Diplomarbeit
Electronic Privacy Management

Eingereicht von

Vladimira Ioveva

Studienkennzahl: J151

Matrikelnummer: 9752159

Diplomarbeit

am Institut für Informationswirtschaft

WIRTSCHAFTSUNIVERSITÄT Wien

Studienrichtung: Betriebswirtschaft

Betreuer: Dipl.-Ing. Mag. Dr. Albert Weichselbraun

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

AIM	AOL instant messenger.
Browser	Client-Programm zur Benutzung eines Datensystems (beispielsweise Webbrowser für das World Wide Web).
B2C	Abkürzung für Business to Customer = Privatkundengeschäft.
COPPA	Children's Online Privacy Protection Act = Gesetz zum Schutz der Privatsphäre von Kunden im Internet.
Cookies	Cookies sind kleine Textdateien, die die Webseite auf der Festplatte des Computers speichert. Sie enthalten z. B. Informationen über das spezifische Verhalten des Benutzers und seine Interessen. Sie verwalten Zustandsinformationen, wenn Benutzer verschiedene Seiten auf einer Webseite durchsuchen und später zu der Webseite zurückgehen. Das hilft der Webseite, die Ansicht für den nächsten Besuch des Benutzers anzupassen.
CMU	Carnegie Mellon Universität.
CRM	Customer Relationship Management. Das ist ein Verfahren, bei dem Kunden gezielt angesprochen und ans Unternehmen gebunden werden, vorhandene Kundenbeziehungen werden weiter gepflegt und ausgebaut, um die Wettbewerbsfähigkeit des Unternehmens zu steigern.
CPO	Die englische Abkürzung für Chief Privacy Officer = Privacy Chef.
Data Mining	Das Suchen nach Relationen und Mustern in großen Datenbanken, ohne von vornherein irgendwelche mögliche Relationen definiert zu haben.
DSG	Datenschutzgesetz.
DS-RL	Datenschutzrichtlinie.

ECG	Electronic-Commerce-Gesetz.
FTC	Federal Trade Commission: überwacht die Einhaltung des fairen Wettbewerbs im Internet (nicht nur). Sie stellt das Funktionieren eines konkurrenzbestimmten Marktes sicher, kann aber nicht auf Betreiben einer Privatperson einschreiten.
HTML	HyperText Markup Language ist eine textbasierte Auszeichnungssprache zur Strukturierung von Inhalten wie Texten, Bildern und Hyperlinks in Dokumenten. HTML-Dokumente sind die Grundlage des World Wide Web.
IE	Microsoft Internet Explorer.
IP-Adresse	Nummer, über die jeder Rechner im Netz zu erreichen und eindeutig identifizierbar ist. Sie besteht aus vier, durch Punkte getrennten, dezimalen Ziffern zwischen 0 und 255.
ISP	Abkürzung für „INTERNET Service Provider“.
Listbroker	Das sind Personen, die systematisch Informationen zu bestimmten Personen oder Unternehmen zusammenstellen. Dazu benötigt man Know-how über betriebswirtschaftliche Bedürfnisse und die Funktionszusammenhänge des Internets.
MUD	„Multiuser Dungeon“: ein virtueller Platz zum Spielen, der ein textbasiertes Spielmedium benutzt.
ÖDSG	Österreichisches Datenschutzgesetz.
P3P	Abkürzung für „Plattform for Privacy Preferences“: Protokoll, über das maschinenlesbare Datenschutzerklärungen ausgetauscht werden.
PETs	Abkürzung für Privacy Enhancing Technologies.

Phishing	Das Wort kommt vom Wort „fishing“ (fischen/angeln) und „password“ und ist einer der technischen Entwicklung angepasster Form von „Bankraubs“. Der Täter versucht durch eine gefälschte E-mail vertrauliche Informationen wie Zugangsdaten und Passwörter zu bekommen.
PIN	Persönliche Identifikationsnummer.
PII	Abkürzung für Personally Identifiable Information: jede personenbezogene Information, die uns identifiziert und der Website erlaubt, mit uns Kontakt aufzunehmen. Solche Daten können zum Beispiel der Name, die E-Mail Adresse und die Telefonnummer sein.
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung (in Deutschland).
Scoring	Ein automatisches Vorurteilungssystem. Durch eine Kombination einer Vielzahl von persönlichen Daten (Alter, Stadt, Adresse, Nachbarschaft, Anzahl Umzüge u. a) wird eine Bewertung der Kreditwürdigkeit einer Person mittels einer Zahl (Score) ermittelt.
SMS	Short Message Service“, Textnachricht mit begrenzter Anzahl von Zeichen (i.d.R. um 160 Zeichen), die via Handy oder Internet an ein Handy geschickt werden kann. Die empfangene Nachricht kann auf dem Display des Handys gelesen werden.
SPAM	Abkürzung von „Spiced Pork and Ham“ oder später als Spam-Send Phänomenal Amount of Mail“ = unaufgeforderte, unerwünschte E-Mails.
Spamming	Massenhafte Sendung unerwünschter Werbe-Emails.
Spearing	Spearing (Spear-Phishing) ist eine gezielte Phishing-Attacke, bei denen einzelne, ausgewählte Benutzer adressiert werden (z. B. vom Namen eines Personalchefs des Benutzers), um vertrauenswürdige Informationen wie Benutzername und Passwort zu erhalten.

TAN	Eine Transaktionsnummer, die im elektronischen Bankengeschäft (Online-Banking) benötigt wird.
UCE	“Unsolicited Commercial E-Mail” = Spamming.
UCM	„Unsolicited Commercial E-Mail“= Spam.
VoIP	Unter Voice over IP bzw. IP-Telefonie versteht man das Telefonieren über Computernetzwerke.
Web-Browser	Programm zur Kommunikation im World Wide Web auf der Ebene des Users (Web-Client).
W3W	World Wide Web Consortium.
XML	Extensive Markup Language = eine Metasprache für Dokumentbeschreibungen, die vom W3C (World Wide Web Consortium) betreut wird. Die Sprache ist strukturiert und maschinenlesbar.

Kapitel 1

1 Einleitung

„Privatsphäre ist wie Sauerstoff – man schätzt sie erst, wenn sie fehlt“ – John Emontspool

Wenn wir versuchen, einen Tag lang so wenig Datenspuren wie möglich zu hinterlassen, werden wir feststellen, dass dies fast unmöglich ist.

Im Zuge der Entwicklung der sogenannten Informationsgesellschaft eröffnen sich nicht nur für „Firmen neue, globale Vermarktungschancen, sondern auch den Einzelnen, Möglichkeiten der internationalen Informationsbeschaffung und auch neue Arten der Unterhaltung “ [CaPeJo00]. Diese ist aber nicht nur mit Chancen, sondern auch mit Risiken verbunden, nämlich mit der Bedrohung der Privatsphäre.

Zahlreiche Konsumentenbefragungen haben gezeigt, dass die Endbenutzer sehr beunruhigt in Bezug auf ihre Privatsphäre sind [Kob07].

In vielen Lebensbereichen hinterlassen Konsumenten Datenspuren, immer häufiger werden Daten gesammelt. Im Zuge der Inanspruchnahme von Dienstleistungen sind dem Endbenutzer die dahinter stehenden Datensammlungen meistens unbewusst [CaPeJo00].

1.1 Motivation

Ziel der Arbeit ist es daher die Chancen und die Risiken beim Sammeln, Speichern und der Weitergabe von personenbezogenen Daten im Internet aufzuzeigen. Führen diese seitens des Endbenutzers zu einem Verlust der Privatsphäre, sind die Risiken bei der Preisgabe von persönlichen Daten bekannt und was für Chancen eröffnen sich durch die enorme Datensammlung für Unternehmen?

Die rechtlichen Rahmenbedingungen für die Datensammlung helfen nicht immer Datenschutzansprüche international durchzusetzen, da diese mitunter recht problematisch sind. Daher ist es von besonderer Bedeutung, Privacy-Technologien, die sogenannten Privacy Enhancing Technologien einzuführen und die Harmonisierung und Verbesserung von E-Privacy-Politiken auf grenzüberschreitender Ebene zu lösen, um den komplexen Gesamtbereich „E-Privacy“ überhaupt managen zu können. Ein zuverlässiges Zugriffschutzsystem könnte dazu führen, dass Benutzer

erhöhte Bereitschaft zeigen, persönliche Informationen herauszugeben [Wörndl03].

Dadurch, dass die personenbezogenen Daten vom Unternehmen genutzt werden, stellt der Datenschutz einen Wettbewerbsfaktor dar. Je mehr die Unternehmen offen legen, wie sie die Daten nutzen werden, desto mehr Vertrauen genießen sie bei den KonsumentInnen und können so einen Wettbewerbsvorteil lukrieren [CaPeJo00].

Daher sind nicht nur die gesetzlichen Rahmenbedingungen wichtig, sondern auch transparente Privacy-Politiken, um Konsumenten vor Datenschutzmissbrauch zu schützen. Damit sich der Endbenutzer dem E-Commerce anvertraut, müssen die dargestellten E-Datenschutzerklärungen (Privacy Policy) auch eingehalten werden.

