Ambivalenz von Vertrauen

bei der Sicherung von „Privacy“ in elektronischen Räumen

Rainer Kuhlen

Informationswissenschaft – Universität Konstanz

Wirtschaftsethische Fragen der E-Economy

15.-17 November 2001

Stuttgart (IBZ)

Vertrauen – Faktoren des Vertrauensmanagement

Situationen von Unsicherheit in elektronischen Räumen

Erweiterungen im Privacy-Begriff

Vertrauenssicherung für Privacy

Lösungsansätze für Vertrauenssicherung für Privacy

Konsequenzen

Vertrauen – Faktoren des Vertrauensmanagement

Situationen von Unsicherheit in elektronischen Räumen

Erweiterungen im Privacy-Begriff

Vertrauenssicherung für Privacy

Lösungsansätze für Vertrauenssicherung für Privacy

Konsequenzen

Vertrauen – Vertrauensmanagement

notwendige Marketing-Massnahme der Informationswirtschaft
oder
Recht auf Sicherung persönlicher Grundrechte als Erbe der bürgerlichen Emanzipation

Vertrauen - Wettbewerbs- und Akzeptanzfaktor

Alle Studien zum elektronischen Handel stellen heraus, dass **mangelndes Vertrauen in Aktionen und Transaktionen** auf elektronischen Märkten als wichtigster Grund dafür eingeschätzt wird, die Dienste der Informationswirtschaft bzw. aller Anbieter nicht oder nur eingeschränkt zu nutzen.

Vertrauen bzw. vertrauensbildende Maßnahmen werden zu einem **Wettbewerbsfaktor in der Wirtschaft** und sind Voraussetzung zur Akzeptanz jeden Dienstes in elektronischen Informationsräumen

Vertrauen ist auch eine Funktion von Privacy-Sicherung

Faktoren der Vertrauensbildung

- ontologische Sicherheit durch Primäre[illegible]ung
- bislang gemachte persönliche Erfahrungen
- öffentlich dominante Wertesysteme
- implementierte und durchgesetzte Rechtssysteme
- Grundvertrauen in Technik
- Verfügung über institutionelle Sicherungsinstanzen,
- Medienöffentlichkeit
- Öffentlichkeitsarbeit der Anbieter
- Bedeutung von access points
- Vertrauen in Experten als Ersatz für fehlendes Wissen
- Image von Repräsentationsfiguren
- geglückte Ersatzhandlungen über (selber gar nicht kompetente) Vertrauensmittler
- Institutionelle Vertrauensmittler (trust center)
- Sicherung über (transparente) Software
- individuelle oder soziale Vertrauensnetze (web of trust)

Rainer Kuhlen: Die Konsequenzen von Informa--tionsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden? Suhrkamp Taschenbuch Wissenschaft 1443 Frankfurt 1999

Situationen der Unsicherheit in elektronischen Informationsräumen

Vertrauen und Unsicherheit

Vertrauen ist in Situationen der Unsicherheit vonnöten, wenn wir uns also auf Personen oder Systeme einlassen wollen oder müssen, über deren Verläßlichkeit wir uns keine Gewissheit verschaffen können.

Vertrauen kompensiert fehlende Gewißheit

Wird eine Situation sicher beherrscht, ist kein Vertrauen erforderlich.

Situationen der Unsicherheit - Übersicht

- Suchmaschinen
- Qualität
- kommerzielle oder freie Nutzung von öffentlicher Information - Schutz des geistigen Eigentums
- Authentizität
- Filtern, Blocken, Rating
- Transaktionen
- Software-Agenten
- Privacy: Interaktionsdaten

Privacy – aktive Kontrolle

In dem konstruktiven Verständnis von Access control bedeutet ***Privacy*** nicht das (passive) Recht, in Ruhe gelassen zu werden, sondern die (aktive) Kontrolle über die in der Kommunikation (auch in der *elektronischen* Interaktion) abgegebenen persönlichen Daten.

