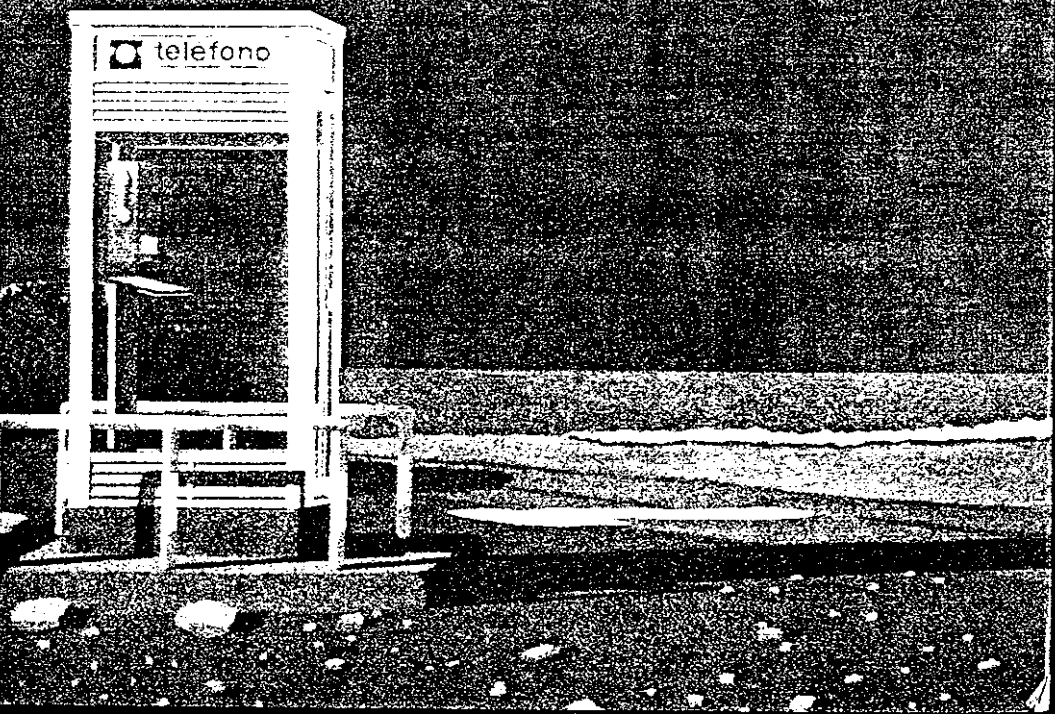
Verlag
C.F. Müller
Karlsruhe

Herbert Kubicek (Hrsg.)

Telekommunikation und Gesellschaft

Kritisches Jahrbuch der Telekommunikation



Kritisches Jahrbuch der Telekommunikation

Herausgeberbeirat

Emil Bock, stellvertretender Vorsitzender der Deutschen Postgewerkschaft
Prof. Dr. **Hans Brinckmann,** Vorsitzender der Gesellschaft für Rechts- und Verwaltungsinformatik
Prof. Dr. **Claus Eurich,** Institut für Journalistik, Universität Dortmund
Dr. **Hansjürgen Garstka,** Berliner Datenschutzbeauftragter und Vorsitzender der Arbeitsgruppe Medien und Telekommunikation der Internationalen Konferenz der Datenschutzbeauftragten
Prof. Dr. **Nicholas Garnham,** Centre for Communication and Information Studies, Polytechnic of Central London
Monika Gebauer / Manfred Dimper, Arbeitsgemeinschaft der Verbraucherverbände
Prof. Dr. **Bernd Lutterbeck,** TU Berlin (Informatik und Gesellschaft)
Prof. Dr. **Barbara Mettler-Meibohm,** Universität Essen (Politikwissenschaft)
Prof. Dr. **Arno Rolf,** Universität Hamburg (Angewandte und sozialorientierte Informatik)
Prof. Dr. **Alexander Roßnagel,** Fachhochschule Darmstadt, Projektgruppe provet
Dr. **Roland Schneider,** Deutscher Gewerkschaftsbund, Abt. Technologie und Humanisierung
Prof. Dr. **Ursula Schumm-Garling,** Universität Dortmund
Prof. Dr. **Wilhelm Steinmüller,** Universität Bremen

Redaktion/Layout: **Uwe Albers,** Universität Bremen

Herbert Kubicek (Hrsg.)

Telekommunikation und Gesellschaft

Kritisches Jahrbuch der Telekommunikation

Mit Beiträgen von
Susanne Bickel, Ulrich Dolata, Herbert Kubicek, Eli M. Noam, Lars Qvortrup, Alexander Roßnagel, Johann Welsch u.a.

Verlag C. F. Müller Karlsruhe

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Telekommunikation und Gesellschaft: kritisches Jahrbuch der Telekommunikation. – Karlsruhe: Müller.
Erscheint unregelmäßig. – Aufnahme nach Bd. 1 (1991)

Bd. 1 (1991) –

1. Auflage 1991
© Verlag C. F. Müller GmbH, Karlsruhe
Umschlag: Johannes Nawrath, Hamburg
Satz: Uwe Albers, Annegret Bausch, Bremen
Druck und Bindung: Druckerei Ernst Grässer, Karlsruhe
Printed in Germany
ISBN 3-7880-7392-6

Inhalt

Eli M. Noam

Privacy bei Telekommunikationsdiensten*

I. Einführung

In diesem Beitrag werden die neuartigen Bedrohungen der Privacy[1] analysiert, die mit der schnellen Evolution der Telekommunikationstechnologie und der Marktstrukturen der Netzanbieter entstehen. Im Anschluß an die Darstellung der neuen Probleme und der konfligierenden öffentlichen Ziele werden Prinzipien für den Schutz der Privacy in der Telekommunikation vorgeschlagen. Diese Diskussion ist nicht hypothetisch. Sie ist Bestandteil eines regulativen Verfahrens, das noch immer läuft und das der Autor initiierte und entwarf, als er Mitglied der Public Service Commission (PSC) des Staates New York war.

Ein Wort der Erklärung an den europäischen Leser: In den Vereinigten Staaten wird der größte Teil der innerstaatlichen Kommunikation (ebenso wie andere Versorgungsgüter wie Elektrizität, Gas, Wasser usw.) von unabhängigen, regulierenden Kommissionen überwacht, deren Funktion es ist, die Öffentlichkeit vor monopolistischen Praktiken privater Versorgungsunternehmen zu schützen. U.a. setzen sie die Gebühren und Geschäftsbedingungen fest, sie überprüfen das Management, billigen Investitionen, überwachen die Qualität, erteilen Lizenzen für neue Anbieter und befassen sich mit allen möglichen Verbraucherbeschwerden. Diese Kommissionen werden im Ausland im allgemeinen kaum wahrgenommen, da sich dort das Augenmerk auf das Bundesamt FCC (Federal Communication Commission) richtet. Die bundesstaatlichen Kommissionen können jedoch ganz aktiv sein und haben auch die entsprechenden Erfahrungen und Ressourcen. Die New Yorker Kommission z.B. verfügt über ein Personal von mehr als 600 Leuten. Neben Wisconsin ist sie die älteste bundesstaatliche Kommission und geht zurück auf die heiß umkämpfte Gouverneurswahl von 1906 (der in dem Film Citizen Kane ein Denkmal gesetzt wurde). Damals verlor der Demokrat William Randolph Hearst, der sich für die Nationalisierung der Versorgungsunternehmen einsetzte, gegen den ebenso berühmten Charles Evans Hughes, der für ein System der öffentlichen Regulierung privater Versorgungsunternehmen eintrat. In neuerer Zeit haben viele der innovativen politischen Entwicklungen in Amerika auf bundesstaatlicher Ebene stattgefunden. In diesem Beitrag wird die Notwendigkeit einer Privacy-Politik in der Telekommunikation diskutiert und die Entwicklung allgemeingültiger Prinzipien im Staate New York verfolgt, dem ersten Versuch dieser Art in Amerika.

* Der Beitrag wurde aus dem Englischen übersetzt von Annegret Bausch.

1 Auf die Übersetzung des Begriffs "Privacy" wurde verzichtet, weil die deutschen Ausdrücke Privatheit, Privatsphäre oder Datenschutz nicht den vom Autor gemeinten und im Text erläuterten Inhalt treffen.

II. Eine Privacy-Politik in der Telekommunikation ist notwendig

Was ist Privacy? Die Privacy im Telekommunikationssektor besteht aus zwei unterschiedlichen, aber miteinander verknüpften Aspekten[2]:

a) aus dem Schutz gegen das Eindringen unerwünschter Information; das wird manchmal als "das Recht, in Ruhe gelassen zu werden" bezeichnet[3] und entspricht dem verfassungsmäßigen Schutz des eigenen Heims gegen Eingriffe des Staates;

b) aus der Fähigkeit, über Informationen über sich und die eigenen Aktivitäten zu bestimmen. Dies ist in mancherlei Hinsicht ähnlich dem Eigentumsschutz, der für andere Formen von Informationen, z.B. im Urheberrecht, gewährt wurde.[4] Ein damit verbundener Aspekt ist der Schutz von persönlichen Informationen vor dem Mißbrauch durch Dritte.

Der gemeinsame Aspekt dieser beiden Punkte ist, daß sie eine Sperre für die Informationsflüsse zwischen dem Individuum und der Gesellschaft in ihrer Gesamtheit bilden. Im ersten Fall ist es eine Sperre gegen zufließende Informationen, im zweiten gegen abfliessende.

Die Entwicklung der Telekommunikationsdienste hat sich in den letzten Jahren beschleunigt. Aber Technologie kann eine zweischneidige Sache sein. Neue Dienste erzeugen neue Probleme oder alte in neuem Gewand. Eines dieser Probleme ist das der Privacy.