1.2 Aufbau der Arbeit

Im Anschluss an die Darstellung der konkreten Arbeitsproblemstellung und des Forschungsvorhabens der vorliegenden Diplomarbeit wird im **Kapitel 2 (Privacy, Datenschutz, informationelle Selbstbestimmung)** der Begriff „Privacy“ begriffsexplorativ bzw. differenzlogisch abgegrenzt. Hierbei wird nicht nur die genaue Definition des Terminus „Privacy“ erläutert, sondern auch retrospektiv die Veränderung der historischen Entwicklung der Privatsphäre im Laufe der Jahre bis hinauf zum heutigen Informationszeitalter dargestellt. Das Voranschreiten der Technik führt dazu, dass viele unterschiedliche Unternehmen und Personen die Lücken in den bestehenden Datenregelungen ausnutzen und beginnen personenbezogene Daten zu sammeln, mit dem Ziel, personenbezogene Profile zu erstellen. Daher werden im **Kapitel 3 (Datensammlung)** die einzelnen Interessensgruppen (Staat, Firmen und Spammer) genauer dargestellt und die Folgen der Datensammlung diskutiert. Damit der Privatsphäre ein Schutzrahmen geboten werden kann, werden die rechtlichen Bedingungen im **Kapitel 4 (Gesetzliche Rahmenbedingungen)**, nämlich die Privacy-Gesetze (Datenschutzgesetz und Telekommunikationsgesetz in Österreich), der Aufbau, die Ziele und die grundlegenden Begriffe dazu, sowie auch aktuelle Entwicklungen von Privacy-Gesetzen dargestellt. Es wird aufgezeigt, dass „Privacy“ immer mehr an internationaler Bedeutung gewinnt. Daher wird auf die Problematik der internationalen Harmonisierung der Privacy-Gesetze eingegangen. Die Grundsätze von OECD Richtlinien werden im

Rahmen des Forschungsprozesses dieser Arbeit ebenfalls dargestellt, da sie die Grundlage für alle Nationalgesetze bilden. Zudem geht der Erkenntnisfindungsprozess innerhalb dieser Arbeit, auch auf die Privacy-Situation in den Vereinigten Staaten von Amerika näher ein. Weiters beschäftigt sich dieser Arbeitsabschnitt auch mit E-Privacy und E-Commerce, wobei hier insbesondere die Grundbausteine der Privatsphäre (Anonymität, Vertraulichkeit, Transparenz, Vertrauen und Absicherung) näher betrachtet werden, sowie die Privacy-Situation im virtuellen Raum aus der Konsumenten- und Unternehmenssicht.

Dadurch, dass man schwierig eine ganzheitliche internationale Gesetzgebung durchsetzen kann, soll Privacy durch Technologien unterstützt werden. Im **Kapitel 5 (Privacy Enhancing Technologien)** werden daher die Privacy Enhancing Technologien im Allgemeinen dargestellt, die dazu führen sollen, dass das Privacyrisiko reduziert und das Vertrauen gegenüber Konsumenten erhöht wird. Diese Technologien sollen den Nutzern im Internet dabei helfen, kontrollieren zu können, was mit ihren personenbezogenen Daten passiert, wenn sie eine Webseite besuchen. Vor diesem Hintergrund benötigt man eine Privacy-Politik, die verständlich und durchsetzbar sein soll. Daher wurde von W3C[1] (World Wide Web Consortium) die technische Plattform zum Austausch von Datenschutzinformationen, „Plattform for Privacy Preferences Project“ (P3P), „A P3P Preference Exchange Language“ (APPEL) und „Enterprise Privacy Authorization Language“ (EPAL) entwickelt. Diese Zugriffsschutzmodelle insbesondere das Privacy Preferences Project (P3P) werden in diesem Kapitel näher beschrieben.

Hierbei wird insbesondere auch die Frage des Vertrauens der Benutzer geklärt. Wird dieses Vertrauen verstärkt, führt dies dazu, dass Konsumenten freiwillig mehr Informationen über sich preisgeben. Daher ist es notwendig, dass die Datenschutzerklärungen im Internet konsumentenfreundlicher sind und auch tatsächlich eingehalten werden. Daher beschäftigt sich dieser Teil der Arbeit mit der Bestimmung und dem Management der Privacy-Politik in einem Unternehmen und wie es möglich wird, dass die veröffentlichte Datenschutzerklärung auch bestimmten gesetzlichen Richtlinien entspricht. Es werden verschiedene Selbstregulierungsmaßnahmen erläutert wie die Non-Profit Organisationen TRUSTe und BBBOnLine (angeboten von Better Business Bureau), die „Gütesiegel“ anbieten, welchen einen Hinweis darauf bieten, dass gewisse Privacy-Mindeststandards eingehalten wer-

[1] http://www.w3c.org/.

den [CaPeJo00, S.23]. Es wird im Rahmen des Kapitels zudem aufgezeigt, was eine gute, standardisierte E-Privacy Politik ist und wie wichtig es ist, dass zwischen dem Benutzer und dem Unternehmen ein Vertrauen aufgebaut wird, sodass die Angabe persönlichen Informationen ohne Bedenken erfolgen kann.

Der darauffolgende Arbeitsteil **(Kapitel 6 Privacy–Missbrauch)** widmet sich den unterschiedlichen Fällen vom Privacy-Missbrauch. Es wird hierbei ein besonderes Augenmerk auf die Bedeutung von unerwünschten Werbe-E-Mails (SPAM) gelegt. Dieser Abschnitt betrachtet auch unterschiedliche Risiken bei den sozialen Netzwerken wie MySpace und Facebook.

Im letzten Teil der Arbeit **(Kapitel 7 Fallstudie)** werden aufgrund der dargestellten Sachverhalte Hypothesen gebildet, welche mittels eines Fragebogens verifiziert und anschließend **(Kapitel 8 Schlussfolgerung)** ausgewertet werden. Zudem werden alle relevanten Forschungserkenntnisse- und Ergebnisse der Arbeit noch einmal systematisch untereinander in Bezug gesetzt und einer reflektierten Analyse unterzogen. Überdies wird ein Ausblick auf mögliche zukünftige Entwicklungen gewährt.

Kapitel 2

2 Privacy, Datenschutz, informationelle Selbstbestimmung

Nachfolgend wird der Begriff „Privacy“ abgegrenzt, es wird die historische Entwicklung von der Entstehung der „Privacy“ bis hin zur Bedeutung des Terminus in der modernen Informations- und Kommunikationsgesellschaft verfolgt. Das Ziel dieses Kapitels ist es, die Grundbausteine und die Veränderung der E-Privacy im Laufe der Zeit aufzuzeigen, um die Idee der Sammlung und Auswertung von persönlichen Daten zu explizieren, und damit gleichzeitig den Bedarf von neuen Regelungen und Gesetzen zum Schutz persönlicher Daten ins Treffen zu führen.

2.1 Begriffsabgrenzung

“Every man should know that his conversations, his correspondence, and his personal life are private.“ Lyndon B. Johnson, President of the United States, 1963-1969

Debatten über den Schutz der Privatsphäre haben eine lange Geschichte. Schon 1361 fand sich im englischen Recht der „Justices of the Peace Act“, der das Belauschen und heimliches Beobachten anderer unter Strafe stellte [Lau03]. 1763 folgte der berühmte Ausspruch von William Pitt, seinerzeit Mitglied im englischen Parlament: “The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail – the storm may enter - the rain may enter - but the King of England cannot enter! – all his forces dare not cross the threshold of the ruined tenement! “[Bro39].

Die erste bekannte Definition vom deutschen Begriff „Privatsphäre“ (engl. “Privacy“) wird Mitte des 20. Jahrhunderts verwendet und geht auf den Schriftsteller und Rechtsanwalt Samuel D. Warren und den späteren Richter am Obersten Gerichtshof der USA Louis D. Brandeis zurück. In ihren bekannten Artikel „The Right to Privacy“ („Das Recht auf Privatsphäre“), veröffentlicht in Harvard Law Review 1890, bestimmen sie den Begriff folgendermaßen:

“...The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world… so that solitude and privacy have become more essential to the individual; but modern enterprise and invention

have, through invasion upon his privacy, subjected him to mental pain and distress far greater than could be inflicted by mere bodily injury" [WB1890].

Sie waren der Meinung, dass nicht nur die physische Beeinträchtigung von Rechtsgütern wie körperlicher Zwang, Entzug der Freiheit oder Eingriffe in das Eigentum von Bedeutung sind, sondern auch das Sammeln von Informationen, wobei dieser Begriff den beiden Autoren in der damaligen Zeit noch unbekannt war [Garstka].

Weiters definieren sie Privacy als das Recht in Ruhe gelassen zu werden („the right to be alone"). Der Grund dieser Veröffentlichung war, dass durch die Entwicklung von neuen Formen von Technologien die Privatheit bedroht schien. Die Fotografie und die Veröffentlichung von Bildern in Boulevard-Zeitungen zum Beispiel waren, nach Einsicht der Autoren, ein Angriff auf die persönliche Freiheit [Fischer01, 6].

Obwohl dieser Text viele Jahre zurückliegt, ist die Bedeutung der Privatheit (engl. Privacy) und ihre Verbesserung für das Individuum immer noch ein aktuelles Thema.

Nach Egger ist Privacy die Differenzierung der Person oder die Unterschiedlichkeit von Handlungsweisen in Bezug auf Gruppen von Personen [Egg93, 135]:

"Privacy in our common sense is strongly connected with the idea that there are some things another person should not be able to see or know."

Mit dem Voranschreiten der Informationstechnik scheint die Definition Warrens und Brandeis' Definition – „the right to be left alone"- kaum mehr praktikabel zu sein. Eine zeitgemäße Definition der „informationellen Privatheit" kommt von Alain Westing, einem US-amerikanischen Privacy-Forscher, der im Jahr 1967 aufgrund der zunehmenden Verbreitung von maschineller Informationsverarbeitung diese als Recht definiert, selbst zu bestimmen wie viel von unserer personenbezogenen Information für die anderen zugänglich sein soll [West70, 7]:

"Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others"

Westing definiert diese „Privacy"-Bestimmung, er gibt aber auch an, dass es überhaupt nicht möglich ist, eine abschließende Definition zu finden. "no definition of

privacy is possible, because privacy issues are fundamentally matters of values, interests, and power".