Weiterhin gehört nach dieser konstruktiven Bestimmung von ***Privacy*** als ***Access control*** nicht nur die Kontrolle über die ***abgegebenen*** Daten, sondern auch die Kontrolle über die ***eingehenden*** Daten und die Kontrolle über die auf Märkten zum Einsatz kommenden **Filterverfahren**.

Klassische Privacy-Bestimmung

‚the right to be let alone'« (Warren/Brandeis aus dem Jahre 1890)

steht das im Widerspruch zur grundsätzlich kommunikativen Struktur elektronischer Märkte oder zu der Grundidee offener Gesellschaften?

radikaler:

ist der Privacy-Begriff nicht ein (obsoletes) Überbleibsel der an individualistischen Prinzipien orientierten bürgerlichen Gesellschaft, der nicht mit den Rahmenbedingungen vernetzter kooperativer elektronischer Räume kompatibel ist?

Situationen der Unsicherheit – Interaktionsdaten

Ein besonders vertrauenskritischer Bereich ist gegenwärtig die Unsicherheit über die Verwendung von Interaktionsdaten, die beim elektronischen Handel abgegeben werden

Access control

Das Problem des Mißbrauchs von Datenspuren bringt in die seit den 60er Jahren intensiv geführte Datenschutz-Debatte eine neue Dimension ein.

»Privacy can be defined as a capability to determine what one wants to reveal and how accessible one wants to be« (Bellotti 1997, S. 89)

Privacy: Informationelle Selbstbestimmung

"Damit wird deutlich, daß der Zugang zu Informationen und der Schutz von Informationen zwei Seiten derselben Medaille darstellen ... **Informationelle Selbstbestimmung hat nicht nur abwehrrechtliche Funktion, sondern auch Zugriffssicherung**, um das Leben frei und selbstverantwortlich gestalten zu können."

Informationelle Selbstbestimmung = Datenschutz + Sicherstellung des Informationszugangs + Kontrolle der Informationsflüsse

Eckwerte-Papier der SPD-Bundestagsfraktion zu einem "modernen Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft" (Ute Vogt und Jörg Tauss Anfang 1999)

Ambivalenz von Datenschutz/Privacy

Personenbezogene Daten sind eine Ware, wie jede andere auch, und sie können dementsprechend als Ware behandelt werden. Will jemand die Kontrolle über seine eigenen personenbezogenen Daten behalten, so muß er die Daten erwerben.

ist auch Position für geistiges Eigentum/Urheberrecht

eher US-Position

Personenbezogene Daten gehören der jeweiligen Person und müssen als deren Eigentum geschützt werden (Datenschutz). Ein Individuum kann der Benutzung seiner Daten zustimmen oder die Benutzung verbieten.

ist auch Position für geistiges Eigentum/Urheberrecht

eher europäische/ deutsche Position

Privacy-Ansprüche – informationelle Selbstbestimmung

Respekt vor den persönlichen Daten anderer: Jedes Datum, das auf eine Person referenziert werden kann, ist ein persönliches Datum.

- Offenlegung der Privacy-Politik, insbesondere Transparenz bezüglich der Verwendung

- Nicht-Weitergabe erhobener Interaktionsdaten
- Möglichkeit, seine persönlichen Daten einzusehen
- Möglichkeiten, seine persönlichen Daten löschen zu lassen

Vertrauenssicherung für Privacy eine Funktion von Zeit?

Hypothese **Cheskin-Study:** Vertrauenswürdigkeit wächst mit der Zeit

Ecommerce Trust Study Cheskin Research 11/99:
http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf

Gegenhypothese/ **Jarvenpaa et al**: Skepsis bis Mißtrauen wächst mit größerer Erfahrung mit elektronischen Diensten (und ist kulturabhängig)

Jarvenpaa, Tractinsky, Saarinen et Vitale, Consumer Trust in an Internet Store : A Cross-Cultural Validation, 2 mai 2001, p. 2
(http://www.ascusc.org/jcmc/vol5/issue2/jarvenpaa.html)

Wer sichert Vertrauen für Privacy?