Das soll nicht heißen, daß Privacy bei Telekommunikationsdiensten etwas Neues sei. In der Vergangenheit schufen Handvermittlung, Gemeinschaftsanschlüsse und fehlende Vorschriften für das Anzapfen einer Leitung[5] ihre eigenen Probleme. Das erste Patent für ein Gerät zur Stimmenverzerrung wurde 1881 vergeben, nur 5 Jahre nach der Erfindung des Telefons. Es gibt Beweise für das Anzapfen von Telefonleitungen von privater Seite und durch Einzelpersonen 10 Jahre nach Bells Patent.[6] Die New Yorker Polizei hört seit mindestens 1895 Telefone ab. 1916 führte das zu einem Skandal, weil die privaten Unterhaltungen eines katholischen Priesters und die Telefonate einer Anwaltsfirma, die zu J.P. Morgan & Co. bei Munitionslieferverträgen für den 1. Weltkrieg in Konkurrenz stand, abgehört wurden[7]. Aber diese Probleme wurden einigermassen bewältigt, und mit der Zeit entwickelten sich relativ hohe Ansprüche an die Privacy. Doch heute ist eine

2 Siehe z.B. **Richard Posner** (1981)

3 **Warren und Brandeis** (1890)

4 Der Schutz des Urheberrechts im Common Law sah in erster Linie vor, daß Informationen, die jemand in seinem Besitz hatte, jedoch nicht veröffentlichte, auch von niemandem sonst übernommen und veröffentlicht werden konnten. Das kam einer widerrechtlichen Aneignung mit Recht auf Schadensersatz gleich.

5 **Olmstead v. United States**, 277 U.S. 438 (1927)

6 **Westin** (1967)

7 **Seipp** (1981)

neue Generation von Privacy-Problemen entstanden, die teilweise in Abschnitt III aufgeführt sind. Zu den Gründen gehören:

- Immer mehr Transaktionen werden elektronisch ausgeführt.[8]

- Es ist einfacher und billiger geworden, Informationen über Vorgänge und Personen zu sammeln, zu speichern, darauf zuzugreifen, abzugleichen und weiterzuverteilen.[9]

- Die Zahl der Netzbetreiber und Diensteanbieter ist enorm angestiegen; das führt zu einem zunehmend offenen Netzsystem, in dem Informationen über die Benutzung und die Benutzer über die Grenzen des jeweiligen Anbieters hinaus ausgetauscht werden.

- Übertragungskanäle enthalten zunehmend ungesicherte Abschnitte, z.B. aufgrund des Mobilfunks.

Die Beschäftigung mit der Privacy bei elektronischer Kommunikation hat zu verschiedenen politischen Strategien geführt. Westeuropäische Länder haben z. B. umfassende Datenschutzgesetze erlassen und institutionalisierte Ausschüsse und Kommissionen eingerichtet, die oft recht rigorose Beschränkungen für das Sammeln von Informationen und für Datenflüsse eingeführt haben.[10] In den Vereinigten Staaten ging man das Problem weniger systematisch an, was zu einer Reihe von ad hoc-Gesetzen auf Bundesebene und in den einzelnen Bundesstaaten führte. Diese Gesetze, soweit sie sich auf Telekommunikation beziehen, wurden normalerweise außerhalb der Public Utilities Commissions der Bundesstaaten oder der FCC erlassen, und sie gelten oft nur für ein spezielles Problem.[11]

Privacy-Probleme treten jedoch in unterschiedlicher Gestalt immer wieder auf; daher ist es hilfreich, sie systematisch zu prüfen und allgemeine Regulierungsprinzipien zu entwickeln. Das hat verschiedene Vorteile:

a) Anbieter von neuen Diensten wüßten im voraus, wie ihre Angebote gestaltet sein müssen, und könnten sie, wo dies erforderlich ist, zügig genehmigen lassen.[12] Selbst wo eine regulative Zulassung nicht notwendig ist, könnten diese Prinzipien die Sensibilität der Dienstebetreiber für Privacy-Belange erhöhen.

b) Ein breit gefaßter Regelungsrahmen wäre hilfreich für die Gestaltung einer durchgängigen Politik, die verschiedene gesellschaftliche Interessen ausgleicht und einen Kurs

8 Z.B. hatte die Bundesregierung 1962 1.030 Computer-Zentraleinheiten, 1972 6.731, 1982 18.747 und 1985 über 100.000. Linowes (1989)

9 In den letzten 20 Jahren sind die Zugriffskosten für einen Namen auf einer computergestützten Verteilerliste auf ca. ein Tausendstel der früheren Kosten gesunken

10 Siehe **Eli M. Noam**, Telecommunications in Europe, Band I, Oxford University Press, im Druck.

11 Ein Beispiel aus dem Jahre 1990 ist eine Gesetzesvorlage im Kongreß zur Überwachung von computergestützten Nachrichtenverteilern durch die Bediener des Host Systems, um die Verwendung für illegale Aktivitäten zu verhindern.

12 Natürlich wäre oft vielleicht trotzdem eine dienstespezifische Analyse notwendig; aber eine solche Analyse könnte von einer soliden Grundlage ausgehen.

zwischen technikfeindlicher Maschinenstürmerei auf der einen Seite und technokratischer Nichtbeachtung von Privacy-Belangen auf der anderen Seite steuert. Es wäre politisch klug, vorbereitet zu sein.

c) Ein breiterer Ansatz würde eine Definition der Erwartungen an die Privacy erleichtern. Solche Erwartungen haben konkrete Folgen. In zahlreichen Fällen[13] hat das Oberste Gericht der Vereinigten Staaten entschieden, daß die Privacy von den Grundsätzen vernünftiger Erwartungen bestimmt wird. Wenn jemand z.B. vernünftigerweise erwarten kann, daß keine Überwachung stattfindet, wäre die Überwachung in diesem Fall ein unzulässiger Eingriff. Das heißt, offiziell akzeptierte Privacy-Prinzipien könnten für die Formulierung vernünftiger Erwartungen hilfreich sein, die wiederum den Bereich des rechtlichen Schutzes festigen könnten.

d) Wenn die Privacy weiterhin nur fallweise geregelt wird, kann es teuer werden, diese Regelungen auf schon installierte Hardware- und Software-Systeme anzuwenden. Wahrscheinlich ist es für die Hersteller viel billiger, Software-Programme im voraus entsprechend zu konfigurieren, wenn sie sich der Privacy-Erwartungen bewußt sind.

Das Konzept der Privacy ist nicht ohne Kritiker.

(a) *"Nur die Schuldigen brauchen Privacy."*
Im Gegenteil, die Privacy ist einer der Prüfsteine einer zivilisierten und freien Gesellschaft.[14] Autoritäre oder rückständige Gesellschaften schätzen eine Privatsphäre nicht hoch ein, da sie Individualität kaum respektieren und sie den Forderungen von Herrschern oder sozialen Gruppen unterordnen.[15]

(b) *"Die Privacy ist ein Hemmschuh für die Wirtschaft."*
Der Datenschutz erhöht die Kosten der Informationsbeschaffung. Potentielle Arbeitgeber und Käufer müßten z.B. mehr Aufwand betreiben und Geld ausgeben, um herauszufinden, mit wem sie es zu tun haben, wenn der Zugang zu persönlichen Informationen beschränkt wäre. Betrug würde erleichtert, und die Transaktionskosten steigen.

Aber es gibt auch gute wirtschaftliche Argumente für die Privacy. Sie betreffen die Fähigkeit von Firmen und Organisationen, ihre Betriebsgeheimnisse zu wahren und Einzelheiten ihrer Aktionen geheimzuhalten und sich gegen das Durchsickern von Insider-Informationen zu schützen. Informationen haben oft reellen Wert, und da sie meist nicht

13 Z.B. **Katz** gegen **U.S.**, 389 U.S. 347 (1967)

14 Richter **Louis Brandeis** schrieb in einer berühmten Entgegnung von "dem Recht, allein gelassen zu werden - das umfassendste und vom zivilisierten Menschen am höchsten geschätzte Recht". Olmstead gegen U.S., 277 U.S. 438, zu 478 (1927)

15 Zur Geschichte des Persönlichkeitsrechts siehe **Posner**, 1981; **Simmel**, 1906; **Westin**, 1965; **Seipp**, 1978. In den Vereinigten Staaten ist das Persönlichkeitsrecht eine überparteiliche Angelegenheit. Das Gesetz zum Persönlichkeitsrecht von 1974 wurde von den Senatoren Edward Kennedy und Barry Goldwater unterstützt.

durch Eigentumsrechte geschützt sind, müssen sie durch Vertraulichkeit oder Geheimhaltung geschützt werden.[16]

Könnte dieser Schutz leicht gebrochen werden[17], würde das zu einer abnehmenden Produktion solcher Informationen führen. In einem Lehrsatz von Greenawalt und Noam (1979) wurde gezeigt, daß unter normalen Bedingungen "wertvolle Information, die einmal an eine Person (oder höchstens an einige wenige Personen) weitergegeben wurde, - selbst wenn keine Kooperation stattfindet - an alle Teilnehmer weitergelangt." Daher wird das Fehlen von Privacy-Regelungen zur Eindämmung des Informationsabflusses zu einer verminderten Produktion solcher Informationen führen.

Ebenso kann Anonymität die wirtschaftliche Risikofreude erhöhen (jedoch auch das Risiko für die Transaktionspartner); bestimmte Investitionen könnten gekürzt werden, wenn die Identität der Investoren enthüllt würde. In diesem Sinne wirkt die Privacy als Investitionsantrieb, ebenso wie der Schutz durch beschränkte Haftung für Firmen. (Allerdings werden illegale Aktivitäten ebenso vereinfacht.)

Das Fehlen der Privacy führt auch zu Ineffizienz bei Informationsflüssen, ebenso wie das bei überzogenen Privacy-Regelungen möglich ist. Wenn es keine Privacy-Regelungen beim Telefon gibt, werden alle möglichen Andeutungen und Codes verwendet, um den Abfluß von Informationen zu verhindern. Oder man trifft sich persönlich, anstatt das Telefon zu benutzen.