Das Recht auf Privatheit führt uns zu einem Zustand, „der es erlaubt, sich an einen sicheren Ort zurückzuziehen, an dem man vor unautorisierten Zutritt geschützt ist und welcher die Kontrolle über persönliche Daten gewährleistet" [Zehentner02]. Wichtig ist, dass der Benutzer jederzeit überwachen und bestimmen kann, welche persönlichen Daten wie verwendet werden, und keine Informationen ohne seine Zustimmung weitergegeben werden [Wörndl03]. Dieser Aspekt wird näher im Kapitel 5 Privacy Enhancing Technologien geschildert.

Im Allgemeinen gibt es drei verschiedene Aspekte oder Dimensionen von Privatheit [Rosen92]:

- *Territoriale Privatheit* (hier wird der physische Bereich einer Person geschützt, wie z. B. der Schutz der eigenen vier Wände, des Arbeitsplatzes oder des öffentlichen Raumes);
- *Privatheit des Individuums bzw. körperliche Privatheit* (hier wird die Person selbst geschützt, wie z. B. der unzulässige Eingriff auf Informationen, bei denen eine Person selbst verletzt wird, körperliche Untersuchungen etc.) und
- *Informationelle Privatheit* (hier werden die personenbezogenen Daten, gesammelt, aufbewahrt, bearbeitet, selektiv weiterverbreitet und geschützt).

Personenbezogene Daten („personally identifiable information") sind definiert als jede Information, die sich auf die persönliche oder materielle Situation einer Person bezieht [Fischer01, 6]. Das sind Informationen, aus denen man evtl. die Identität der Person ableiten kann, wie z. B. das Geburtsdatum eines Menschen.

Dadurch, dass sich das Internet immer mehr verbreitet und die Speicherung von personenbezogenen Daten immer häufiger wird, verändert sich auch die Dimension von Privacy, was mitunter auch sehr problematische Auswirkungen auf das Management der E-Privacy hat. Diese wird als „Information Privacy" bezeichnet und wie folgt definiert:

"Information Privacy refers to the claims of individuals that information about themselves should generally not be available to other individuals or organizations, and

that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use." [Cla99].

Es gewinnt eine neue Dimension der Privatsphäre an Bedeutung und zwar die der Kontrolle der Daten. Es geht nicht mehr darum, wie viel gesammelt, gespeichert und ausgewertet wurde, sondern die aktive Kontrolle von personenbezogenen Daten steht im Vordergrund.

Unter dem Recht auf **informationelle Selbstbestimmung** versteht man nach der Definition von Katsh das Recht zur Kontrolle von Informationen über einen selbst, sowie das Recht in Ruhe (alleine) gelassen zu werden [Schoe95; CaPeJo00, 5]. Der Begriff wird auch von dem Deutschen Bundesverfassungsgericht in Karlsruhe am 15. Dezember 1983 eingeführt. Jeder Bürger darf selbst bestimmen, " wie viele und welche Daten er an andere weitergeben will. Damit wird die Freiheit auf Selbstdarstellung realisiert, die davon ausgeht, dass jeder mündige Bürger ein Recht auf Individualität hat" [FCho96, 52].

Daher erfordert das Zeitalter elektronischer Massenkommunikation Kontrollmechanismen, die dem Individuum helfen, seine elektronischen Transaktionen zu verstehen und zu kontrollieren, inwieweit seine personenbezogenen Daten für andere identifizierbar und erreichbar sind [Braun00d][2].

Privacy (Zurückgezogenheit, Privatsphäre, Privatheit) kann auch als **Datenschutz** übersetzt werden. Mit dem Begriff „Datenschutz" ist hauptsächlich die rechtliche Bedeutung gemeint, welche nur einen Teil der Privatheit ausmacht [Wörndl03].

Der Anspruch auf Datenschutz ist nicht unabdingbares oder absolutes Recht, es unterliegt gesetzlicher Vorgaben, welche helfen, die Privatheit beim Sammeln, Speichern und der Weitergabe der personenbezogenen Daten zu schützen [Fischer01, 6]. Im Kapitel 4 wird wie bereits angesprochen näher auf die gesetzlichen Rahmenbedingungen eingegangen.

Die vorliegende Diplomarbeit konzentriert sich auf die informationelle Privatheit eines Individuums. Dadurch, dass die Begriffe „Privacy", „Privatheit", „Privatsphäre" oder „Datenschutz" in den verschiedenen Ländern unterschiedliche Dimensionen

[2] Siehe NETHICS. Portal zur Informationsethik: http://www.nethics.net/nethics_neu/n3/news/netznews.htm/.

annehmen und es keine einheitliche Definition gibt, werden sie hier als Synonyme verwendet.

2.2 Historische Entwicklung von Privacy

Die Entwicklungen in der Gesellschaft haben bewirkt, dass auch die Idee von Privacy nie statisch geblieben ist und sich mit einem schnellen Tempo weiterentwickelt.

Privat muss selbstverständlich als „nicht öffentlich“ verstanden werden.

Die Kategorie des Privaten, im Gegensatz zu der des Öffentlichen, hat ihren Ursprung im griechischen Stadtstaat, wo unterschieden wurde zwischen der Sphäre, die allen Bürgern gemeinsam ist (koine), und jener, die jedem einzelnen zusteht (idia). Schon Aristoteles hat 350 Jahre vor Christus in seinem Artikel „Politics“ zwischen den politischen Aktivitäten (polis), die von der Autonomie des Hausherrn abhängen und der Privatsphäre des Haushaltes (oikos), welche an das Haus gebunden ist, unterschieden. Die Privatheit habe eine hierarchische Struktur, die den Bürgern die reale Fähigkeit vermittelt, in einer öffentlichen Sphäre zu handeln. Nur wer privat materiell abgesichert ist, also keine existentiellen Nöte hat, kann frei für die Teilnahme am politischen Leben sein. Daher ist Privacy ein unabdingbares Mittel für die reibungslose Entwicklung der „Öffentlichkeit“ [SmSh07; FCho96, 47].

Privacy existierte schon bei den Griechen und Römern. Der “Römische Raum“ und die “Griechische Agora“ wurden dazu benutzt, öffentliche und gesetzliche Angelegenheiten zu diskutieren und jeder freie Mann konnte direkt am öffentlichen Leben teilnehmen.

Die Griechen haben ursprünglich nicht an eine Abgrenzung zwischen den zwei Sphären geglaubt. Die Lehre, das Individuum sei getrennt von der polis, wurde von den radikalen Sophisten im fünften Jahrhundert vor Christus auf der Griechischen Halbinsel eingeführt. Diese waren der Meinung, dass der Mensch ein Maßstab für alles sei – nicht die Stadt oder die Götter, wie dies die herrschende Philosophie lehrte [Sax83].

Diese Einsicht war völlig fremd und besonders radikal, setzte sich aber langsam innerhalb der griechischen Gesellschaft durch und wurde permanent von den großen griechischen Philosophen diskutiert. Zudem war diese Inspiration für Aristote-

les, der in seinem Trakt „Politics“ versuchte, zwischen den entgegensetzten Meinungen zu vermitteln.

Die Römer haben „Privacy“ vom „Public“ unterschieden. Der Begriff „Public“ war mit dem Wohl des Staates und seiner Souveränität gleichgestellt, während Privacy mit den Interessen des Individuums im Imperium verbunden war [Hab89; Weintraub97].

Dieser Gedanke war so fundamental verbreitet und von allen akzeptiert, dass es später im ersten Kapitel (der Gesetzessammlung „Corpus Iurius Civilis“, die Erfassung des Römischen Rechtes unter Kaiser Justinian im Jahr 533-534 n. Chr.) im Römischen Recht aufgenommen wurde [Weintraub97].

Im Mittelalter entwickelte sich die Idee von der Trennung von Staat und Individuum, Public und Privacy aus dem Volksbewusstsein heraus. In dieser Zeit konnte die Gesellschaft keinen signifikanten Unterschied zwischen public und privacy finden, grundsätzlich wegen des Feudalismus, der auf Loyalität und naher Verwandtschaft basierte – ein Netzwerk von persönlichen Eigenschaften, indem kein Unterschied zwischen Staat und Individuum gemacht wurde.

Eine neue Trennung der beiden Begriffe kam in der modernen Geschichte mit der Aufklärung und mit der Entwicklung des Kapitalismus, als zwischen Souveränität und Bürger differenziert wurde und sich eine allgemeine politische Gesellschaft entwickeln konnte.

In dieser Zeit stellte sich der Grundgedanke von Privacy langsam als ein konkreter menschlicher Wert heraus und begann als solcher zu wachsen. Mit dem Beginn des gesetzlichen Schutzes dieses wichtigen menschlichen Rechtes trat für die Privacy eine neue Ära an.

2.3 Privacy im Informationszeitalter

Die zunehmende Informatisierung der Gesellschaft ändert den Umgang mit der Privatheit kontinuierlich. Die Entwicklung der Computertechnik und die damit verbundenen technischen Möglichkeiten der Datenverarbeitung machen es notwendig, grundsätzliche Fragen nach dem Recht auf Privatsphäre zu stellen [Mähr99]. Es ist erstaunlich, wie viele von unseren personenbezogenen Informationen wir oftmals zielbewusst oder ohne es zu realisieren, preisgeben.

Gibt es überhaupt eine Privatheit oder sollen wir in Zukunft diese total aufgeben, indem wir zu „gläsernen Menschen“ werden? In einer Analyse unter dem Begriff „Insight for the Connected World“ (bei der es um „Emerging High-Impact Trends“ geht) schreibt die Gartner-Unternehmensberatung [MaLa01]:

“by 2010, driven by the improving capabilities of data analysis…privacy will become a meaningless concept in Western societies.”