Gesichert: Mißtrauen bei wiederholtem Mißbrauch persönlicher Interaktionsdaten und bei fortgesetzter Verletzung von Privacy läßt eine pathologische Kunden-/Anbieter-Beziehung entstehen, mit der elektronische Publikumsmärkte nicht realisiert werden können.

Privacy is a precondition for trust – an attitude developed on the basis of situational or experiential factors. Trust affects privacy. A user's trust in the information practices of a system is likely to make possible consensual surveillance which can enhance trust. The resultant spiral will lead to stable and productive customer relationships

Samarajiva 1997, S. 284

Welche Lösungsansätze?

Welche Lösungsansätze?

Modell - Lessig – Spinello:

Law – Code – Market - Norms

- **Institutionalisierte Normen (Konventionen, Deklarationen)**
- **Staat – Überstaatliche Organisationen**
- **Softwarelösungen**
- **Sicherung über Verfahren**
- **Trusted third parties: institutionell: Trust center**
- **Trusted third parties: Vertrauensnetzwerke**
- **Trusted third parties: Selbstregulierung der Wirtschaft**
- **organisierte Koregulierung**

Institutionelle Privacy-Sicherung: Staat

Staat bzw. zwischenstaatliche Organisationen werden in seinen Institutionen kaum als der selbstverständliche Partner für die Vertrauensbildung in Funktionstüchtigkeit, Freizügigkeit und Privacy-Sicherheit der Netzkommunikation angesehen, dennoch:

Deutschland: IuKDG, Teledienstedatenschutzgesetz, Telekommunikationsgesetz Telekommunikationsdatenschutz-verordnung, Die **Bundesregierung** hat am 14. Juni 2000 den Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze beschlossen.

Europäische Richtlinien: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

Council of Europe (1981) Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data: http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt

U.S. Department of Commerce: Draft International Safe Harbor Privacy Principles.

Internationale Datenschutzempfehlungen:

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

UNO: Richtlinien betreffend personenbezogene Daten in automatisierten Dateien (14.12.1990).

Privacy-Sicherung über normative Grundlagen internationaler Normen

- Allgemeine Erklärung der Menschenrechte (III) vom 10.12.1948 (UN)
- Europäische Menschenrechtskonvention (E
- UNESCO – Infoethics Ro
- Okinawa Charter on Global Information So
- Charta der Grundrechte der Europäischen Union
- United Nations Millennium Declaration von 2000

UNESCO-Infoethics: We consider that among the most urgent problems in this context are those of freedom of access and personal privacy ... Privacy is one of the most threatened values and needs special protection in the electronic world.
Rec. 1 promote and defend freedom of expression and privacy protection in cyberspace as well as in traditional media

Okinawa: Development of effective and meaningful privacy protection for consumers, as well as protection of privacy in processing personal data, while safeguarding the free flow of information (7)

UN Artikel 12 Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

EU-Charta - Artikel 7
Achtung des Privat- und Familienlebens
Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Privacy-Sicherung über Software – P3P

The Platform for Privacy Preferences Project (P3P) - World Wide Web Consortium

- an **industry standard** providing a simple, automated way for users to gain more **control** over the use of personal information on Web sites they visit.
- presents a clear snapshot of **how a site handles personal information** about its users.
- P3P-enabled Web sites make this information available in a **standard**, machine-readable format.
- P3P enabled browsers can "read" this snapshot automatically and compare it to the **consumer's own set of privacy preferences**.
- P3P enhances **user control** by putting **privacy policies** where users can find them, in a form users can understand, and, most importantly, enables users to act on what they see.

Privacy-Sicherung über Software – P3P

Nine aspects of online privacy are covered by P3P. Five topics detail the data being tracked by the site.

Who is **collecting** this data?
Exactly **what information** is being collected?
For what **purposes**?
Which information is being **shared** with others?
And **who** are these data **recipients**?

The remaining four topics explain the site's internal privacy policies.