Teilweise als Antwort auf ökonomische und soziale Bedürfnisse wurden viele Transaktionen mit einem spezifischen Informationsschutz ("Privilegien") versehen, z.B. zwischen Anwalt-Klient, Beichtkind-Beichtvater, Patient-Arzt, Bürger-Volkszähler usw. Die Idee ist in jedem Fall, daß der Schutz der Information zu einem sozial höher zu bewertenden Ergebnis führt, selbst wenn es im Einzelfall für Dritte unbequem ist.

(c) *"Privacy ist nur für eine kleine Elite von Interesse."*
Im Gegenteil, die Aufmerksamkeit für die Privacy ist weitverbreitet. Z.B. haben laut einer Information der New Yorker Telefongesellschaft 34 % aller Haushalte in Manhattan und 24 % aller Haushalte des Staates unveröffentlichte Telefonnummern ("Geheimnummern") auf Antrag der Teilnehmer. Die meisten Polizisten, Ärzte oder Richter, um nur einige Berufe zu nennen, haben Geheimnummern. An der Westküste ist die Verbreitung der Geheimnummern noch weiter fortgeschritten und erreicht in Kalifornien 55 %![18]

16 Im Extremfall sind private Informationen für eine Einzelperson so wertvoll, daß sie das Ziel einer Erpressung werden. Siehe auch **Brown/Gordon** (1980) als eine wirtschaftliche Perspektive der FCC.

17 In einer auf Information gegründeten Gesellschaft und Wirtschaft steigen die Anreize zur Informationsbeschaffung ständig. Siehe **Posner** (1981, S. 231-347) mit der umfassendsten Diskussion der Wirtschaftlichkeit der Privacy.

18 Weitere Hinweise gibt eine Umfrage von American Express unter ihren Karteninhabern. 90 % meinten, daß Adressenlisten in unangemessener Weise bekanntgemacht werden, 80 %, daß Informationen nicht ohne Genehmigung an Dritte weitergegeben werden dürfen, und über 30 % glaubten, daß eine bundesweite Gesetzgebung notwendig sei, um den Gebrauch der Listen zu beschränken. "Datenschutzstudie enthüllt Mangel an Verbraucher-Vertrauen", Direct Marketing, Dez. 1988, S. 8, in **McManus**, 1989. 1988 stellte das Amt für

Wird der Wettbewerb sich der Privacy-Probleme annehmen? Nicht unbedingt. Der Wettbewerb könnte einige Privacy-Probleme lösen, besonders, wenn es dem Anwender möglich ist, einen Diensteanbieter auszuwählen, der das gewünschte Privacy-Niveau anbietet. Das Geschäft von Netzbetreibern könnte zurückgehen, wenn die Kunden sich der Privacy bei der Benutzung nicht sicher sind. Aber in vielen anderen Fällen könnte die größere Offenheit eines Konkurrenzsystems und die größere Komplexität seiner verzweigten Netze auch einen erweiterten Zugang zu Informationen gewähren. Es ist einfacher, in einem monopolistischen Zusammenhang die Verbreitung von Informationen zu verhindern. Ein Netz ist von Natur aus eine gemeinsame Einrichtung. In der Vergangenheit bezog sich die Verteilung hauptsächlich auf physische Dinge wie Leitungen und Schalter. Aber in dem Maße, wie die "Intelligenz" der Netze wächst und wie sich Mehrwertdienstenetze und Transportnetze entwickeln, die Teile von Telekommunikationsdiensten sind, bezieht sich die Verteilung immer mehr auf Daten und andere Informationsressourcen.

III. Telekommunikationsdienste und Privacy-Gefährdungen

Fast jeder neue Dienst hat neuartige Privacy-Fragen und -Probleme aufgeworfen. Es folgt eine Liste von Telekommunikationsdiensten und der damit verbundenen Privacy-Probleme - zum Teil potentielle und hypothetische, zum Teil konkrete.

A. Drahtlose Übertragung

1. *Mobiltelefone (Zellulare Telefone)*: Das Abhören von Gesprächen ist möglich,[19] dabei ist dem stationären Teilnehmer oft nicht klar, daß sein Anruf an einen mobilen Empfänger "gefunkt" wird. Es ist auch möglich, den Weg eines Teilnehmers zu verfolgen, indem man anhand der Daten prüft, welche Zellen aktiviert wurden. Damit kann z.B. ein Arbeitgeber die Bewegungen seiner Angestellten überwachen. Die nächste Zellentechnologie (sog. persönliche Kommunikationsnetze, PCN) ist eher personenbezogen als ortsbezogen und verbessert noch die Möglichkeit, Bewegungen festzustellen.

2. *Schnurlose Telefone*: Das Abhören von Gesprächen mit einem in der Nähe befindlichen Radioempfänger ist möglich, ebenso der unbefugte Gebrauch der Telefonnummer eines Teilnehmers, indem man sich mit einem schnurlosen Telefon der gleichen Frequenz Zugang zu dessen Leitung verschafft.

3. *CT-2*: Diese schnurlosen *öffentlichen* Telefone, die zur Zeit in Großbritannien unter der Bezeichnung "Telepoint" eingeführt werden, sind auch für die Vereinigten Staaten

Verbraucherangelegenheiten Massachussetts (Massachussetts Executive Office of Consumer Affairs) bei einer Umfrage nach den wichtigsten Beschwerden der Verbraucher fest, daß Telemarketing und Werbung per Post an oberster Stelle standen. The Boston Herald, 5. Jan. 1989, S. 47. 1986 wollte Pacific Bell Teilnehmerinformation wie z.B. neue Telefonbestellungen verkaufen. Über 75.000 Beschwerden gingen ein, und die Firma gab ihren Plan auf. "Pac Bell verkauft keine Listen", Alameda Times Star, 16. Apr. 1986, zit. nach **McManus**, 1989.

19 Z.B. können ältere Fernsehapparate UHF-Zellenfrequenzen empfangen.

vorgeschlagen worden. Sie gestatten die Überwachung von Gesprächen von diesen öffentlichen Telefonen mit einem in der Nähe befindlichen Monitor.

4. *Pager und Beeper-Systeme* (Cityruf und Eurosignal): Es ist möglich, den Aufenthaltsort des Anrufers festzustellen und Informationen über den Umfang der Nachrichten an den Angerufenen zu sammeln.

5. *Satelliten- und Mikrowellen-Übertragung* (Richtfunk) erlaubt leichteres Abhören als leitungsgebundene Übertragung.

B. Vermittlungsdienste

6. *Voice Mail* erlaubt den unbefugten Zugang Dritter zu Nachrichten, ebenso das unerwünschte Aufbewahren alter Nachrichten.

7. *Rückverfolgung von Anrufen* kann von einer unbefugten Person und ohne Einwilligung des Betroffenen ausgeführt werden.

8. *Brücken- oder Konferenzschaltungen*: Weitere Personen können ohne Wissen des Anrufers zuhören.

9. *Sicherheitsboxen für Informationen* ermöglichen den unbefugten Zugang zu einer Vielzahl personenbezogener Informationen.

C. Endgeräte

10. *Fax-Geräte* gestatten das Hinterlassen von unaufgefordert eingesandten Mitteilungen beim Empfänger (und kostet dessen Thermopapier).

11. *Automatische Wählgeräte* haben zu einem starken Anwachsen ungebetener und aufdringlicher "Müll"-Anrufe geführt.[20]

12. *Synthetische Stimme* vereinfacht die oft aufdringlichen automatisierten Telemarketing-Anrufe, die keine Antwort oder Frage zulassen. Ermöglicht subliminale Nachrichten.

13. *Anrufbeantworter* ermöglichen Dritten den unbefugten Zugang zu Nachrichten (über Fernabfrage). Ebenso ist das allgemeine Aufzeichnen ankommender Gespräche möglich.

14. *Telefone mit Lautsprecheinrichtung*: Wenn kein Signal gegeben wird, weiß der Anrufer u.U. nicht, daß er weitere Zuhörer bei einem privaten Gespräch hat.[21]

20 Eine Analyse des Datenschutzes bei Telemarketing findet sich bei Nadel, 1986.

21 Das passierte kürzlich Präsident Bush, als er ein vertrauliches politisches Gespräch begann und dabei Hunderte von Zuhörern hatte.

15. *Bildtelefone*: Der Empfänger könnte eine Video-Aufnahme des Gesprächs zum Verkauf anbieten.

16. *Fernmesssen und Telemetrie* (Temex) kann als Eingriff in die Wohnung aufgefaßt werden (unbefugter Zutritt).

17. *Passive Überwachungsgeräte* ermöglichen ein sehr spezialisiertes Sammeln von Informationen (z.B. das Messen der Betonung in der Stimme per Telefon) ohne Benachrichtigung der Testperson.

D. Netze und Übertragungsverfahren

18. *Breitband-Netze*: Die aktuellen Pläne beinhalten auch Bus-Architekturen als technische Lösung für eine lokale Verteilung per Glasfaser, wodurch eigentlich eine "Konferenzleitung" hergestellt wird und damit die Möglichkeit besteht, daß unbefugte Dritte in dem Verteilsystem Signale abzweigen können.

19. *Paket-Übertragung*: Pakete können abgezweigt werden, ähnlich wie oben. Darüber hinaus gestattet sie die Identifizierung von Absender und Empfänger von Paketen durch Dritte, die Zugang zum Overhead-Teil des Pakets haben. Sie kann in einem zukünftigen SONET-Breitband-Schnellpaket-Standard zum Problem werden.

20. *Interaktive oder adressierbare Breitband-Videodienste* gestatten die Erstellung von Rechnungen mit detaillierten Angaben über die inhaltliche Nutzung, wie die, die mit der "Bork"-Bill für Video-Läden verboten wurden.[22]

21. *ISDN*: Die Verwendung des "D-Kanals" kann Transaktionen und Steuerungsinformationen Dritten zugänglich machen.