Müssen wir dieser Aussage unwidersprochen hinnehmen oder gibt es Lösungsansätze, die verhindern, dass wir in eine totale Überwachungsstruktur geraten?

Nach Moor brauchen wir verschiedene „Zonen von Privacy“, um in verschiedenen Situationen den Zugang zu der von uns preisgegebenen Information zu kontrollieren. Er behauptet, dass Privacy eine Vereinigung von der Tatsache sei, dass der Begriff entweder die Kontrolle der preisgegebenen Information bedeutet oder die Bestimmung, wie viel wir von unseren Privatheit für andere zugänglich machen. Obwohl die Kontrolle über die gegebene Information erwünschenswert ist, ist es nach seiner Meinung nicht möglich, eine absolute Kontrolle zu erreichen [Moor97].

Benutzerbefragungen nach Kobsa [Kob07] zeigen, dass Computerbenutzer beunruhigt sind, wenn es um ihre eigene Privacy im Internet geht. Dort wird aufgezeigt, dass 80% von ihnen an der Wahrung ihrer Anonymität interessiert sind. Weiters finden sie wichtig, zu wissen, wie ihre persönliche Information benutzt wird, und stimmen darüber ein, dass die Kontrolle der Benutzung ihrer Information wichtig ist. 94% wollen das Recht haben, zu wissen, was die Betreiber von Webseiten über sie wissen. In einer anderen Befragung von Kobsa [Kob07b] geben 63% von den Befragten an, falsche Information über sich selbst anzugeben oder es überhaupt abzulehnen, irgendwelche personenbezogene Information preiszugeben. Sie wären mit der Veröffentlichung der notwenigen Information im Internet einverstanden, wenn die Seite vorher umfassend darüber informiert, was mit ihren preisgegebenen Daten passiert, vorausgesetzt, dass sie mit den Bedingungen einverstanden sind.

Moors These basiert darauf, dass sich das Individuum tatsächlich an der personenbezogenen Information bzw. Privacy im Informationszeitalter interessiert. Aber nicht jeder glaubt an diese tatsächliche Privacy. Ein wichtiger Punkt ist, dass, obwohl viele Benutzer über ihre Privacy beunruhigt sind, diese ohne zu zögern, ihre persönliche Information im Internet preisgeben. Deswegen lässt sich schließen,

dass die Beibehaltung der Privatsphäre der Benutzer nicht so wichtig sei, obwohl sie das Gegenteil behaupten und daher entsprechende Bedenken problemlos ignoriert werden können [Smith07].

Um die Situation genauer zu erforschen, befragten Ackerman, Cranor und Reagle eine Zahl von Internetbenutzern in Amerika. Sie zeichneten deren Internetaktivitäten auf und analysierten diese anschließend [AckCraRea99]. Die Ergebnisse zeigten, dass die Personen ein hohes Interesse an ihre Privacy haben und ganz anders reagieren, wenn sie sich mit der realen Online-Situation auseinandersetzen. Aufgrund dieser Erkenntnis teilte die Forschen die Benutzer in drei Grundkategorien ein: Privacy Fundamentalisten (privacy fundamentalists), die Pragmatiker, die die Mehrzahl ausmachen (pragmatic majority) und jene, die nur wenig Interesse an ihre Privacy daran haben („marginally concerned“).

Die Privacy-Fundamentalisten, die 17% der Befragten ausmachten, sind sehr an ihrer Privacy interessiert, daher geben sie fast nie oder nur sehr ungern ihre persönlichen Informationen preis. Die Pragmatisten (56%), die auch um ihre Privacy besorgt sind, geben personenbezogene Informationen nur dann an, wenn diese durch bestimmte Zugriffmaßnahmen geschützt sind. Sie sind weniger als die Fundamentalisten um ihre Privatheit besorgt, aber legen ihre personenbezogene Information nur offen, wenn sie den Grund für deren Benutzung erfahren oder irgendwelche Vorteile daraus ziehen könnten [Kob07]. Die wenig Interessierten (27%) sind bereit, ihre persönlichen Daten unter allen Umständen preiszugeben. Daraus wird ersichtlich, dass zwar eine kleine Zahl von Personen ihre eigenen Daten öffentlich preisgibt, die Mehrzahl der Benutzer (73%) jedoch sehr ungern Informationen preisgibt, wenn es sich um personenbezogene Daten handelt [SmSh07].

Westin teilt die Benutzer ebenfalls in drei Kategorien ein [Les01]:

- Menschen, die sehr beunruhigt bezüglich ihrer Privatheit sind (25% laut [Les01] und starke Einschränkungen in Kauf nehmen, um ihre Privatheit zu schützen.
- 12% der Personen sind überhaupt nicht besorgt und geben ihre Daten beliebig preis.

- Die Mehrzahl der Menschen (63%) fällt in eine dazwischenliegende Kategorie: Einerseits haben sie Bedenken bezüglich der Gefahren, andererseits sind sie daran interessiert, Vorteile zu haben, wenn sie persönliche Daten preisgeben (z. B. bei der Verwaltung von Benutzerprofilen zur Personalisierung von Diensten).

Benutzer haben folgende Bedenken in Bezug auf die Privatheit ihrer persönlichen Daten [Cra99; MaLa01]:

- Gewährleistung einer sicheren Speicherung und Übertragung sensibler Daten;
- Unwissenheit darüber, welche Benutzerinformationen überhaupt von wem gespeichert sind;
- Befürchtung einer unbefugten Preisgabe oder Verwendung personenbezogener Daten;
- Uneinheitliche oder unklare gesetzliche Situation;
- Verbesserte technologische Möglichkeiten, große Mengen an personenbezogenen Daten mit relativ geringem Aufwand zu sammeln und auszuwerten (z. B. Methoden mit Data Mining[3]).

In einer Welt, wo alles sein Preis hat, wo eine 100%ige Anonymität unmöglich ist, damit wir überhaupt existieren können, sollen Schutzmechanismen (wie z. B. P3P)[4] zur Verfügung gestellt werden, die es erlauben, eine Privatheit der personenbezogenen Daten sicherzustellen. Diese Technologien sollen Benutzer informieren, was mit ihren personenbezogenen Daten passiert, ob sie gespeichert und verwendet werden und ihnen dadurch die Entscheidung über die Verwaltung der Daten erleichtern [Wörnd03].

Die Verbesserung von Privacy und der Kontrolle von personenbezogenen Daten kann signifikante wirtschaftliche Vorteile mit sich bringen:

Es ermöglicht den Menschen, Vorteile aus ihren personenbezogenen Daten zu ziehen. Die Kontrolle über diese Daten wird es ihnen erlauben, dass sie mehr Einfluss auf wirtschaftlichen Transaktionen, die ihre Daten betreffen, ausüben können.

[3] Beim Data Minings wird versucht, durch statistische Methoden komplexe Zusammenhänge in Massendaten herauszufinden.
[4] Siehe Kapitel 5.1 Plattform for Privacy Preferences Project (P3P).

Und mehr Einfluss bedeutet, dass sie einen besseren „Deal“ für sich selbst erzielen können.

Mit diesem Informationsaustausch sind nicht nur Vorteile, sondern auch Risiken verbunden, nicht nur für den Einzelnen, sondern auch für andere Interessengruppen, wie Unternehmen, Staat und Spammer. Im nachfolgenden Arbeitsabschnitt soll die Frage geklärt werden, warum Daten überhaupt gesammelt werden, und wem diese Datensammlung konkrete Vorteile oder Nachteile bringt.

Kapitel 3

3 Datensammlung

Die technologischen Möglichkeiten, personenbezogene Information zu sammeln, speichern, analysieren, und weiterzugeben, ermöglichen einen grenzenlosen Datenaustausch, der für das Individuum meistens problematisch ist.

Öffentliche Kommunikationsnetzwerke, wie zum Beispiel Telefonnetzwerke, mobile Netzwerke und das Internet können die personenbezogene Information leicht übermitteln, manchmal sogar ohne dass der Betroffene dies merkt. „Im Unterschied zur Zeitung, wo wenige Daten an viele Adressaten unkontrollierbar weitergegeben werden, ermöglicht das neue Medium „Computer“ die Vermittlung beliebig vieler personenbezogener Daten an selektiv ausgewählte Interessenten“ [FCho96, 49]. Nachfolgenden werden genau diese Interessengruppen dargestellt und erkenntnisrelevante Fragen beantwortet wie z. B. Wieso bzw. zu welchen Zwecken werden überhaupt Daten gesammelt? Was für Folgen hat dies für denjenigen, der dies tut?

3.1 Firmen

Die Menge der gesammelten Daten steigt rasant. Der durchschnittliche Österreicher findet sich nach Cas und Peissl [CaPeJo00, 11] in 400 Datenbanken. Auch bei den Niederländern wird viel mehr gespeichert als die Bürger erwartet haben[5].

Die Zahl der Datensammlungen hängt natürlich vom individuellen Verhalten des Konsumenten ab. Wer stundenlang „online“ ist, sein Mobiltelefon immer eingeschaltet lässt, wird mehr analysiert als jemand, der die Sache vorsichtiger angeht. Eine Vielzahl von Unternehmungen wie z. B. Supermärkte, Warenhäuser, Garagenbetreiber, Telekommunikationsanbieter usw. sammeln, speichern und verwerten personenbezogene Daten bewusst oder unbewusst und ziehen Vorteile daraus. Der Preis ist die Aufgabe unserer Privatsphäre [TiPa01].