Can users make **changes** in how their data is used?
How are disputes **resolved**?
What is the **policy for retaining data**?
And finally, **where** can the detailed policies be found in "human readable" form?

Privacy-Sicherung über Software – P3P

Kritik an P3P aus deutsche Datenschutzsicht (Rossnagel)

http://www.emr-sb.de/news/jtg-p3p.pdf

Vom deutschen Datenschutzrecht her gesehen verbessert P3P nur die **Transparenz der Datenverarbeitung und bietet keine Unterstützung des Systemdatenschutzes**, der Zweckbindung und der Nutzerrechte. Insbesondere werden folgende Anforderungen nicht unterstützt und müssen auf andere Weise gewährleistet werden:

•P3P macht keine Aussagen über das Verhalten eines Dienstes, wenn ein Nutzer in eine vorgeschlagene Policy **nicht einwilligt**. Nach § 3 Abs. 4 TDDSG und § 12 Abs. 5 MDStV darf ein Diensteanbieter einen Nutzer nicht von einem Dienst ausschließen, wenn diesem Nutzer kein anderer Zugang „zu diesen Telediensten“ überhaupt oder in zumutbarer Weise möglich ist.
•Weder die **Authentifizierung** der Policy noch die elektronische Einwilligung des Nutzers ist vorgesehen, schon gar nicht in der von § 3 Abs. 7 TDDSG und § 12 Abs. 8 MDStV geforderten Art und Weise.

Privacy-Sicherung über Software – P3P

Kritik an P3P aus EU-Datenschutzsicht

http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp11de.pdf

Eine **technische Plattform** für den Schutz der Privatsphäre wird per se **nicht ausreichen**, um die Privatsphäre im Netz zu schützen. Sie muß im Zusammenhang mit einem **Rahmen verbindlicher Datenschutzbestimmungen** Anwendung finden, der für alle Individuen ein Minimum an nichtverhandelbarem Datenschutz vorsieht.

Die Verwendung von P3P ... in Ermangelung eines derartigen Rahmens bringt die Gefahr mit sich, die **Verantwortung für den eigenen Schutz vordringlich dem einzelnen Nutzer zuzuschieben**, und diese Entwicklung würde den weltweit eingeführten Grundsatz untergraben, demzufolge der Dateiverantwortliche für die Einhaltung der Grundsätze des Datenschutzes zuständig ist (OECD-Leitlinien 1980, Überein-kommen Nr. 108 des Europarats aus dem Jahre 1981, VN-Leitlinien 1990, EU-Richtlinien 95/46/EG und 97/66/EG).

Eine derartige Umkehrung der Zuständigkeit setzt außerdem einen Kenntnisstand im Hinblick auf die Gefahren voraus, die die Datenverarbeitung für die Privatsphäre des Individuums nach sich zieht, der realistischerweise von den meisten Bürgern **nicht erwartet** werden kann.

Vertrauens-/Privacy-Sicherung über Verfahren/Institutionen der Informationswirtschaft

- D21-Initiative
- TRUSTe
- VeriSign
- WebTrust
- GlobalSign

Vertrauens-/Privacy-Sicherung über Verfahren/Institutionen der Informationswirtschaft

D21-Initiative

D21 – Qualitätskriterien für Internet-Angebote (im B2C-Bereich): Um die wirtschaftlichen Chancen des E-Commerce auszuschöpfen, muss ... beim Verbraucher die Unsicherheit über die rechtlichen Bestimmungen und die Angst vor Betrug und Datenmissbrauch abgebaut werden. Vertrauen durch Transparenz, Verlässlichkeit und Glaubwürdigkeit sind die entscheidenden Voraussetzungen für eine breite Akzeptanz des elektronischen Handels.