22. *Privatnetze innerhalb von Organisationen* machen es möglich, die Gespräche der Angestellten zu verfolgen, deren Anwesenheit, Aufenthaltsort und Produktivität festzustellen (z.B. Anzahl der Tastenanschläge, die für ein Gespräch verwendete Zeit, Gesamtzeit am Telefon usw.); sie ermöglichen das Abhören von Gesprächen, ohne daß die Angestellten oder der externe Gesprächspartner es bemerken.

23. *Rufweiterleitung*: Das Weiterleiten von Gesprächen an einen nicht einverstandenen Dritten kann als Eingriff in dessen Privacy aufgefaßt werden. Wo eine Mehrfachweiterleitung möglich ist, können Berechtigte Telefonate so umleiten, daß sie abgehört werden können.

22 Der Konservative Robert Bork war zum obersten Gericht nominiert. Während der Senat ihn begutachtete, publizierte eine Zeitung seine Video-Selektionen. Daraufhin wurde eine Gesetz verabschiedet, das solche Informationen schützt.

E. Informationsdienste

24. *Elektronische Post-/Mitteilungsbretter*: Die Verwendung durch Randgruppen hat zu Gesetzesvorlagen im Kongreß geführt, die die Überwachung der Mitteilungsbretter durch die Systembetreiber fordern.

25. *Wähldienste*: Eine obligatorische Vor-Subskription bestimmter Informationsdienste erleichtert die Aufstellung von Listen ihrer Benutzer.

26. *Videotext, Audiotext* ermöglicht die Aufzeichnung der vom Teilnehmer benutzten Seiten oder Programme, die zu einem Profil der geschäftlichen Transaktionen oder der persönlichen Gewohnheiten zusammengestellt werden können.

27. *Videotext-Gateways* ermöglichen dem Netzbetreiber, die vom Teilnehmer verwendeten Informationsseiten und -transaktionen zu überwachen.

28. *Datenbanken* gestatten die Aufzeichnung von zahlreichen personenbezogenen Daten und den einfachen Zugang für viele, einschließlich nicht berechtigter Personen; sie ermöglichen das Abgleichen verschiedener Aufzeichnungen zur Erstellung von Profilen und können heimlich von Außenstehenden geändert werden, auch durch die Verwendung eines "Virusprogramms".[23]

29. *Persönliche Informationsdienste*: Datensysteme auf Namensbasis können durch den unbefugten Eintrag von Namen mißbraucht werden.[24]

30. *Fernabfrage für Telefonbücher*: AT&T plant, im Inland (und später international) den Zugang zu örtlichen Telefonbüchern anzubieten.

F. Signalisierungs- und Netzmanagement-Informationen

31. *Zentraler Zeichengabekanal Nr. 7*: Er liefert Informationen über Ruftransaktionen an andere einschließlich des Angerufenen mit Angabe von Namen, Adresse und anderen damit zusammenhängenden Daten.[25]

23 1978 erließ Florida das erste staatliche Gesetz gegen Computer-Kriminalität, in dem Eigentumsrechte an Computerdaten und das Verbot von unbefugten Zugriffen und Änderungen festgelegt wurden. Seitdem haben die meisten Staaten ähnliche Vorschriften erlassen. In zunehmendem Maße wurde den Computerdaten, -zeiten und -diensten der Status von Eigentum zuerkannt.

24 Ein neueres Beispiel bietet eine Petition des Generalstaatsanwalts von New York an die Public Service Commission bezüglich des unzureichenden Schutzes bei computergestützten "Dating"-Diensten.

25 Zu den Anwendungen gehören: ICLID (Identifizierung der Leitung ankommender Verbindungen für den Dienst mit 800- und 900-Nummern); CLASS (Signalisierungsdienst für Kunden im Ortsbereich) zur allgemeinen Verwendung, auch bekannt als ANI oder CNI (Automatische oder Kundennummern-Identifizierung) und der Notdienst 911.

32. *Automatische Nummernidentifizierung (ANI)*.[26] Die Anzeige der Nummer des Anrufers stellt ein starkes Instrument für telekommunikationsgestützte Transaktionen dar. Sie gestattet auch den Abgleich mit anderen Daten des Anrufers. Dadurch kann die Geheimnummer eines Anrufers dem Angerufenen bekanntwerden. Eine selektive Behandlung und unterschiedlicher Service-Umfang für eingehende Anrufe je nach deren Herkunft werden ermöglicht. Dadurch könnte man von bestimmten Anrufen, z.B. bei Beratungsstellen oder Journalisten, abgeschreckt werden.

Oft wird erklärt, die Automatische Nummernidentifizierung sei vergleichbar damit, nach dem Namen eines Besuchers zu fragen, bevor man die Tür öffnet. Das ist richtig, aber unvollständig. Eine gleichwertige Analogie wäre, wenn sich Käufer in einem Laden oder Besucher in einem Theater vollständig identifizieren müßten und diese Informationen aufbewahrt und an Dritte verkauft würden. Auf jeden Fall ist das Entscheidene nicht, welches die naheliegendste Analogie zu ANI ist, sondern welche vernünftigen Privacy-Erwartungen und welche Privacy-Muster bei einem Telefonat sich mit der Zeit entwickelt haben und wie sie beeinträchtigt werden (Marx, 1989).

33. *800- und 900-Nummern* geben den Teilnehmern Informationen über die Nummern der ankommenden Verbindungen.

34. *Informationsdepots in Zentralen*: Telefongesellschaften wollen ihren Kunden elektronischen Speicherplatz für Informationen wie medizinische und Finanzaufzeichnungen zur Verfügung stellen; dadurch wird das Potential für unbefugte Zugriffe erhöht.

35. *Ton-Wählen*: Einige Spielzeughersteller haben Fernseh-Werbespots gebracht, bei denen kleine Kinder aufgefordert wurden, ihren Telefonhörer an den Fernseher zu halten. Dadurch wird mit einem gesendeten Wähltonsignal das Wählen eines 800-Rufs ausgelöst, um die Telefonnummer für Marketingzwecke aufzuzeichnen und zu verwenden.
Oft wird erklärt, die Automatische Nummernidentifizierung sei vergleichbar damit, nach dem Namen eines Besuchers zu fragen, bevor man die Tür öffnet. Das ist richtig, aber unvollständig. Eine gleichwertige Analogie wäre, wenn sich Käufer in einem Laden oder Besucher in einem Theater vollständig identifizieren müßten und diese Informationen aufbewahrt und an Dritte verkauft würden. Auf jeden Fall ist das Entscheidende nicht, welche die naheliegendste Analogie zu ANI ist, sondern welche vernünftigen Privacy-Erwartungen und -Muster bei einem Telefonat sich mit der Zeit entwickelt haben und wie sie beeinträchtigt werden (Marx, 1989).

G. Ortsüberwachung

36. *Navigationssysteme und "Tripmaster"-Systeme*: Damit können der Aufenthaltsort von Fahrzeugen und die Aktivitäten des Fahrers einschließlich Geschwindigkeit, Schaltung, Leerlauf usw. verfolgt werden.

26 Auch als Anrufer-Identifizierung bekannt. Eine umfassende Analyse der mit ANI zusammenhängenden rechtlichen Probleme findet sich bei **Smith**, 1989.

37. *Armreifen mit passivem Piepsignal* zur Überwachung des Aufenthaltsorts einer Person durch telefongestützte Geräte. Sie werden zur Zeit für Hausarrest als Alternative zum Einschließen in Zellen verwendet, könnten jedoch auch zur Arbeitsüberwachung, für Sozialfälle usw. eingesetzt werden.

38. *Schlüsselkarten*: Im Zusammenhang mit Kommunikationsanschlüssen ermöglichen sie die Überwachung der Bewegungen einer Person innerhalb eines Gebäudes.

39. *Cam-corder*: In Verbindung mit einem Telekommunikationsanschluß können stark miniaturisierte elektronische Kameras und andere Fernsensoren versteckte Video- und Audioüberwachung möglich machen.

H. Informationen über Transaktionen

40. *Einzelgebührenrechnung*: Unbefugte Personen können sich Zugang zu Einzelheiten der Telefongebührendaten verschaffen.[27]

41. *Telefonrechnungen in Hotels*: Die Daten des Benutzers sind vor Einsichtnahme durch das Hotelpersonal und auch durch andere Gäste oft nur wenig geschützt.

42. *Allgemeine Telefondienste*: Art und Einzelheiten eines Telefonabonnements können von Unbefugten leicht festgestellt und geändert werden, ohne daß zur Zeit eine Identifizierung notwendig ist.

43. *Deregulierte Rechnungstellung* ermöglicht die Weitergabe von Telefondaten an andere, ohne daß die Teilnehmer notwendigerweise davon wissen.

44. *Informationen über Eigentümernetze (CPNI)*: Die Transaktionsdaten des Anwenders ergeben wertvolle Marketingdaten für den Netzbetreiber; sie könnten auch an Dritte verkauft werden.

45. *Smart Cards* ermöglichen die Speicherung der mit der Karte geführten Telefonate auf der Karte. Wo Smart Cards allgemein zum Bezahlen verwendet werden, können Aufzeichnungen über das Konsumverhalten, die Telefonbenutzung und -bezahlung und die persönliche Historie angefertigt werden, die dem Verkäufer (einschließlich dem Telekommunikationsnetzbetreiber) am nächsten Ort eines Einkaufs zur Verfügung stünden. Wo Smart Cards für staatliche Zwecke wie z.B. Lebensmittelmarken verwendet werden, können sie über die Verwendung und die Bewegungen des Empfängers Aufschluß geben.