Viele Befragungen bestätigen, dass sich Internetbenutzer unterschiedlich in Bezug auf die Offenlegung ihrer personenbezogenen Daten verhalten [Kob07b]. Die

[5] Eine Untersuchung des niederländischen Verbraucherverbands Den Haag hat erhoben, dass über einen Konsumenten über 900 Datensätze geführt werden; 66% der Konsumenten glaubten in weniger als 25 Datenbestände erfasst zu sein und nur 4% in mehr als 100 [vgl. Borking98, 286].

meisten der Benutzer sind bereit, Informationen wie Hobbys, Wünsche, allgemeine demografische Informationen preiszugeben. Wobei hingegen Detailauskünfte über Internetgewohnheiten, Internetkäufe und eine detaillierte demografische Auskunft von vielen Usern meist abgelehnt werden. Die heikelste Privacy-Angelegenheit liegt vor, wenn es um die Offenlegung von Finanzdaten, Kontoinformationen, Kontaktinformation, Kreditkarten- und Versicherungsnummern geht. Der Grund, wieso 63% von den Konsumenten ihre personenbezogene Information im Internet nicht preisgeben, liegt laut einer Befragung von Kobsa daran, dass sie kein Vertrauen zum jeweiligen Webseitenbetreiber haben [Kob07]. Stabile Kundenbeziehungen werden durch Vertrauen geschaffen und profitable Dauerbeziehungen für beide Seiten entstehen nur dann, wenn die informationelle Asymmetrie zwischen Individuum und Unternehmen abgebaut wird.

Das Vertrauen[6] ist ein wichtiger Motivationsfaktor nicht nur für Unternehmen gegenüber von Benutzern, sondern auch für die einzelnen Anwender. Die Unternehmen „müssen von einer informationellen „Einbahnstraßenpolitik“ Abschied nehmen, nach der möglichst viele Informationen über Kunden angesammelt werden, der Einzelne jedoch nur über geringe Information über das Unternehmen verfügt“ [Braun00c].

Daher versuchen Firmen, dieses Vertrauen aufzubauen, indem die Privatsphäre des Individuums gewahrt wird. Je mehr der Endbenutzer die Privacy Policy des Unternehmens kennt und sich mit dieser identifizieren kann, desto eher gibt er seine persönliche Information preis. Dieser Prozess der auch durch den Einsatz von Technologie unterstützt wird, wird im Kapitel 5 (Privacy Enhancing Technologies) noch eingehend erklärt.

Viele Firmen benutzen personenbezogene Daten, die sie von Endbenutzer sammeln, speichern und für kommerzielle Zwecke verwerten, vor allem durch Data Mining, das die Spuren der Menschheit in der elektronischen Welt auffängt und analysiert. Typisch ist der Einsatz von Data Mining im Handel, wo die Kunden in Gruppen zusammengefasst werden. Von den Datensammlungen werden Zusammenhänge ausgearbeitet und vom bisherigen Verhalten des Kunden wird das zukünftige Verhalten mit großer Wahrscheinlichkeit prognostiziert.

[6] Näheres dazu im Kapitel 4.7.1.3.

CRM (Customer Relationship Management) z. B. erstellt auch Kundenprofile und trifft Vorhersagen, ob ein Kunde dem Unternehmen treu bleibt oder ob er zu einer anderen Gruppe mit unterschiedlichen Interessen gehört [TiPa01]. 2007 nutzten 15% der europäischen und 20% der deutschen Unternehmen so ein CRM-System [Strück07]. Von der harmlosen kommerziellen Datenverarbeitung entstehen oft Informationen über Personen, die „einseitig und unrichtig sind“ [Petri]. Einseitig, weil die Daten meistens den Zielen ihres Erzeugers dienen sollen und unrichtig, weil sie ein Benutzerprofil erstellen, welches nur von einer entsprechenden Stelle zusammengestellt bzw. sehr oft für verschiedene Zwecke genutzt wird. So entsteht das Problem der De-Kontextualisierung. Daten werden für ganz andere Zwecke erhoben als für die, nach denen sie ausgewertet werden. Es entstehen falsche Bilder obwohl die Daten an sich „richtig“ sind [TiPa01].

Ein typisches Beispiel dazu verdeutlicht der Film „The Truman Show“, einer der erfolgreichsten Kinofilme des Jahres 1998. Truman Burbank (gespielt von Jim Carey) wird als Baby von einer amerikanischen Firma adoptiert. Es wird ein Ort um ihn aufgebaut und mit 5000 Videokameras überwacht. Jede einzelne Bewegung von ihm wird beobachtet. Die Sendung finanziert sich durch „Product Placement“, indem die Darsteller Produkte anpreisen. Truman selbst merkt überhaupt nicht was mit ihm passiert. Sogar seine Frau und die Freunde in seiner Welt sind Schauspieler. Am Ende des Filmes, als der erwachsene Truman den Sachverhalt erkennt und aus dieser virtuellen Gefangenschaft entkommen will, belehrt ihn der Regisseur mit den Worten: Er sei sicher dort aufgehoben, die reale Welt sei viel gefährlicher. Er kenne ihn so gut, er habe ihn durch sein ganzes Leben mit Kameras beobachtet und dabei behütet. Die entscheidende Antwort von Truman darauf lautete: „ Ihr habt nie eine Kamera in meinem Kopf gehabt!“ [vgl. Petri].

Der Film zeigt, dass die Überwachung von Menschen das Gefühl vermittelt, dass sie innerlich nicht frei und ständig beobachtet sind. Die unfreiwillige Überwachung produziert bei uns Angst und Misstrauen. Die Geschichte erklärt, wieso im Rahmen der kommerziellen Datenverarbeitung auch ein effektiver Datenschutz vorhanden sein muss.

Ähnlich wie in diesem Film ist die Situation im Internet. Tausende von Menschen merken nicht, dass durch die unzähligen Dienstleistungen im Cyberspace ihren persönlichen Daten von Firmen gesammelt werden. Gleichzeitig werden laufend

neue Technologien entwickelt mit deren Hilfe das Verhalten des Nutzers verfolgt wird. Beispiele dafür sind, wenn eine Verbindung zu einem ISP (Internet Service Provider) über ein Modem[7] aufgebaut wird. Der Provider erhält Daten wie:

- Stammdaten, die den Namen, Adresse und die Login -Daten beinhalten
- Verbindungsdaten, die Auskunft darüber geben, wer sich im System wann an- und wann abgemeldet hat. Der Provider erkennt, wann der Benutzer das System benutzt hat oder ob dieser momentan online ist. Über dies weiß er wie lange der User das Internet benutzt und wann er sich das letzte Mal eingeloggt hat.

Bei Verwendung eines Proxy-Servers kann man durch die obenerwähnten Informationen das Internetverhalten jedes Benutzers analysieren (welche Internetseiten aufgerufen werden oder für welche Produkte sich jemand interessiert). Und wenn sich der Benutzer irgendwo für ein kostenloses Webservice registriert, um auf einer Website eine Dienstleistung zu nutzen, z. B. kostenlose SMS-Nachrichten (Short Massage Services), dann muss er Daten wie Name, Email-Adresse und Telefonnummer hinterlassen. Und angenommen der Nutzer ist ein ehrlicher Mensch, dann macht er es genauso, wie es auf der Seite von ihm verlangt wird. Er liest die Privacy-Politik der Seite nicht, da diese kleingedruckt ist und die ausgewiesen Informationen sowieso keiner versteht.

Daten können auch gesammelt werden, wenn Personen z. B. im Internet surfen und zufälligerweise einen Fragebogen ausfüllen, damit sie an einem Gewinnspiel teilnehmen können. Durch diese Information wertet das Marktforschungsinstitut aus, welche Bedürfnisse die Gesellschaft nach bestimmten Produkten hat. Wenn jemand z. B. gerne im Internet Bücher kauft und diese Tatsache beim oben erwähnten Fragenbogen mitteilt, kann das Unternehmen alle Daten von allen Teilnehmern statistisch auswerten und beurteilen, wie viele Menschen prozentual das Internet benutzen, um Bücher zu kaufen. Normalerweise erfolgt die Auswertung solcher Informationen anonym, ohne die Kenntnis der Nutzeridentität. Aber dadurch, dass z. B. etwas verlost wird, erfolgt die Sammlung von personenbezogenen Informationen nicht anonym. Die erlangten Daten können von Unternehmen

[7] Modems sind Geräte, die zwischen den Computer und die Telefondose geschaltet werden. Beim Internetsurfen wandeln sie digitale Daten (Texte, Bilder) aus dem Computer in analoge Daten (Töne) um, die in das Telefonnetz übertragen werden. Bei dem Empfänger der Daten wandelt das Modem diese analogen Daten wieder in digitale Daten um.

an weitere verkauft werden, z. B. an Informations- oder Listbroker[8] [vgl. Petri]. Listbroker werden von interessierten Unternehmen beauftragt, Werbespot über ein bestimmtes Produkt an hunderttausende Verbraucher zu senden. Sie vermieten quasi als Makler die Adressen anderer Unternehmen. Die entsprechende Person wird dann zukünftig ständig E-Mails oder per Post Werbung über Bücher bekommen. Dabei verdienen Unternehmen, die die E-Mail- oder die Postadresse an andere Unternehmen veräußern, 10 Cent bis zu mehreren Euro pro Benutzer. Der Preis hängt davon ab, wie groß die Wahrscheinlichkeit ist, dass der jeweilige Benutzer auf die Werbezuschrift reagiert. Wenn der Nutzer z. B. mit großer Wahrscheinlichkeit ein Buch online kauft, wird er die entsprechende auf ihn zugeschnittene Werbung bekommen. Und automatisch wird seine E-Mail-Adresse in diesem Fall teurer als die von Benützern, die keine Bücher kaufen. Bei einem derartigen Vorgang verdient ein Marktforschungsinstitut mehrere hundert Euro[9] [Petri].