- Anbieterkennzeichnung
- Preisinformation
- Vertragsbedingungen
- Leistungserbringung/Lieferung
- Widerruf und Rückgabe
- **Datenschutz/Privacy**
- Beschwerde und alternative Streitschlichtungsverfahren
- Gütezeichen

Vertrauens-/Privacy-Sicherung über Verfahren/Institutionen der Informationswirtschaft

◆WebTrust: http://www.webtrust.org/

Eine Initiative des American Institute of Certified Public Accountants:

WebTrust identifies and helps to reduce e-Commerce business risks and encourages online confidence and activity. Performed by CPAs and their equivalents worldwide, WebTrust can:

◆Identify risks, including possible privacy breaches, security gaps, and other systems affecting the customer interface

◆Benchmark and encourage best practices

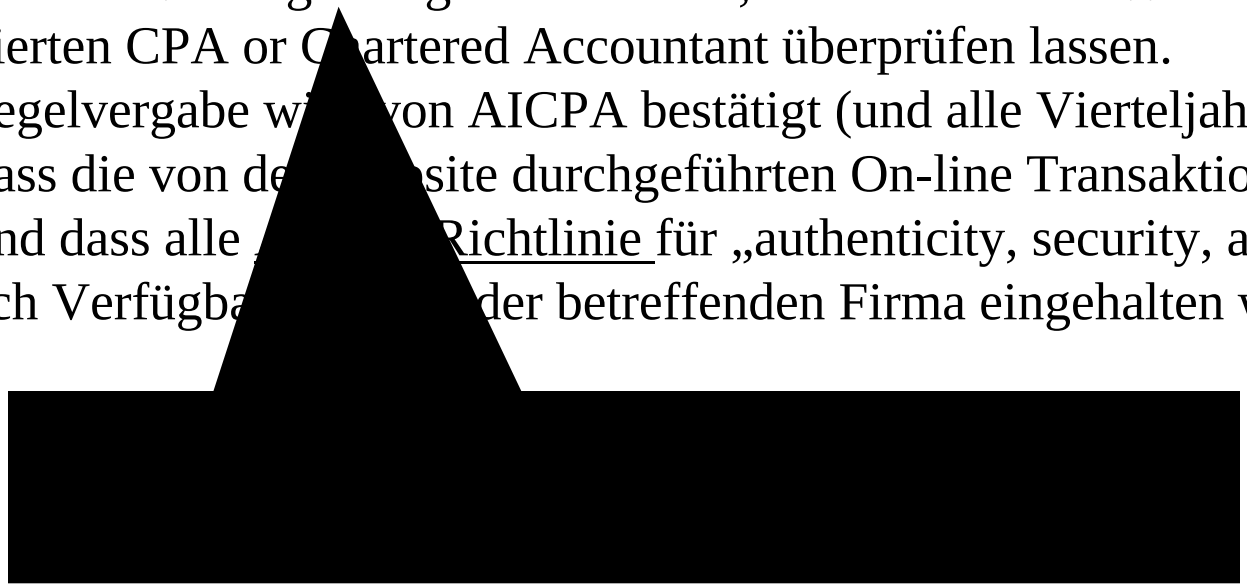
◆Provide independent verification that the site complies with the international WebTrust Standards for e-Commerce.

Vertrauens-/Privacy-Sicherung über Verfahren/Institutionen der Informationswirtschaft

WebTrust: American Institute of Certified Public Accountants http://www.cpawebtrust.org/ und des Canadian Institute of Chartered Accountants (CICA) – **Selbstregulierung über Verbände und Wirtschaft**

Ist eine Initiative von VeriSign: http://www.verisign.com/webtrust/index.html
Das Siegel wird ergänzt durch die von VEriSign vergebene Digital ID.

Um das WebTRust/VeriSign-Siegel zu erhalten, muss man seine Website von einem lizensierten CPA or Chartered Accountant überprüfen lassen.
Durch die Siegelvergabe wird von AICPA bestätigt (und alle Vierteljahr überprüft), dass die von der Website durchgeführten On-line Transaktionen sicher sind und dass alle Richtlinie für „authenticity, security, and privacy“ (auch Verfügbarkeit) der betreffenden Firma eingehalten werden.