27 Die Watergate-Aufklärer hatten einen Trick herausgefunden und machten es nach eigenen Angaben so: "Bernstein hatte mehrere Quellen im Bell-System. Er zögerte immer, sie für die Informationsbeschaffung über Telefonate zu nutzen und zwar wegen der ethischen Fragen im Zusammenhang mit dem Bruch der Vertraulichkeit der Telefondaten... Ohne über sein Problem nachzudenken, rief Bernstein seinen Informanten bei der Telefongesellschaft an und bat um eine Liste der Anrufe von Barker." **Carl Bernstein und Bob Woodward**, "All the President's Men", Simon and Schuster, New York 1974, S. 35.

IV. Gegenläufige Interessen

Es ist für die Privacy kontraproduktiv, sie nur isoliert zu betrachten. Es gibt andere legitime gesellschaftliche Interessen, die mit der Privacy ausgeglichen werden müssen. Dazu gehören:[28]

1. Pressefreiheit, Informationsfreiheit, Zugang zu Verwaltungsunterlagen: Die Privatsphäre eines Individuums steht gegen den Wunsch der Presse, Einzelheiten über diese Person zu veröffentlichen und gegen das "Recht auf Unterrichtung" der Öffentlichkeit.[29]

2. Gesetzesvollzug und Effektivität der Verwaltung: Überwachung, Sammlung elektronischer Daten und Computerabgleich können machtvolle Instrumente zur Bekämpfung von kriminellen oder terroristischen Aktivitäten sein. Der Zugang zu elektronischen Technologien kann dem zunehmenden finanziellen und technologischen Fortschritt der Gesetzesbrecher entgegenwirken.

3. Verbraucherschutz: Der Einzelgebührennachweis bietet den Teilnehmern finanziellen Schutz vor falschen Gebühren, selbst wenn diese Daten die Privacy einschränken.

4. Wirtschaftliche Freiheit: Jeder Schutz, der nicht auf freiwilligen Vereinbarungen beruht, kann die Möglichkeit reduzieren, bestimmte Dienstleistungen und Leistungsmerkmale anzubieten oder zu beschaffen.

5. Reduzierung des Geschäftsrisikos: Verkäufer oder Kreditinstitute würden weniger Risiken auf sich nehmen, wenn sie einen umfangreicheren Zugang zu den Daten von Kunden, Angestellten und Lieferanten und unmittelbarere Rückmeldung auf ihre Marketing-Aktivitäten hätten. Das Ergebnis könnte besserer Service, weniger Verluste und niedrigere Preise sein.

6. Erhöhung der Informationskosten: Privacy-Regelungen können die Kosten für Informationssuche, -speicherung und -übertragung erhöhen. Dadurch werden informationsgestützte Transaktionen teurer.

7. Effizienz und Innovation: Die Kosten für Privacy können die Einführung und Entwicklung neuer Telekommunikationsdienste behindern, verzögern oder verteuern. Privacy kann eine Verlangsamung der technologischen Entwicklung zur Folge haben.

8. Einfachheit der Bedienung: Die Handhabung eines Netzes kann durch Privacy-Vorkehrungen beeinträchtigt werden. Das Konzept eines Netzes basiert auf der Verteilung von Ressourcen einschließlich der Informationen. Größere Schwierigkeiten bei der Ko-

28 Wie bei den im vorigen Kapitel aufgelisteten Bedrohungen der Privacy können einige dieser Gegengründe hypothetisch sein.

29 Siehe die Entscheidung des Obersten Gerichts der USA 1989 in dem Fall B.J.F. v. The Florida Star (U.A. 109 S. Ct. 2603(1989)), in dem das Gericht zu der Auffassung kam, die Presse sei sehr wohl zu belangen, wenn sie, auch bei wahrheitsgemäßer Berichterstattung, den staatlichen Privacy-Schutz verletze.

ordinierung des Zusammenwirkens von integrierten Netzen können das Ergebnis von Privacy-Vorkehrungen sein, die dieses Verteilen einschränken, z.B. bei Computer-Datenbank-Verbindungen.

9. Persönliche Mobilität: Die Kommunikationstechnologien bieten die Möglichkeit für eine viel größere persönliche Mobilität (z.B. durch Zellulartelefone oder durch Anrufe, die den Angerufenen auf ihrem Weg von einem Ort zu einem anderen folgen), die unter Umständen eingeschränkt würde, wenn die für diese Systeme benötigte "Intelligenz" der Datenbanken begrenzt würde.

10. Kollidierende Privacy-Interessen: Die Ansprüche auf eine Privatsphäre von verschiedenen Teilnehmern an einer Kommunikationsverbindung können kollidieren, wenn z.B. der Wunsch des Angerufenen nach Ungestörtsein und Schutz vor Belästigung im Widerspruch zu dem Wunsch des Anrufenden nach Anonymität steht.

11. Erschwingliche Telefongrundgebühren: Die Einnahmen aus neuen Diensten halten die Grundgebühren auf einem niedrigen Stand. Wenn diese neuen Dienste durch Privacy-Vorkehrungen eingeschränkt oder verzögert werden, entstehen möglicherweise keine Einkünfte, die zu den Grundgebühren beitragen könnten.

12. Landesweite Gleichheit: Wenn bundesstaatspezifische Privacy-Regelungen eingeführt werden, kann das die Einführung von landesweiten Diensten einschränken.

13. Offene Netze: Die Entflechtung auf der Grundlage der Architektur offener Netze (Open Network Architecture, ONA) sorgt für die Gleichbehandlung der Betreiber von Mehrwertdiensten, die mit Grundversorgungsunternehmen konkurrieren.[30] Um vollständige Wettbewerbsgleichheit zu erreichen, müssen die Netzbetreiber u.U. Transaktions- und Kundeninformationen an jene Dienstebetreiber weitergeben. Wenn diese Weitergabe durch Privacy-Regelungen eingeschränkt würde, könnte auch der Telefonnetzbetreiber die Möglichkeit zur Verwendung der Daten verlieren, die ihm zur Verfügung stehen, und das wäre angesichts ihres ökonomischen Wertes und ihrer Verfügbarkeit ineffizient.

V. Allgemeine Prinzipien des Privacy-Schutzes

Die im Anhang aufgeführten Bundes- und Länderstatuten decken einige der in Abschnitt III herausgestellten Privacy-Probleme ab. Die meisten Statuten gelten jedoch für andere Beschäftigungszweige (z.B. Kreditbüros) oder für das Verhalten von Regierungsstellen, oder sie zielen auf flagranten Mißbrauch wie z.B. Computer-"Einbrüche". Das bedeutet, vieles ist nicht abgedeckt, z.B. die Behandlung von Signalisierungs- und Transaktionsdaten. Hinzu kommt, daß die Benutzer nicht über die Privacy-Gefährdungen aufgeklärt werden.

30 Die FCC-Richtlinien in der Zweiten Anfrage zu Computern fordern, daß örtliche Vermittlungsträger alle "netzbezogenen Informationen des Kunden" bekanntgeben, wenn sie von einem Teilnehmer dazu bevollmächtigt werden. "Geheime" und unveröffentlichte Telefonnummern dürfen jedoch nicht freigegeben werden.

Um mit den anderen und telekommunikationsspezifischen Problemen umzugehen ist es zunächst notwendig, ein Konzept für allgemeine Prinzipien des Privacy-Schutzes aufzustellen. Diese vom Autor ausgearbeiteten Prinzipienvorlagen wurden von der Public Service Commission des Staates New York am 31.1.1990 als Diskussionsgrundlage zur Stellungnahme veröffentlicht. Sie basieren auf den Prinzipien der Wahlmöglichkeiten und der Übernahme der Kosten durch diejenigen, die den Status quo des Privacy-Schutzes ändern.

A. Einführung eines Systems von Privacy-Wahlmöglichkeiten

1. Keine Maschinenstürmerei für die Sicherung der Privacy
Für den Privacy-Schutz sollten die "Intelligenz" und die Möglichkeiten des Netzes nicht reduziert werden. Stattdessen sollte es Ziel der Telekommunikationspolitik sein, ein System vielfältiger Hardware- und Software-Optionen aufzubauen, das die Privacy sicherstellt.

2. Mehr-Ebenen-Konzept zur Sicherung der Privacy
a) Erstens: Ein "Standard-Privacy-Schutz" auf angemessenem Niveau als Grundlage. Er wäre Teil des Basis-Service der Netze; dafür würde keine Extra-Gebühr erhoben. Zu den Verpflichtungen eines Netzbetreibers gehört eine akzeptable Qualität des Service; und diese Qualität schließt eine Privacy-Komponente ein.

b) Zweitens: Für die jeweiligen Anwender und Betreiber von Netzen und Mehrwertdiensten, die einen besonderen Bedarf haben, sollte es zusätzliche Optionen für einen "gehobenen" Privacy-Schutz geben, die Extra-Gebühren kosten. Die Schlüsselfragen für neue Dienste sind daher:

(a) Welches Niveau muß der Standard-Privacy-Schutz haben?
(b) Welche zusätzlichen Elemente des gehobenen Privacy-Schutzes sollten dem Anwender zur Verfügung stehen?
(c) Was soll dieser gehobene Privacy-Schutz kosten?

Wenn der Standard-Privacy-Schutz minimal und der gehobene Schutz teuer ist, werden die meisten Benutzer ungeschützt bleiben. Wenn andererseits der Standardschutz auf einem hohen Niveau ist und der Preis für den gehobenen Schutz künstlich niedrig gehalten wird, könnte das zu einem übertriebenen Privacy-Schutz führen, und zwar abhängig von den direkten Kosten und von dem Gewicht einiger der in Abschnitt IV aufgeführten Gegengründe.

Es ist auch vorstellbar, daß ein Anwender ein *niedrigeres* Privacy-Schutzniveau haben möchte als den Standard. Ein solcher Schutz unterhalb des Standards sollte ebenfalls zur Verfügung stehen, solange er nicht die Privacy-Belange Dritter beeinträchtigt und solange seine Wahl Gebühren kostet, wenn damit Kosten verbunden sind.

