ist, dass er dies auch will. Nur so einfach ist es nicht, da das Kalkül der Nutzer meist anders lautet: Diese werden meist durch entsprechende Anreize getrieben. Der Rabattkartenutzer z.B. erwartet laut

Umfragen, dass etwa ein Rabattsatz von etwa 15% erzielbar sei. Entgegen dieses Mythos liegt der tatsächlich ausgezahlte Betrag im Durchschnitt unter 1% der Kaufsumme. Die Privatheit ist dem Einzelnen also nicht viel wert. Dabei zeigt jede Umfrage, dass der Einzelne die Privatheit und die Sicherheit sehr hoch schätzt. Die Sicherheit und Privatheit muss demnach automatisiert werden. Bezüglich der Automatisierung kann auf zwei Ansätze zurückgegriffen werden: Zum einen das von Andrew Yao 1982 entworfene Modell des homomorphen Rechnens. Im hier häufig angeführten Beispiel treffen sich zwei Millionäre, wobei der einzelne keine Kenntnis über das wahre Vermögen des anderen besitzt. Welche Fragen müssen in diesem Kontext gestellt werden, um über den Vermögensstand des anderen Bescheid zu wissen? Man könnte den für solche Problemstellungen von Yao konzipierten Ansatz nutzen, um z.B. ohne Kenntnis der Identität zu kontrollieren, ob Banken oder Staaten Finanztransaktionen vornehmen, die im Sinne des Gemeinwohles als schädlich erkannt werden. Als zweite Option Privatheit herzustellen, kann das automatische Herstellen der Anonymität gesehen werden. David Chaum hat hierzu ebenfalls in den Achtzigern die Möglichkeiten und Grenzen definiert.

In beiden Konzepten kann mit ausgefeilten Techniken Datensparsamkeit erzwungen und ein unberechtigter Zugang verhindert werden. Dennoch finden beide Ansätze durch den Durchschnittsnutzer wenig Anwendung. Um eines vermeintlichen Vorteils willen werden Daten preisgegeben – deren weitere Nutzung würde man aber schon gerne kontrollieren.

2. **Privatheit ist dann gegeben, wenn man keine Personen identifizierenden Informationen (PII) erfasst.**

Wäre dies der Fall hätten weder Google, noch Facebook, noch Apple ein Problem mit der Privatheit. Alle sozialen Netze sammeln Daten und finanzieren mit deren Bearbeitung und Verkauf die Kosten und erzielen darüber hinaus Gewinne. Die Dienste sind das Lockmittel, die Daten der Preis. Sie sind jedoch an wirklich persönlichen Daten nicht weiter interessiert. Die Ursache liegt evtl. im veralteten Denken über Computing, das noch vielfach auf einem arithmetischen Modell basiert, bei dem alle Daten an der richtigen Stelle zur richtigen Zeit sein müssen, um punktgenau eine Person identifizieren zu können. Statistisches Rechnen des E-Commerce, auch als **Data Mining** oder **Business Intelligence** bekannt, braucht diese Exaktheit nicht. Es genügt, wenn

Muster entdeckt werden. So zielt die Strategie von Google auf die Mustererkennung bei „Ortsdiensten“ oder „Location Based Services“ und den hieraus generierbaren Umsätzen ab.

3. **Mitteilung und Optionen zur Wahl sind die Grundpfeiler des Datenschutzes.**

Häufig wird das Bedürfnis nach Privatheit in Abrede gestellt, da man nichts Peinliches zu verbergen und daher kein Problem habe, wenn Daten über einen gesammelt würden. Die Annahme bei solchen Aussagen ist, dass man zum Erhebungszeitpunkt weiß, was mit den Daten in einem jeden zukünftigen Kontext gemacht werden kann. Es ist kein Geheimnis, dass Facebook z.B. in der Wirtschaft genutzt wird, um über Bewerber Persönliches zu erfahren. Die „Mitteilung“ nach Brandeis über und eine sinnvolle Optionenliste zum Umgang mit den Daten ist häufig für Nutzer vorhanden. Nur die Nutzung dieser Möglichkeiten ist so niedrig, dass man ihr Angebot schon als Täuschungsmanöver für den Gesetzgeber bezeichnen muss, sollte dieser Nutzer wirklich schützen wollen. Alle Internetnutzer werden in Europa auf die Nutzungsbedingungen und Gefahren hingewiesen. Sie entscheiden sich überwiegend aus Bequemlichkeitsgründen, bzw. aus kurzfristigen Optimierungsgründen heraus für die Weitergabe persönlicher Daten, um eine spezielle Transaktion abschließen zu können. Im Nachhinein wird die Datenpreisgabe dann verdrängt. Meist nimmt man an, man habe wirklich nichts Wichtiges preisgegeben und theoretisch könne jeder davon wissen.

Helfen würde da nur eine dauerhafte und obligatorische Kontrolle durch vertrauenswürdige Dritte, die gewissermaßen per Institution die Aufmerksamkeit aufbringen, die der Einzelne nicht aufbringen kann oder will. Eine solche verordnete Überwachung ist aber eine technisch nicht triviale Aufgabe und widerspricht unserem gegenwärtigen Modell der freien, unbeobachteten Entscheidung des Einzelnen. Man kann den Teufel ja nicht mit dem Beelzebub austreiben.