Privacy-Sicherung über „NGO/Netizen“-Verfahren

- Customer Internet Privacy Statement: Global Electronic Commerce, LLC
- EFF´s 12 Ways to Protect your Online Privacy: http://www.eff.org/pub/Privacy/eff_privacy_top_12.html
- Anonymizer Privacy Services: http://www.anonymizer.com/
- CDMA Code of Ethics & Standards of Practice: Protection of Personal Privacy: http://www.cdma.org/privacy/ethics.html
- Cyber Pass: http://www.cyberpass.net/ („Home of Anonymity on the Web“)
- Idzap.com: http://www.idzap.net/ mit den Diensten: Free Anonymous Browsing, IDsecure Browsing, Anonymous Web Hosting, Web hosting with your domain name
- Rewebber: http://www.rewebber.com/: Anonymes Browsing

Privacy-Sicherung über „NGO/Netizen“-Verfahren

EFF´s 12 Ways to Protect your Online Privacy

1) Do not reveal personal information inadvertently
2) Turn on cookie notices in your Web browser, and/or use cookie management software or infomediaries
3) Keep a "clean" e-mail address
4) Don't reveal personal details to strangers or just-met "friends„
5) Realize you may be monitored at work, avoid sending highly personal e-mail to mailing lists, and keep sensitive files on your home computer
6) Beware sites that offer some sort of reward or prize in exchange for your contact or other information
7) Do not reply to spammers, for any reason
8) Be conscious of Web security
9) Be conscious of home computer security
10) Examine privacy policies and seals
11) Remember that YOU decide what information about yourself to reveal, when, why, and to whom
12) Use encryption!

Privacy-Sicherung über „NGO/Netizen“-Verfahren

Siegesoft

Siegesoft: http://www.siegesoft.com/_html/issue.asp?menuID=6&issueID=4
(ähnlich Panicware, Inc)

Surfing and Searching the Internet.

- I want to control what sites and content my child can view on the Internet.
- I want to avoid being identified and/or profiled while I surf/search the Internet.
- I want to prevent others who have access to my computer (ISP, boss, co-worker, family member etc.) from knowing where I go or what I do online.

Communicating (email, chat etc.) over the Internet.

- I want to keep my messages (email, instant messages, etc.) private and secure from interception.
- I do not want to receive unsolicited email (spam)
- I want to communicate in chatrooms, and discussion groups etc. without anyone knowing my real identity.
- I want to prevent others who may have access to my computer from reading my communication (email, etc).

Fazit

Konsequenzen

Grenzen der Vertrauenssicherung - Fragen

- Entlastet Vertrauen von unvermeidbaren Situationen informationeller Unsicherheit mit Blick auf Privacy?
- schafft Vertrauen Unmündigkeit, indem es aus dem Interesse Dritter, vor allem der Anbieter der Informationswirtschaft, auch dort reklamiert wird, wo eigentlich höchstes Mißtrauen angebracht wäre (Verwendung Interaktionsdaten)?
- Wie können wir sicher sein, daß Vertrauensmanagement nicht eine raffiniertere Form von Manipulation ist?
- Wie kann man den Vertrauen Zusichernden vertrauen: how to trust trust?
- Welche institutionellen Formen sind für Vertrauenssicherung und Regulierung von Privacy geeignet?

cont

Konsequenzen der Institutionalisierung des Vertrauensmanagement

Die Kosten für (vorbeugendes und erst Recht reparierendes) Vertrauensmanagement und für Privacy-Sicherung werden den Kosten für die Erstellung von Informationsgütern/-diensten vergleichbar sein.

Bei allen Institutionen in elektronischen Informationsräumen muss Vertrauensmanagement und Privacy-Sicherung als Teil des sozialen Informationsmarketing integriert werden.

Verfahren der Privacy-Sicherung sollten auf Prinzipien der organisierten Koregulierung beruhen.

Vielen Dank

für Ihre

Aufmerksamkeit!