So stünden also den Anwendern mehrere Ebenen des Privacy-Schutzes zur Verfügung. Diejenigen mit einem hohen Anspruch an den Privacy-Schutz brauchen den Standard nicht zu akzeptieren, noch müssen die meisten Anwender mit einem für ihre Zwecke zu strikten Privacy-Schutz arbeiten.
Um den Standardschutz zu erhalten, braucht der Anwender nicht tätig zu werden, während für einen abweichenden Schutz (entweder auf höherer oder auf niedrigerer Ebene) eine Auswahl getroffen werden muß.

3. Ermutigung der Privacy-Schutz- und Sicherheitstechnologie.
Eine telekommunikationsregulierende Kommission oder Behörde sollte innerhalb ihres Zuständigkeitsbereichs die Entwicklung und das Angebot von Privacy-förderlichen Service-Elementen in Hardware und Software sowohl für den Standard- als auch für den gehobenen Schutz fördern (Beispiele: Elemente des Basis-Service, die einen hohen Zugriffsschutz gewährleisten; die automatische Nummernidentifizierung, die von den Anrufenden ein- und ausgeschaltet oder auf Dauer eingestellt werden kann ("Geheimnummern"); Option einer zentralen Blockierung für einen sich nicht identifizierenden Anrufer; Option einer Blockierung gegen unaufgefordert eingehendes Telemarketing; ein Signal "Keine Werbung" in der Vermittlungsstelle oder im Endgerät, um unaufgefordert eingehende Telemarketing-Anrufe abzuwehren; Ende-zu-Ende-Verschlüsselung; Pufferspeicher und Blindnummern, die eine Informationsdistanz zwischen den Kommunikationspartnern herstellen, usw.[31] Die Geheimnummern müssen sichergestellt werden. In einigen Fällen sollte die Kommission Versuche mit Privacy-Schutz-Technologie, -Software und -Anwendungen fördern.

4. Der gehobene Datenschutz sollte sich selbst tragen.
Die Gebühren für Erweiterungen des Privacy-Schutzes über den Standardschutz hinaus sollten die Kosten decken. Der Standardschutz sollte als Teil des Grundservice keine Extragebühren kosten.

5. Die Kosten der Wiederherstellung des Status quo im Privacy-Schutz sollten von denen getragen werden, die ihn ändern.
Neue Dienste sollten die Kosten einer signifikanten Reduzierung des Status quo des Privacy-Schutzes, die anderen Netzteilnehmern entstehen, decken. Man nehme z.B. an, daß ein neuer Dienst (wie z.B. Rufnummernidentifizierung) viele Teilnehmer, die ihre Privatsphäre hoch schätzen, dazu bringt, die Unterdrückung der Anzeige zu fordern, um den Status quo ihrer Privacy aufrechtzuerhalten. Also müßten in den Kosten für den neuen Dienst die Kosten für eine solche Anpassung der vorhandenen Teilnehmer enthalten sein; und die Teilnehmer oder Betreiber eines neuen Dienstes müßten die durch die Teilnehmer entstehenden Kosten tragen, die ihren Status quo beibehalten. Auf der anderen Seite könnte es dadurch abschreckend teuer werden, einen neuen Dienst anzubieten oder ihn als einer der ersten anzuwenden. Darüber hinaus muß die potentielle Brauchbarkeit eines neuen Dienstes als Option für viele als Vorteil betrachtet werden. Daher muß zwischen den Kosten für jetzige und zukünftige Anwender und Nutznießer ein Ausgleich geschaffen werden.

31 Für die automatische Nummernidentifizierung würde zu den Schutzoptionen eine Unterdrückung der Nummer des Anrufenden gehören, und zwar sowohl für einzelne Rufe als auch für alle Rufe eines Teilnehmers, der diese Option wählt. Der Angerufene erhielte ein "P"-Signal, das anzeigt, daß der Anrufer sich nicht identifizieren möchte und der Anruf würde entgegengenommen, je nachdem, ob der Angerufene dies wünscht oder nicht. Solche Wünsche könnten auch in das Terminal oder die Nebenstellenanlage des Kunden einprogrammiert oder als Blockierungsoption im Schalter angeboten werden. Eine andere Option wäre ein Signalton, mit dem die Anrufer auf das Vorhandensein einer Anrufer-Identifizierung hingewiesen würden; sie könnten dann den Anruf vor Beginn beenden.

B. Prinzipien der Bekanntgabe (Disclosure)

6. Darlegung der Gefährdung der Privatsphäre erforderlich.
Wenn gebührenpflichtige Dienste bei der Kommission eingereicht werden, sollte eine Beschreibung ihrer möglichen Privacy-Auswirkungen und der Möglichkeiten kleiner und großer Anwender, sich dagegen zu schützen, beigefügt werden. Sowohl für gebührenfreie als auch für gebührenpflichtige Dienste sollte die Kommission entsprechend ihren Vorschriften eine Darlegung der Privacy-Gefährdung für die Kunden, insbesondere für Privathaushalte, verlangen.

7. Informationelle Symmetrie
Wo es technisch möglich ist, sollten verdeckte Privacy-Gefährdungen dem Kommunikationspartner durch ein Signal im Netz oder Endgerät angezeigt werden.[32]

8. Informationstreuhänderschaft
Organisationen, die den Netzbetreiber oder andere Kommunikationsdienste für andere auswählen, müssen diese auf Privacy-Gefährdungen hinweisen. Der Umfang der Verantwortlichkeit hängt von der Art der Beziehung ab. Gespräche mit nicht angestellten Dritten, die über ein öffentliches Netz gehen, sollten nicht ohne Benachrichtigung überwacht werden dürfen. Angestellte können mit Recht erwarten, daß sie über unbefugte Überwachungspraktiken ihrer Arbeitgeber im Zusammenhang mit dem Telefon informiert werden.

C. Prinzipien der Nicht-Bekanntgabe (Non-Disclosure)

9. Bedarf an Wissen; Bedarf an Speicherung (Need-to-know; need-to-save)
Anbieter von Kommunikationsdiensten sollten interne Strukturen und Verfahren zum Schutz von Informationen über Anwender vor unbefugten Außenstehenden und Mitarbeitern einführen. Diese Verfahren müßten sicherstellen, daß in Engpaßsituationen gesammelte Daten gelöscht werden, sobald sie vernünftigerweise für den Betrieb nicht mehr benötigt werden. Dabei sind Transaktionsdaten wie Abrechnungsdaten oder Inhaltsdaten sowie Voice-Mail-Nachrichten eingeschlossen.

32 Z.B. wenn der stationäre Partner eines Gesprächs nicht weiß, daß er mit einem zellularen Telefon spricht und das Gespräch daher leicht abzuhören ist. Ein einfacher periodischer Piepton, in zellulare oder Brücken-Kommunikationsverbindungen einprogrammiert, würde dieses Problem lösen.

10. Informationsstückelung
Netzbetreiber, die Gateway-Dienste anbieten, sollten zu den Informationen über spezifische Daten oder Texte, auf die der Anrufer zugegriffen hat, keinen Zugang haben. Die Einzelgebührennachweise für Informationsdienste sollten keinen Aufschluß über den Inhalt der Nutzung geben, es sei denn, der Benutzer wünscht dies.

11. Privacy bei Koppelungen
Netz- und Dienstekoppelungen müssen unter Berücksichtigung der Privacy-Belange der Endbenutzer eingerichtet werden.

12. Kern vs. Peripherie
Der Transfer von Zeichengabe-Informationen zwischen den Kommunikationsnetzbetreibern ist akzeptabel für den Aufbau der Basisübertragung. Je mehr Zeichengabeinformationen die Öffentlichkeit oder keinen Vorschriften unterliegende Diensteanbieter erreichen, desto größer ist die Erwartung an die Bekanntgabe- und Schutzoptionen (falls keine gegenteiligen vertraglichen Regelungen vorliegen).

D. Transaktionsinformationen

13. Gemeinsamer Besitz transaktionserzeugter Informationen
Beide Parteien einer der Public Service Commission unterliegenden Telekommunikationstransaktion haben Besitzrechte an den durch die Transaktion entstandenen Informationen. Die Teilnehmer der Transaktion sind gemeinsame Besitzer der durch die Transaktion erzeugten Information, wenn sie in dieser Information identifizierbar sind, es sei denn, sie hätten eine abweichende Abmachung getroffen. Eine solche Information kann daher nicht ohne ihre Zustimmung an Dritte verkauft werden.

E. Schutz vor dem Eindringen in die Privatsphäre

14. Das Recht, in Ruhe gelassen zu werden.
Als Schutz gegen unerwünschte Anrufe und Fax-Sendungen müssen netzseitige Optionen zur Verfügung gestellt werden. (Dazu könnten gehören: Ein Signal "Keine Werbung" in der Vermittlungsstelle oder im Endgerät, um unerwünschte Anrufe abzuwehren; vom Benutzer ausgelöste Blockierung bestimmter Vorwahlen, die den Telemarketingfirmen zugeordnet sind[33]; und ein Marktsystem, in dem Telemarketingfirmen die Telefonteilnehmer für den Zugang zu ihrem Heim und ihrer Zeit bezahlen könnten, z. B. durch eine Gutschrift auf ihre Telefonrechnung.)

33 Die Klassifizierung als Telemarketing geschähe nach eigenem Ermessen, aber Telemarketingfirmen, die sich nicht als solche ausweisen, können mit einer Zivilklage wegen Erregung öffentlichen Ärgernisses belangt werden. Ein Gesetz zur Einschränkung des Sendens unerwünschter Telefaxe liegt der gesetzgebenden Körperschaft New Yorks vor.

15. *Die von privater Seite durchgeführte, absichtliche Überwachung von Kommunikationsverbindungen, die nicht für sie bestimmt sind, ist illegal.*

16. *Die Verletzung der Privatsphäre ist kein Sport.* Das absichtliche Anzapfen eines Computers ist ein ernstzunehmender Bruch der Privatsphäre anderer. Es ist ein kriminelles Vergehen, einen "Virus" einzugeben oder Computer anzuzapfen: die Verantwortung trägt auch der, von dessen Anschluß das Vergehen ausging, wenn der Anschlußinhaber es wußte oder hätte wissen können.