Eine Adresse kann aufgrund einer Verknüpfung als gut oder schlecht beurteilt werden. Die Adressenhändler verfeinern die Adressen, indem Daten von Computerprogrammen mit diversen Dateien verknüpft werden, z. B. werden Postleitzahl- und Straßenverzeichnis abgeglichen. Danach laufen die Daten über eine Kaufkraftdatei und jede Adresse wird mit dem entsprechenden Kaufkraftindex verknüpft. Je höher der Wert, desto besser ist die Adresse. Diese kann also aufgrund der Verknüpfung als gut oder schlecht beurteilt werden [Mähr99, 42]. So gewinnen Daten in Verbindung mit anderen Daten an Aussagekraft (“Mosaiktheorie“) [Egg90, 57].

Die US-Firma Doubleclick[10] hat die weltweit umfassendste Datenbank von Internetanwendern und ist dazu in der Lage, unglaublich viele Informationen über einen Anwender bereitzustellen, wie z. B. Informationen über das Betriebssystem auf seinem Computer, den Namen und den Standort seiner Firma und seine besonderen Interessen [vgl.WolfIR97]. Auch die Datenbank des österreichischen „Compass-Verlages“[11] wird als Direktmarketinginstrument genutzt. Die amerikanische

[8] Das sind Personen, die systematisch Informationen zu bestimmten Personen oder Unternehmen zusammenstellen. Dazu benötigt man Know-how über betriebswirtschaftliche Bedürfnisse und die Funktionszusammenhänge des Internets.
[9] Der Wert der personenbezogenen Information nimmt mit der Zeit ständig ab. Die Verwertung von Konsumentendaten zu Werbezwecken lohnt sich nur etwa zwei bis drei Jahre ab der Datenerhebung [Petri].
[10] http://www.doubleclick.com/.
[11] http://www.compass.at/.

Firma Focalink Communication[12] stellt Benutzerprofile von Nutzern mit ihren Vorlieben und Interessen im Web dar. Dank dieser Information können Firmen gezielt Spam[13] versenden [Mähr99, 54].

Daten über die Kreditwürdigkeit von Personen werden zum Beispiel ermittelt, wenn jemand Einkäufe im Internet per Kreditkarte tätigt. Hat sein Arbeitgeber zufälligerweise seinen Lohn nicht überwiesen, so wird er sofort als nicht zahlungsfähig eingestuft und der Einkauf kann nicht erfolgen. Bestellt der Kunde wenig später etwas auf Rechnung, wird die Bestellung automatisch verweigert, da die Unternehmen Partner einer Warndatei sind und der Kunde als nicht kreditwürdig erfasst wurde.

Das Geschäft mit der Warndatei funktioniert so, dass die Vertragspartner meistens zwischen 15 Euro für Inlandskurzberichte, bis zu 120 Euro für einen Vollbericht über ein ausländisches Unternehmen zahlen, damit ein bestimmtes Kreditbüro die Kreditwürdigkeit der Person (hier der Endbenutzer) meldet. So ein Kreditbüro ist die deutsche Schufa AG – Schutzgemeinschaft für allgemeine Kreditsicherung. Das Unternehmen spezialisiert sich darauf, seinen Vertragspartnern gegen Entgelt Auskünfte über die Kreditwürdigkeit von Bürgern und Unternehmen zu erteilen. Im Jahr 2005 erwirtschaftete die AG einen Umsatz von rund 76 Millionen Euro und einen Gewinn von 2,9 Mio. Euro.[14]

Falls der Nutzer das Produkt auf einer anderen Art und Weise bestellt und dann nicht bezahlt, wird er überall im Internet als „säumiger Zahler“ dargestellt und ist als solcher für jedermann gegen eine Gebühr einsehbar [Petri].

Wenn die Person eine Suchmaschine, z. B. Google aufsucht und seinen Namen eingibt, wird sie sich wundern, wie viele personenbezogene Informationen über ihn zu finden sind und wie viele falsche Informationen gespeichert wurden.

[12] http://www.focalink.com/.
[13] mehr über Spam siehe Kapitel 3.2 Spammer.
[14] Schufa Holding AG (früher SCHUFA e. K. - Schutzgemeinschaft für allgemeine Kreditsicherung) http://www.schufa.de/.

3.2 Spammer

"Spam is no random event, but specifically targets those with purchasing power" [HaLaLePNG06]

Eine andere Gruppe von Datensammler sind die sogenannten Spammer.

Der Begriff Spammer kommt von dem Begriff „Spam" und stand ursprünglich für die massenhafte Sendung unerwünschter Werbung in den Newsgroups, also speziellen Diskussionsbereichen im Internet. Dort tauchte zum ersten Mal das Wort „Spam" auf. Die englische Bedeutung von „Spam" ist einfach eine unerwünschte E-Mail. Aber wenn das tatsächlich so ist, dann sollten alle E-Mails, die wir nicht wollen und bekommen, „Spam" heißen. Für andere ist „Spam" "unsolicited commercial email" (UCM), was soviel wie unaufgeforderte E-Mail bedeutet, die Werbung für Produkte oder anderweitige Angebote beinhaltet. Eine massenhaft unerwünschte Nachricht muss aber nicht immer in Form einer E-Mail auftreten. Es kann sein, dass der Internetbenützer durch ständige Veröffentlichung ein und desselben Beitrages in den Newsgruppen belästigt wird. Diese Form der virtuellen Belästigung im Cyberspace zählt auch als Spam im Internet (Usenet) [PlöDuHel02, 167]. Es ist auch möglich SPAM per SMS oder Fax zu bekommen.

Der Begriff SPAM kommt aber aus einem völlig anderen Bereich. SPAM in Großbuchstaben geschrieben ist eigentlich eine Abkürzung von "Spiced Pork and Ham", ist eine geschützte Wortmarke von der US-amerikanischen Firma Hormel Foods[15] und steht für Dosenfrühstücksfleisch. Der Zusammenhang zwischen diesem Fleisch und unerwünschter Werbung erzeugte indirekt Monthy Python, ein britischer Komiker. In seinem Sketch "Viking Spam" versuchte ein Gast in einem Restaurant, dessen Karte ausschließlich Speisen enthält, die nur aus SPAM basieren, ein Gericht ohne dieses Fleisch zu bestellen. Er fragte die Kellnerin nach entsprechenden Angeboten und in diesem Moment begann „eine Horde von Wikingern einen aus dem einzigen Wort „spam" bestehenden Song" zu singen, „immer lauter und lauter, bis die übrigen ihr eigenes Wort nicht mehr verstehen" [Braun00b][16].

[15] http://www.spam.com/.
[16] siehe NETHICS. Portal zur Informationsethik: http://www.nethics.net/nethics_neu/n3/news/netznews.htm/.

Woher die Wurzeln von „Spam“ kommen, ist immer noch unklar. Viele denken, dass es ursprünglich von MUDs in den 80er Jahren kommt. MUD („multiuser dungeon“) ist ein virtueller Platz zum Spielen, der ein textbasiertes Spielmedium benutzt. Dort taucht das erste Mal für unerwünschte Werbung der Begriff „Spam“ auf. Andere leiten den Begriff vom Pythons Sketch ab und definieren ihn als jede Unterbindung des Kommunikationsmediums. „Genau dies droht im Internet: die Spammer sind dabei, das schnelle und elegante Kommunikationsinstrument E-Mail mit ihrem Gedröhne zu knebeln.“ [Braun00b][17]. Egal woher der Begriff kommt, es konnte keine bessere Bezeichnung gegeben werden [ZD05; Eggen05, 20].

Die überwiegende Meinung in Fachbereichen versteht unter „Spamming“ unerwünschte (unverlangte) Werbe-E-Mails („Unsolicited Commercial E-Mail“, was UCE heißt), die der Benutzer ohne vorherige Einwilligung bekommt. In Österreich besteht gemäß § 107 TKG[18] ein allgemeines Verbot von unerwünschten E-Mails an Verbraucher und Unternehmen, mit der Ausnahme von §107 Abs. 3 TKG [Ja04, 69] [InternetRecht06]. Spammer dagegen sind alle Personen, Organisationen oder Unternehmen, die unbestellte E-Mails verschicken, um so neue Kunden zu akquirieren. Wie Thomas Mandl, technischer Leiter beim österreichischen Sicherheitsunternehmen Ikarus Software[19] sagt: „Spam ist Geld. Der extreme Anstieg der Spambelastung hat einen rein kommerziellen Hintergrund, denn selbst wenn nur 0,01 Prozent der Adressaten auf eine Spam-Werbung reagiert und kauft, ist es bei 15 Milliarden Spam-Nachrichten täglich noch immer lukrativ“ [Weiss08].

Im globalen Computernetz bekommt „SPAM“ als „Send Phänomenal Amount of Mail“ eine neue Bedeutung. Damit „Spam“ überhaupt verschickt werden kann, durchforsten sogenannte Harvester-Programme zuerst das WWW (World Wide Web) oder die Diskussionsforen des Usenet nach E-Mail-Adressen. Übliche Harverster sind die sogenannten Email-Spiders, die ähnlich wie Robots bei einer Suchmaschine funktionieren und auf Webseiten nach E-Mail Adressen suchen, und diese speichern. Landet man auf so einer Spammerliste, wird man ständig mit unerwünschter Werbung überflutet [Weiss08]. So werden ohne große technische Anforderungen neue Dimensionen des Direktmarketings erschlossen.

[17] NETHICS. Portal zur Informationsethik: http://www.nethics.net/nethics_neu/n3/news/netznews.htm/.
[18] TKG = Telekommunikationsgesetz.
[19] http://www.ikarus.at/.

Jeder Nutzer beginnt aufgrund seiner Onlineaktivitäten personenbezogene Daten im Internet zu hinterlassen. Sehr wahrscheinlich ist es, dass seine E-Mail-Adresse durch mehrere Spammer aufgefangen wird und er in Folge ständig E-Mails über „interessante Produkte“, sogenanntes Hotmailing, was Direktwerbung oder Spamming heißt, bekommt. Das bedeutet, dass der Werbende unaufgefordert E-Mails an den Internetbenutzer sendet, deren Adresse er bekommt.