Zusätzliche Folien zu **Situationen von Unsicherheit** als Ausgang für den Bedarf nach Vertrauenssicherung

Situationen der Unsicherheit - Suchmaschinen

- Nicht den Deckungsgrad der referenzierten/indexierten Information abschätzen, also keine Aussage über Recall der nachgewiesenen Treffer machen zu können.
- Nicht in der Lage zu sein, die Kriterien für das Ranking der nachgewiesenen Treffer nachvollziehen zu können.
- Bei unzureichender Referenzierung kaum in der Lage zu sein, valide Information von beliebiger unterscheiden zu können.

Situationen der Unsicherheit - Qualität

- Unsicherheit über die Qualität/Validität (Wahrheitswert und Handlungsrelevanz) der aus elektronischen Diensten, z.B. Fachinformationssystemen, Online-Datenbanken, Such- oder Surfmaschinen, erarbeiteten Informationen.

Situationen der Unsicherheit - Qualität

- Ist der Auftritt des Angebots/der Site professionell?
- Macht die Informationsarchitektur Sinn?
- Kann man in der Site leicht und schnell navigieren?
- Kann die Site leicht benutzt werden?
- Sind die Preise vernünftig bzw. nachvollziehbar?
- Image des Produktes
- Vertrauen andere Leute der Site bzw. den Produkten oder den Anbietern?
- Reputation der Anbieter: ist der Anbieter bekannt und vertraut
- Absicherung/Qualitätskontrolle durch neutrale Dritte und durch Referenzen
- Sind Feedback-Möglichkeiten, auch FAQ, Gästebücher etc geben?
- Kommen Auditing-Techniken zum Einsatz?

Situationen der Unsicherheit – geistiges Eigentum

- Unsicherheit über den Schutz des geistigen Eigentums in der elektronischen Verbreitung von Information bzw. – als Kehrseite der Medaille - Verunsicherung über das Ausmaß der kommerziellen Nutzung von öffentlicher Information aus Kultur, Politik/Verwaltung und Wissenschaft.

Situationen der Unsicherheit – intelligente Assistenten

Es ist zu erwarten, daß auf immer mehr Gebieten mobile und autonome Software-Agenten über die bloßen *Shopping*-/Preisvergleich-Assistenten hinaus von der Informationswirtschaft entwickelt und eingesetzt werden.

Unsicherheit über die Konsequenzen der Delegation von Informationsarbeit an intelligente Softwareagenten

Situationen der Unsicherheit – intelligente Assistenten

Der Eingriff der Software-Agenten in unsere Informationsautonomie wird weitergehend sein, als wir es jetzt schon von den personalen und bisherigen technischen Informationsassistenten gewohnt sind.

Software-Agenten-Technologie ist für den Laien noch schwieriger zu durchschauen als die der gegenwärtigen Suchmaschinen

Situationen der Unsicherheit – Transaktionssicherheit

- Unsicherheit über die Sicherheit (Authentizität) der elektronisch durchgeführten Transaktionen, z.B. Bestellen, Bezahlen, Ausliefern

Problematik der Anwendung, der Sicherheit und der Überwachung von Kryptographieverfahren, vor allem zur Verwendung von digitalen Signaturen

Situationen der Unsicherheit – Transaktionssicherheit

- Werden Verschlüsselungs-techniken angewendet?
- Sind die Transaktionen transparent?
- Kann man jederzeit aus einer laufenden Transaktion aussteigen?
- Sind Logistik, Auslieferungs-verfahren transparent (Tracing)?
- Welche institutionellen Absicherungen der Transaktionen kommen zum Einsatz
- Welche Verfahren der Identitätssicherung
- Welche Verfahren der Authentizität
- Welche Sicherungsverfahren für Zugriff (Passwort etc.)
- Wie wird der After-Sales-Service betrieben?

Situationen der Unsicherheit – Abblocken

- Schwierigkeit, mit der Vielzahl unerwünschter oder sogar als feindlich oder schädlich empfundener Informationen, die über die Netze einströmen, fertig werden zu können

Kinderpornographie, Gewalt, Probleme des Spamming und Problematik des Abblockens durch entsprechende Blocking-Software