Diese umfassenden Diskussionsgrundlagen beschloß die Public Service Commission des Staates New York mit einer Gegenstimme; sie wurden am 31.1.1990 zur Stellungnahme veröffentlicht. 31 schriftliche Stellungnahmen wurden eingereicht: 12 von Kommunikations- und Informationsunternehmen oder Industrieorganisationen, 1 von einer anderen staatlichen Stelle des Verbraucherschutzes, 2 von körperschaftlichen Benutzern, 3 von anderen Versorgungsunternehmen, 4 von gemeinnützigen Organisationen und 8 von Einzelpersonen, darunter 4 Privacy-Experten aus dem Universitätsbereich und ein U.S. Senator (Senator Herbert Kohl aus Wisconsin, der Initiator einer bundesweiten Privacy-Gesetzgebung).

Auf der Grundlage dieser Stellungnahmen beschloß die Kommission - wiederum nicht einstimmig - am 23.5.1990 die folgenden Privacy-Prinzipien[34]:

Privacy-Prinzipien für die Kommunikation

1. *Privacy sollte bei der Einführung neuer Telekommunikationsdienste ausdrücklich berücksichtigt werden.* Zu diesem Zweck müssen die Unterlagen für die Festsetzung neuer Tarife neben den übrigen erforderlichen Informationen eine diesen Prinzipien entsprechende Analyse der Auswirkungen des neuen Dienstes auf die Privacy oder eine Erklärung, daß es solche Auswirkungen nicht gibt, enthalten.

2. *Das Interesse an einem offenen Netz sollte bei der Beurteilung von Alternativen für den Privacy-Schutz anerkannt werden.* Das heißt, Schutzeinrichtungen müssen, wenn möglich, kundenspezifisch ausgerichtet sein; Netzsperren, die die Kunden selbst errichten können, wären automatischen Sperren vorzuziehen, die die Kunden überwinden müßten. Das gilt sowohl für den Zugriff auf das Netz (z.B. Anrufsperre für 900-Nummern) als auch für den Zugriff vom Netz (z.B. Sperre von "Müll"-Anrufen).
3. *Unternehmen sollten ihre Kunden im Hinblick auf die Auswirkungen der von ihnen angebotenen Dienste auf die Privacy erziehen.* Wenn die Unternehmen das Prinzip 1 befolgen, müßten die Gebiete, auf denen eine Erziehung der Kunden notwendig ist, deutlich werden.

34 Dies war die letzte Sitzung des Autors als Kommissionsmitglied.

4. *Die Menschen sollten zwischen verschiedenen Stufen des Privacy-Schutzes wählen können, sowohl was den Abfluß von Informationen über sie selbst als auch den Empfang von eingehenden Mitteilungen betrifft.*

5. *Eine Telefongesellschaft, die einen neuen Dienst anbietet, der die bestehenden Erwartungen an die Privacy nicht erfüllt, müßte verpflichtet sein, den verlorengegangenen Privacy-Schutz kostenlos wiederherzustellen, es sei denn, sie gäbe gute Gründe dagegen an.*

6. *Kosten und Sozialpolitik spielen bei der Preisfestsetzung für Privacy-Schutzeinrichtungen eine Rolle.* Im allgemeinen sollten die Kunden, die den gehobenen Privacy-Schutz wählen, ihn kostendeckend bezahlen, eventuell sogar einen weiteren Beitrag leisten; Kunden, die einen Privacy-Schutz wählen, der nur die vorher bestehende Privacy-Stufe gegen einen neuen Dienst aufrechterhält, sollten dafür nicht zur Kasse gebeten werden. Diese Vorgaben könnten in besonderen Fällen nach erfolgter Glaubhaftmachung außer Kraft gesetzt werden.

7. *Wenn ein Benutzer nicht ausdrücklich zustimmt, sollten Informationen über die Benutzer, die durch ihre Verwendung eines Telekommunikationsdienstes entstanden sind, nur im Zusammenhang mit der Leistung oder Berechnung dieses Dienstes oder für andere, von den Benutzern geforderte Waren oder Dienstleistungen verwendet werden; sie dürfen nicht in anderem Zusammenhang zugänglich gemacht werden.* Die den Vorschriften unterworfenen Unternehmen wären verpflichtet, technische Maßnahmen, Betriebsverfahren und Gebühren so zu gestalten, daß die Wahrscheinlichkeit eingeschränkt wird, daß Informationen für nicht zugelassene Zwecke von ihnen oder den anderen Teilnehmern verwendet werden. Die Kunden können Schadensersatz verlangen, wenn Informationen über sie benutzt wurden. Durch entsprechende Gesetzgebung müßten diese Forderungen auch für nicht den Vorschriften unterworfene Körperschaften verbindlich gemacht werden.

8. *Die Erwartungen an die Privacy können sich im Laufe der Zeit ändern und in einigen Fällen Änderungen der Telekommunikationsdienste erforderlich machen.*

Wahrscheinlich werden diese oder ähnliche Prinzipien in ihrer endgültigen Form im ersten Halbjahr 1991 übernommen. Das wäre der erste Fall eines allgemeinen Privacy-Regelungsansatzes für die Telekommunikation in den USA: Zusammen mit ähnlichen Initiativen in Europa könnte dies zu einem größeren Bewußtsein für Privacy-Belange auf dem Gebiet der Telekommunikation führen, ähnlich wie vor 20 Jahren für Computer und Datenbanken.

Angesichts der Komplexität und Allgegenwärtigkeit der Telekommunikation ist es wichtig zu erkennen, daß einfache Lösungen weder praktisch noch wünschenswert sind. In Gesellschaften, wo praktisch jeder Telekommunikationsnachrichten sendet oder empfängt und jeder unterschiedliche Schutzbedürfnisse hat, haben Einheitslösungen keinen Sinn. Stattdessen müßte es das Ziel der Politik sein, den Kunden vielfältige Schutzmaßnahmen zur Verfügung zu stellen, mit denen sie die für sie angemessene Schutzstufe herstellen können, nachdem sie von den Betreibern von Telekommunikationsdiensten

über die Gefährdungen ihrer Privacy aufgeklärt wurden. Glücklicherweise können moderne digitale Schaltstellen, die wie Computer arbeiten, mit verschiedenen Formen des Schutzes programmiert werden. Solche Schutzmaßnahmen sollten nicht so viel kosten, daß nur wirtschaftlich gutgestellte Menschen sich Privacy leisten können, insbesondere dann nicht, wenn die Privacy durch einen neuen Dienst beeinträchtigt wurde.

Mit Flexibilität und dem Angebot von regulativen und technischen Maßnahmen zum Schutz der Privacy soll die Telekommunikation der Zukunft kein unkontrollierbares elektronisches Leck in dem Schutzwall um die Privacy von Individuen werden.

Anhang

Der vorhandene rechtliche Rahmen des Privacy-Schutzes in den USA

1. In der Verfassung

Die US-Verfassung schützt die individuelle und geschäftliche Kommunikation nur gegen staatliche Eingriffe. Die Entwicklung des Schutzes verlief unregelmäßig, zumal das Wort "Privacy" in der Verfassung nicht auftaucht. Der Maßstab der Gerichte war die Erwartung der Benutzer an die Privacy; dadurch wird jedoch ein Prozeß der Erosion ermöglicht: je mehr man sich an die Überwachung von Anrufen oder Transaktionen gewöhnt, um so weniger werden sie geschützt.

Regelungen in der Verfassung	**Schutzbereich**
Erste Verfassungsergänzung	Rede- und Versammlungsfreiheit, individuelle Autonomie
Vierte Verfassungsergänzung	Schutz von Personen und Eigentum vor unbilliger Durchsuchung
Fünfte Verfassungsergänzung	Freiheit von Selbstbeschuldigung
"Implizierte Rechte"	Schutz des Namens, Grundrechte bei Eingriffen in die Freiheit[35]

Daraus resultierender gerichtlicher Schutz

Informationen über die Verschreibung von Medikamenten oder medizinischen Therapien dürfen nicht individuell identifizierbar festgehalten werden.

Die Mitgliedschaft in einer (kontroversen) Organisation darf nicht bekanntgegeben werden.

Ruf und Würde müssen gegen Verleumdung und Verletzung der Privacy geschützt werden.

35 Richter **William Douglas** schrieb über die verfassungsmäßigen Privacy-Rechte, man fände sie "zwischen den Zeilen, gebildet durch Emanationen".