In Deutschland ist so eine Direktwerbung wettbewerbswidrig. Trotzdem senden Unternehmen unaufgefordert solche E-Mails, weil sie sich darauf verlassen, dass der Internetbenutzer die deutsche Rechtslage nicht kennt oder sich überhaupt mit der Situation nicht auskennt. In anderen Staaten ist Hotmailing erlaubt, insbesondere in den USA, Frankreich und Großbritannien, wo man die Position vertritt, dass man, solange unaufgefordert Werbematerial senden darf, bis der Kunde nicht widerspricht, die sogenannte Opt-Out-Variante. Wenn der Adressat keinen Widerspruch nach dem Erhalt der Werbe-E-Mails ausspricht, ist die E-Mail-Werbung zulässig. Dem Unternehmen oder Privatpersonen steht die Möglichkeit offen, sich in eine „Robinson-Liste“[20] einzutragen, um potenziellen Spammern mitzuteilen, dass sie keine Werbe-E-Mails bekommen sollen.

In Österreich sieht das Telekommunikationsgesetz die Opt-in-Lösung vor. Seit dem 1. März 2006 gilt in Österreich „ein gänzliches Werbeverbot ohne vorherige Zustimmung (Ausnahme in §107 Abs. 3 TKG)“ [InternetRecht06]. Nach dieser sogenannten Opt-in-Lösung ist Spam nur dann zulässig, wenn zuvor eine Zustimmung des Empfängers eingeholt wurde.

§107 Abs. 3 TKG besagt, dass eine Zustimmung dann nicht notwendig ist, wenn

- „der Absender die Kontaktinformation für die Nachricht im Zusammenhang mit dem Verkauf oder einer Dienstleistung an seine Kunden erhalten hat und
- diese Nachricht zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen erfolgt und
- der Empfänger klar und deutlich die Möglichkeit erhalten hat, eine solche Nutzung der elektronischen Kontaktinformation bei deren Erhebung und zusätzlich bei jeder Übertragung kostenfrei und problemlos abzulehnen und

[20] http//www.erobinson.com/.

- der Empfänger die Zusendung nicht von vornherein, insbesondere nicht durch Eintragung in die §7 Abs. 2 E-Commerce-Gesetz genannte Liste[21], abgelehnt hat“ [InternetRecht06b].

Der „Newslettermarkt“ in den letzten Jahren ist stark angestiegen. In einer EU-Studie wurde das Verhältnis zwischen erwünschten und unerwünschten E-Mails analysiert. Dieses lag „2001 noch bei 13 zu eins, 2004 war es eins zu drei, also auf ein erwünschtes Mail folgten drei unerwünschte E-Mails, d.h. ein Plus zu 200% und 2007 mit 1 zu 50, das ist ein Plus von 250%“ [ARGE08c]. Trotz dieser Spammails-Rekordwerte (wo jedes fünfzigste E-Mail heute erwünscht ist), sehen einige Branchen innerhalb der WKO interessante Geschäftsfelder für österreichische Unternehmen in diesem Spammarkt [vgl. ARGE08c]. Aber hinter all diesen Online-Aktivitäten verbergen sich rechtliche Bestimmungen, die vielen Betreibern kommerzieller Websites nicht bekannt sind. Über die Verbotsbestimmungen des Telekommunikationsgesetzes weiß mit 47,6% nicht einmal die Hälfte der Betriebe Bescheid [Lind08]. Daher sind die Aufklärung und die Auskunftspflicht über Spam und IT-Sicherheit wichtige Punkte einer funktionierenden informationellen Selbstbestimmung.

3.3 Staat

“Relying on the government to protect your privacy is like asking a peeping Tom to install your window blinds.“ John Perry Barlow [Neh07]

Seit dem 11. September 2001 hat sich in Hinsicht auf den Datenschutz einiges geändert. Laut Umfragen des Marktforschungsunternehmens Fittkau & Maaß [Pat01] finden es rund 68% der deutschen Benutzer wichtig oder sehr wichtig, sich weiterhin anonym im Internet bewegen zu können. Allerdings sind auch 71% der Benutzer dafür, das das Internet künftig durch Polizei und Ermittler besser überprüfbar ist. Schließlich hat man als Durchschnittsbürger doch nichts zu verbergen, oder?

Es ist nachvollziehbar, dass immer mehr Länder im Rahmen der Maßnahmen der Terrorismusbekämpfung auch vermehrt virtuelle Barrieren errichten. Mit dem Ziel einer Totalüberwachung hoffen die Regierungen dieser Welt, den richtigen Weg

[21] Die Liste nach §7ECG betrifft Werbung mittels elektronischer Post und ist von allen Dienstanbietern zu beachten, die unerbetene Werbung mittels elektronischer Post versenden, mehr dazu unter http://www.rtr.at/de/tk/E_Commerce_Gesetz/Spam_Infoblatt.pdf/.

zur Bekämpfung des Terrorismus gefunden zu haben. In dem sie enorme Datenmengen verarbeiten, die Arbeitswelt per Video überwachen, persönliche Daten über Telefongespräche, SMS (Short Massage Service) und VoIP [22] sammeln und speichern, ziehen sie daraus ihre eigenen Vorteile und schaffen die Basis für eine umfassende Kontrolle des Bürgers. Die unterschiedlich gesammelten und gespeicherten Videodaten zum Beispiel können mit entsprechender Software miteinander verglichen und analysiert werden. Menschen können durch ihre Körperbewegung identifiziert werden, es ist sogar möglich, dass verdächtiges vom normalen Verhalten unterschieden werden kann [TiPa01]. Dabei zerstören sie aber langsam die Privatsphäre des Individuums und die Welt verwandelt sich tatsächlich in eine „gläserne“, wo jeder Knopfdruck ausforschbar ist. Die Konsumenten verlassen sich darauf, dass die Regierung für den Schutz ihrer Privatsphäre sorgt, aber eigentlich installiert genau diese Überwachungsprozesse mittels elektronische Netzwerke und Supercomputer. Damit betritt sie unbefugt die Privatsphäre des Individuums. Die U.S. Regierung (U.S. Department of Homeland Security) entwickelt z. B. eine Data Mining Applikation, um möglichst viele Informationen über Amerikaner zu sammeln, um mögliche Terroristen identifizieren zu können. In der Testphase dieses Systems ist natürlich ein enormer Datenschutzmissbrauch „unvermeidlich“ [Neh07, 372].

Organisationen wie das amerikanische „Electronic Privacy Information Center“[23] und das englische „Privacy International“[24] zeigen, dass sogar Demokratien, in denen die Menschenrechte konstitutionelle Prinzipien sind, in Überwachungsländer umgewandelt werden.

Beide Organisationen stellen 2007 ein Bild von 47 Ländern, inklusive Österreich dar, wo sie nach 14 Kriterien und einer siebenstufige Skala die Situation überall auf der Welt beobachten (siehe die Abbildung 1 und Tabelle 1): Es wurden der Grad der Verankerung des Datenschutzes in der Verfassung, der Status und die Aktivitäten der Datenschutzbehörden, sowie das Maß an Überwachung in verschiedenen gesellschaftlichen Bereichen wie etwa dem Gesundheitswesen bewertet. Es kommen auch diese Art und Weise die Engagements bei internationalen

[22] Unter VoIP (Voice over IP) bzw. IP-Telefonie versteht man das Telefonieren über Computernetzwerke.
[23] Electronic Privacy Information Center: http://epic.org/.
[24] Privacy International: http://www.privacyinternational.org/.

Verträgen oder Regierungsinitiativen zum Thema Datenschutz bei der Bewertung zum Tragen.

Die Tendenz ist sehr beunruhigend. Überall auf der Welt verschlechtert sich die Situation, indem immer mehr Daten gesammelt werden und sich die Überwachungsmechanismen verstärken. Die Rating Privacy Tabelle 2007 zeigt, dass die Regierungen immer mehr dazu neigen, Daten über die geografische, kommunikationelle- und finanzielle Lage von ihren Bürgern und Ausländern zu sammeln und zu speichern.

Erstaunlich ist das Faktum, dass Griechenland das einzige Land ist, das seinen Bürgern einen guten Schutz vor Überwachung und Sammlung personenbezogener Daten bietet. Die griechische Datenschutzkommission ist als unabhängige Institution in der Verfassung verankert und mit Vollmachten ausgestattet, von denen Österreich nur träumen kann.

In Österreich dagegen verschlechtert sich die Situation. Laut der Studie hat Österreich kein eindeutiges Privacy Recht, wohl aber spezielle Gesetze für Zivilrechte, eines von diesen ist der Datenschutz. Die Datenschutzkommission kann zivilrechtliche und kriminelle Angelegenheiten vor Institutionen hervorbringen, wurde aber aufgrund ihrer Unabhängigkeit kritisiert. Die medizinischen Daten werden als sensible Daten[25] behandelt. Die Daten der Studenten werden seit 60 Jahren gespeichert. In den Sozialversicherungskarten mit einmaliger Nummer sind vergleichsweise wenige Daten gespeichert. Das E-Identitätsmanagement wird stark kritisiert [Privacy08].