4. **Datenschutz ist eine Angelegenheit des Individuums.**

Das Credo der Privatheit und der IT Sicherheit in Europa heißt nun, dass jeder in die Lage versetzt werden solle, sich um den Schutz und die Herausgabe persönlicher Daten selbst zu kümmern. Dazu brauche man Aufklärung und

eben die geeigneten Sicherheitsmechanismen, um automatisch Hilfestellung zu geben und Kontrollen ermöglichen zu können. Hier wieder ein paar Fakten: Mehr als 75% aller Geschäftsprozesse in Deutschland erfolgen ebenso wie über 95% aller Finanztransaktionen über 1000 € elektronisch und inzwischen bestimmt die Internetökonomie nahezu 25% aller Transaktionen. 95% der Kommunikation zwischen Unternehmen und innerhalb von Unternehmen basieren auf dem Internet. Es ist offensichtlich: Das Internet ist ein Wirtschaftsfaktor der Werte erzeugt und diese liegen gewissermaßen auf dem Präsentierteller und erweckt Begierden. Die Preisgabe persönlicher Daten wird von mehr als 75% der Konsumenten nicht aktiv behindert. Sollte es der Befriedigung ihrer Nachfrage dienen werden diese sogar bereitwillig weiter gegeben.

Vielleicht versteht man vor diesem Hintergrund sowohl die Aussagen Zuckerbergs, dem Gründer von Facebook, der Privatheit nicht mehr als gültige soziale Norm beschreibt, während Scott McNeally, der ehemalige Vorstand von Sun, die Privatheit als Irrtum der Geschichte erkennt und Eric Smith, der ehemaligen Vorstandsvorsitzenden von Google und jetzige Chef des Aufsichtsrates, meint, man solle sich doch besser korrekt benehmen, denn früher oder später sei alles in Google nachlesbar. Schirrmacher, der Herausgeber der FAZ sieht den Untergang der europäischen Denkweisen in seinem Buch „Payback“ voraus, da die Vielfalt leide und das Argument dem Populismus nicht gewachsen sei. Lobo, der Internetblogger, sieht in Schirrmacher nur die eisigen Schauer der „alternden“ Reaktionäre, die in der Angst der Raupe lebten ehe dieser ein Schmetterling wird.

Der Datenschutz behindert Geschäfte, nicht jedoch die technische Entwicklung. Der Datenschutz ist gerade wegen Annahmen und Szenarien, die aus dem Vor-Internetzeitalter der Volkszählung von 1983 stammen, zu einem Papiertiger verkommen, der von vielen Internetnutzern auch als solcher gesehen wird. Die Annahmen der informationellen Selbstbestimmung der europäischen und deutschen Datenschutzregulierung überfordern zum einen den Nutzer und erzeugen zum anderen ein Verhalten, welches die Gefahren der Transparenz leugnet, so dass eine angemessene Vertrauensinfrastruktur nicht entsteht, da sich fundamentale Gegensätze in der Gefahrenerkennung einander gegenüberstehen.

Meine Überzeugung ist, dass das Internet kein öffentliches Gut mit gleichen Folgen für alle ist. Das Internet hat die Kontrollfähigkeiten bislang mächtiger gesellschaftlicher Gruppen teilweise außer Kraft setzt. Die Reaktion dieser Verlierer ist daher laut. Wir leiden mit den Protestlern im Iran und den chinesischen Bürgerrechtlern und erkennen die gesellschaftsverändernde Kraft des Internet. Wir nutzen die neuen Medien auch selbst und können auf sie nicht mehr verzichten. Wer kann sich ein Studium oder die Wissenschaft z.B. ohne Google noch vorstellen? Der Preis ist jedoch offensichtlich, obwohl man ihn gerne verdrängt. Wir leben dauerhaft in der Ungewissheit, ob andere mehr Aufmerksamkeit für unsere privaten Daten aufwenden als wir es tun. Der führende Blogger in Ägypten ist verhaftet, Google in China erst jetzt wieder zugelassen und die gegenwärtige Diskussion um den Staatstrojaner in Deutschland zeigt die Unsicherheiten und Ängste. Gleichzeitig wächst eine Industrie heran, die sich das Sammeln von Daten zum Ziel setzt. In einer Gesellschaft, die im Überfluss lebt, sind Kenntnisse über die Wünsche der Individuen wettbewerbsentscheidend und Informationen werden zu unverzichtbaren Rohstoffen für wirtschaftliches Wachstum. Nach der Begeisterung für die neue Freiheit kommen erste Rufe nach **Restoration** auf. Eine solche Restoration - egal aus welcher Perspektive sie kommt - wird jedoch fehlschlagen. Es geht um die Schaffung einer neuen Vertrauensinfrastruktur und nicht um die Durchsetzung von illusionären Idealen, die auf einen Weg zurück deuten.