In letzter Zeit hat das Oberste Gericht der USA die Fälle, die mit Privacy-Aspekten von Abtreibungen und Sexualverhalten zusammenhängen, an gesetzgebene Körperschaften und unabhängige Regierungsstellen übergeben.[36]

2. Rechtsvorschriften

Rechtsvorschrift	Schutzbereich
Kommunikationsgesetz (1934)	Unbefugte Personen dürfen Kommunikationen weder abhören noch veröffentlichen.
Katz vs. US 389 US 347 (1969) (verwirft Olmstead vs. US 277 US 438)	fordert eine Genehmigung und Kriterien für einen möglichen Grund für das Abhören.
Omnibus Crime Control Act (1968) Title III	verbietet den polizeilichen Stellen die Verwendung von elektronischer Überwachung, außer bei gerichtlicher Anordnung.
Foreign Intelligence Surveillance Act (1978)	regelt die elektronische Überwachung von US-Bürgern bei ausländischer und Gegenaufklärung.
Privacy Protection Act (1980)	schützt vor Durchsuchungen von Presseakten.
Electronic Communications Privacy Act (1986) (ECPA)	verhindert die Verbreitung von Inhalten von Kommunikationsdiensten an andere als an die vorgesehenen Empfänger.
Freedom of Information Act (1966)	fordert öffentlichen Zugang zu Bundesunterlagen und -dokumenten (außer bei speziellen Ausnahmen).
Fair Credit Reporting Act (1970)	Kreditinstitute müssen ihren Kunden gestatten, ihre Kreditunterlagen einzusehen; diese Vorschrift soll das Bekanntwerden von Kreditinformationen verhindern, es sei denn, es gäbe "eine legitime geschäftliche Notwendigkeit".
Bank Security Act (1970)	fordert, daß Finanzinstitute Unterlagen über ihre Kunden führen.
Rowan vs. Post Office Dept. (1970)	sichert das Recht von US-amerikanischen Postempfängern, daß sie ihre Namen von einer Verteilerliste streichen lassen können.
Crime Control Act (1973)	schützt die Privacy von Informationen in den bundesstaatlichen Strafgesetzsystemen.
Equal Credit Opportunity Act.(1974)	beschränkt Arten von Informationen, die ein Gläubiger sammeln kann.
Privacy Act (1974)	richtet die US-Privacy-Schutzkommission ein, verbietet die Verwendung von Informationen für andere Zwecke als vorgesehen (Lücke in der "Verteilung").
Family Education Rights and Privacy Act (1974)	fordert, daß Erziehungsunterlagen zur Verfügung gestellt werden müssen und verbietet deren Preisgabe an Dritte.
U.S. vs. Miller (1974)	entschied, daß Bankkunden keine Privacy in den Bankunterlagen erwarten können.
Right to Financial Privacy Act (1978)	beschränkt den Zugriff von Bundesstellen auf die Unterlagen von Bankkunden, gilt nicht für staatliche oder lokale Regierungsstellen oder das FBI und US-Staatsanwälte.

36 **Webster vs. Reproductive Health Services**, US 109 S. Ct. 3040, 1989; **Bowers vs. Harwick**, 1987.

Tax Reform Act (1976)	Steuerrückzahlungen und persönliche Daten dürfen nicht ohne Zustimmung bekanntgegeben werden.
Electronic Funds Transfer Act (1980)	fordert die Benachrichtigung des Kunden, wenn Dritte Zugang zu Informationen über elektronische Geldbewegungen haben.
Papermark Reduction Act (1980)	Informationsanforderungen von Bundesstellen müssen ihren Verwendungszweck erkennen lassen und zugelassen werden.
Debt Collection Act (1982)	fordert angemessenen Schutz des Verfahrens, bevor die Schulden eines Individuums beim Bund einem privaten Kreditinstitut bekanntgemacht werden.
Cable Communication Policy Act (1984)	beschränkt die Weitergabe von Kundeninformationen durch Kabelfirmen.
Computer Fraud and Abuse Act (1986)	erklärt den illegalen Zugriff auf Computer zur Entnahme von Informationen zu einem kriminellen Akt.
Budget Deficit Reduction	fordert vom Staat, Steuer-, Gesundheits- und Sozialversicherungunterlagen abzugleichen, bevor Wohlfahrtszahlungen bewilligt werden.
Video Privacy Protection Act (1988)	verbietet Videohändlern, Verleihunterlagen zu verkaufen oder bekanntzumachen.
Computer Matching and Privacy Protection Act (1988)	beschränkt den Gebrauch von Computerabgleichdaten durch Bundesbehörden.
Employee Polygraph Act (1988)	verbietet Lügendetektor-Test bei Angestellten.

Ebenso gibt es eine große Anzahl von bundesstaatlichen Gesetzen, die verschiedene Aspekte der Privacy regeln.

VI. Ausgewählte Bibliographie

Aumente, Jerome: New Electronic Pathways: Videotex, Teletext, and Online Databases. Newbury Park, California, Sage Publications Inc. 1987.

Berman, J. & Goldman, J.: A Federal Right of Information Privacy: The Need for Reform. Benton Foundation, 1989.

Bloustein, Edward J.: Privacy Is Dear at Any Price: A Response to Professor Posner's Economic Theory. 12 Georgia Law Review. 429, 1978.

Bok, Sissela: Secrets: On the Ethics of Concealment and Revelation. New York, Pantheon Books, 1982.

Brown, James Jr. & Gordon, Kenneth: "Economics and Telecommunications Privacy: Framework for Analysis". FCC, OPP, Arbeitspapier, 1980.

Burnham, David: The Rise of the Computer State. New York, Random House, 1983.

Burns, Peter T.: Privacy and the Common Law: A Tangled Skein Unravelling? In: Dale Givson (Hrsg.) Aspects of Privacy Law. Toronto, Butterworths, 1980, S. 21-40.

Collingwood-Nash, Deanna & Smith, John B.: Interactive Home Media and Privacy. Prepared for the Office of Policy Planning, U.S. Federal Trade Commission, Washington, D.C, Collingwood Associates Inc., Januar 1981.

Federal Government Information Technology: Electronic Surveillance and Civil Liberties, Washington D.C., U.S. Congress, Office of Technology Assessment, OTA-CIT-293, October 1985.

Flaherty, David H. (ed.): Privacy and Data Protection: An International Bibliography. London, U.K., Mansell, 1984; Knowledge Industry Publications Inc., 1984.

Flaherty, David H.: Protecting Privacy in Two-Way Electronic Services. White Plains, New York, Knowledge Industry Publications Inc., 1985.

Flaherty, David H.: The Need for an American Privacy Protection Commission. Government Information Quarterly, I, 1984, S. 235-258.

Freedman, Warren: The Right of Privacy in the Computer Age. New York, Quorum Books, 1987.

Gardner, Sidney L. & White, Robin: New Technology and the Right of Privacy: State Responses to Federal Inaction. A Report to the New York State Consumer Protection Board. (Unveröffentlichter Entwurf, August 1982.

Greenawalt, Kent & Noam, Eli: Confidentiality Claims of Business Organizations. In: Harvey J. Goldschmid (Hrsg.): Business Disclosure: Government's Need to Know 378, 1979.

Hirshleifer, Jack: Privacy: Its Origin, Function, and Future. 9J. Legal Stud., 1980.

Hirshleifer, Jack: The Private and Social Value of Information and the Reward to Inventive Activity. 61 Am. Econ. Rev. 561, 1971.

Hixson, R.: Privacy in a Public Society. New York, Oxford University Press, 1987.

Katz, James E.: U.S. Telecommunications Privacy Policy. Telecommunications Policy, Dez. 1988.

Linowes, David E.: Privacy in America: Is Your Private Life in the Public Eye. Chicago, University of Illinois Press, 1989.

Marx, Gary T.: The Iron Fist and the Velvet Glove: Totalitarian Potentials Within Democratic Structures. In: James E. Short (Hrsg.): The Social Fabric: Dimensions and Issues. Sage Publications, Beverly Hills, CA., 1986.

Marx, Gary T.: Testimony before the Pennsylvania Utility Commission, Docket No. R-891200, PPUC vs. Bell of Pennsylvania, Mai 1989.

Marx, Gary T. & Sherizen, Sanford: Monitoring on the Job. Technology Review, Nov./Dez. 1986, S. 63-72.

McManus, Thomas E.: Telephone Transaction-Generated Information: Rights and Restrictions. Program of Information Resources Policy. Harvard University, August 1989.

Nadel, Mark S.: Rings of Privacy: Unsolicited Telephone Calls and the Right of Privacy. 4 Yale J. on Regulation, Nr. 1, Dez. 1986, S. 99-128.

Newpert Jr., John Paul: American Express: Service That Sells. Fortune Vol. 120, Nr. 12, 20. Nov. 1989, S. 82.

Noam, Eli & Greenawalt, Kent: Confidentiality Claims of Business Organizations. In: Harvey J. Goldschmid (Hrsg.): Business Disclosure: Government's Need to Know. McGraw-Hill, 1979, S. 378-412.

Posner, Richard: The Economics of Justice. Cambridge, MA., Harvard Univ. Press, 1981, S. 272.

Presidential Privacy Protection Study Commission, Personal Privacy in an Information Society, Juli 1977, Gov. Printing Office, #052-003-00395-3.

Prosser, William L.: Privacy. 48 California Law Review 383, 1960.

Roszak, T.: The Cult of Information. New York, Pantheon 1986.

Rule, James; McAdams, Douglas; Stearns, Linda; Uglow, David: The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies. New York, Elsevier North Holland Inc., 1980.

Seipp, David John: The Right to Privacy in American History, Cambridge, MA. Harvard Program on Information Resources Policy, 1978, S. 78-3.

Simmel, G.: The Sociology of Secrecy and of Secret Societies. 11 Am J. Soc. 441, 446, 450, 1906.

Smith, Glenn Chatmas: Constitutional to Give it Out? Caller Identification Technology and the Right to Informational Privacy. 37 UCLA Law Review 145, 1989.

Smith, Robert Ellis: Compilation of State & Federal Privacy Laws. Privacy Journal, Washington D.C., 1988.

Spence, A. Michael: Market Signaling. 1974.

Toth, Victor J.: Update on Telecom Privacy and Free Speech. Washington Perspective, Sept. 1989, S. 80-87.

Warren, Samuel & Brandeis, Louis D.: The Right of Privacy. 4 Harvard Law Review 193, 196, 1890

Weingarten, Fred W.: Information Technology and Privacy Trends in Products and Services. In: Invited Papers on Privacy: Law, Ethics, and Technology. Presented at the National Symposium in Personal Privacy and Information Technology. Washington D.C., American Bar Association, 1982, S. 15-26.

Westin, Alan F.: Privacy in Western Society: From the Age of Pericles to the American Republic. 44, Report to Assn. of Bar of City of N.Y., Spec. Comm. on Sci. and Law, 15. Feb. 1965.

Westin, Alan F.: Privacy and Freedom. New York, Atheneum, 1967, S. 7.

Westin, Alan F.: Home Information Systems: The Privacy Debate. Datamation XXVIII, Nr. 7, Juli 1982, S. 104.

Wicklein, John: Electronic Nightmare: The New Communications and Freedom. New York, The Viking Press, 1979, S. 145.