Mit der am 6. Dezember 2007 vom österreichischen Nationalrat verabschiedeten Novelle zum Sicherheitspolizeigesetz, öffnet sich langsam die Tür zu einem Überwachungsstaat. Das Gesetz gestattet der Polizei, Zugriff auf den aktuellen Standort aller Mobiltelefone zu haben, Handytelefonate abzuhören und die Daten über die Internetnutzung von Benutzern zu erlangen. Dabei fühlt man sich auf Kosten unserer Freiheit und Demokratie genau von denen, die uns schützen sollen, bedroht: Der Verfassung, der Justiz und der Polizei. Durch Maßnahmen wie das Datenspeicherungsgesetz, das in Deutschland ab 1 Januar 2008 in Kraft getreten ist,

[25] Sensible Daten gelten als besonders schutzwürdig. Das sind Daten von natürlichen Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben [Ja04].

in Österreich für 18 Monate ab 15. September 2007 aufgeschoben wurde[26], sollen „die Verbindungs- und Standortdaten, welche beim Telefonieren, Versenden von SMS-Nachrichten, E-Mails, VoIP, Faxen und Surven im Internet entstehen, etwa die Benutzerkennung, Name und Anschrift des Teilnehmers, die IP-Adresse, Kennung oder Rufnummer, als auch die erfolglosen Verbindungsversuche“ gespeichert werden [ARGE08d].

Laut der Studie wird die datenschutzrechtliche Situation in Österreich immer schlechter, da sich gewisse Sicherheitsmassnahmen nicht bewahren lassen [Pat08]. Das Land wurde 2007 gleich um zwei Kategorien zurückgestuft und ist damit auf dem 14. Platz der EU-Staaten-Vergleichsskala wiederzufinden: Vom „adäquat geschützten“ (Farbe grün) zum „systematischen Datenschutzversager“ (Farbe rot). Ein Überwachungsstaat ist das immer noch nicht, aber beruhigend ist diese Situation ebenfalls nicht. Besonders negativ wird der grenzüberschreitende Austausch von DNA- und Fingerabdruckdaten mit den USA bewertet. Betrachtet man die Situation auf internationaler Ebene, gelten Länder wie China, Russland, Großbritannien und die USA als Staaten, in denen die Überwachung der Bürger bereits Tradition hat. Österreich ist immer noch zwei Stufen davon entfernt, aber es geht langsam den Weg einer totalen Kontrolle seiner Bürger. Dies hat auch seine Vorteile, aber auch nicht zu unterschätzenden Nachteile. Einen Überblick über die weltweite Entwicklung der Überwachungsgesellschaften und das Privacy Ranking liefern die nachfolgenden Abbildungen.

[26] http://www.bka.gv.at/.

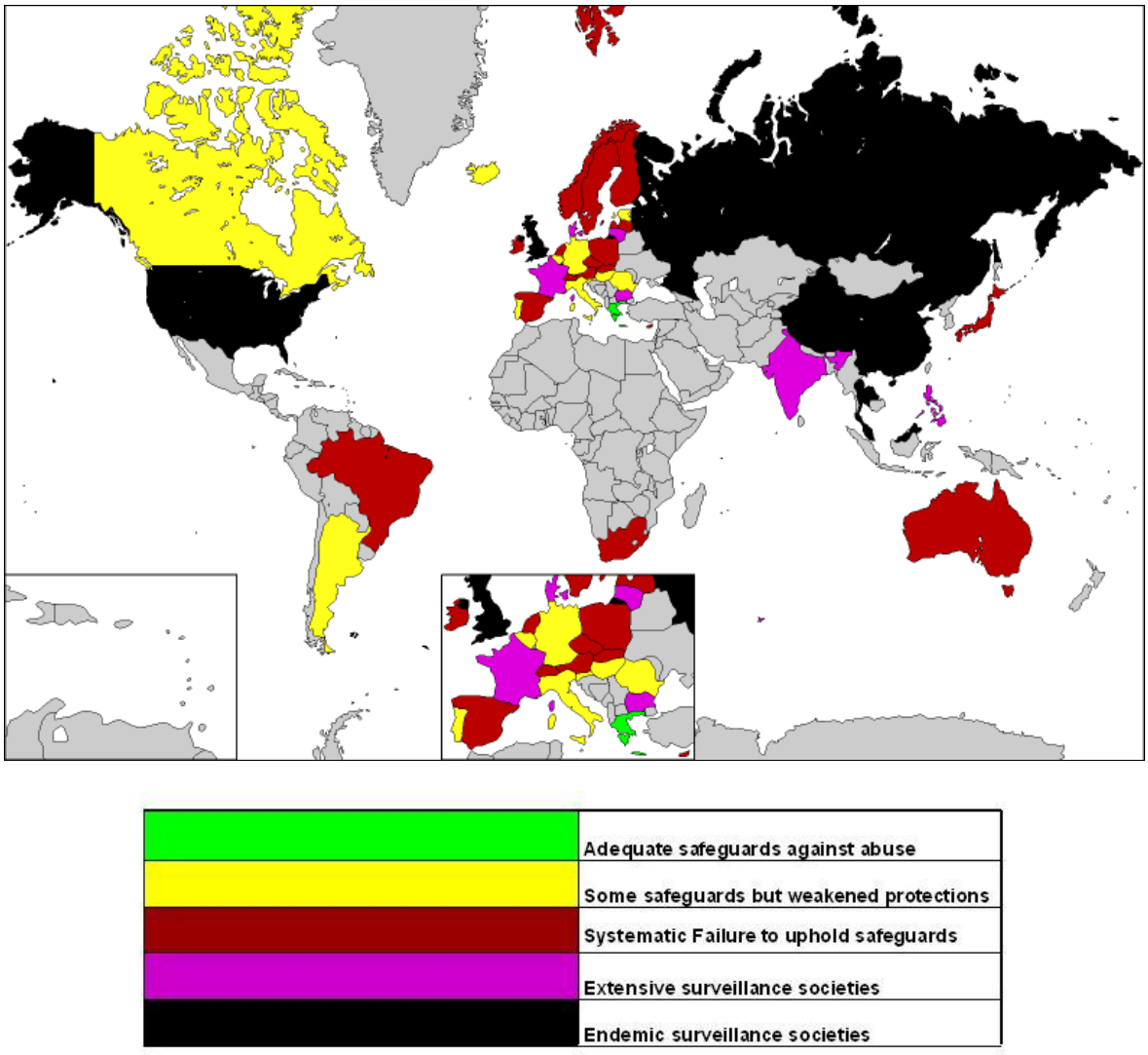


Abbildung 1: Weltkarte der Überwachungsgesellschaften. Quelle: http://www.privacyinternational.org/[27].

[27] entwickelt von http://english.freemap.jp/.

Privacy International

National Privacy Ranking 2007 - Leading Surveillance Societies Around the World

	Constitutional protection	Statutory protection	Privacy Enforcement	Identity Cards and Biometrics	Data-sharing	Visual surveillance	Communication Interception
European Union							
GREECE	4	3	4	3	-	3	1
ROMANIA	3	3	4	-	-	-	2
HUNGARY	4	4	4	4	3	1	1
SLOVENIA	4	4	4	2	3	4	2
PORTUGAL	4	4	3	2	2	2	2
LUXEMBOURG	2	3	3	3	2	-	2
GERMANY	4	4	4	2	4	2	2
ITALY	4	4	4	2	-	3	1
ESTONIA	3	3	4	2	-	-	2
BELGIUM	4	4	4	1	1	-	2
CZECH REP.	4	3	4	2	1	2	1
FINLAND	3	3	3	2	1	-	3
IRELAND	2	3	4	2	2	-	3
MALTA	2	4	3	-	-	-	2
POLAND	3	4	3	1	3	2	1
SPAIN	3	4	4	1	-	2	1
AUSTRIA	2	3	2	2	1	2	2
CYPRUS	3	3	3	2	-	2	1
EU	3	2	3	2	2	-	-
LATVIA	3	2	2	2	2	-	2
NETHERLANDS	2	4	4	1	1	2	1
SLOVAKIA	4	3	3	1	-	-	2
SWEDEN	3	2	3	3	2	3	2
DENMARK	3	2	2	4	1	3	2
BULGARIA	3	2	3	1	-	-	1
LITHUANIA	3	3	2	1	-	1	1
FRANCE	3	2	3	2	1	2	2
UK	1	2	2	1	1	1	1
England&Wales	1	2	2	1	1	1	-
Scotland	1	2	2	3	3	2	-
INTERNATIONAL							
CANADA	4	4	2	2	2	2	3
ARGENTINA	4	4	2	-	2	-	2
ICELAND	4	4	4	2	3	2	3
SWITZERLAND	4	4	2	2	2	1	2
NEWZEALAND	2	2	3	3	2	-	1
SOUTH AFRICA	4	1	1	2	2	-	2
JAPAN	3	1	1	2	2	2	3
AUSTRALIA	1	2	2	3	2	-	2
ISRAEL	4	3	3	2	2	2	2
BRAZIL	3	2	1	2	2	2	2
NORWAY	3	2	3	2	1	2	2
INDIA	3	1	1	-	-	-	1
PHILIPPINES	3	2	1	1	-	-	1
US	3	1	1	1	2	1	1
THAILAND	2	2	2	1	-	2	1
TAIWAN	2	2	1	1	-	-	1
SINGAPORE	1	1	1	1	2	1	1
RUSSIA	3	2	1	2	1	-	1
CHINA	2	2	1	2	1	1	1
MALAYSIA	1	2	1	1	1	1	1

Privacy International

National Privacy Ranking 2007 - Leading Surveillance Societies Around the World

	Communica-tion Data Reten-tion	Government Access to Data	Workplace monitoring	Surveillance of Medical, Financial, and Movement	Border and trans-border issues	Leader-ship	Democratic Safeguards
European Union							
GREECE	-	3	-	3	-	4	3
ROMANIA	3	2	-	-	-	2	4
HUNGARY	4	3	2	2	3	1	4
SLOVENIA	1	2	4	2	-	2	3
PORTUGAL	-	-	3	3	-	2	4
LUXEMBOURG	3	-	4	4	-	1	4
GERMANY	1	3	2	4	2	1	4
ITALY	1	2	4	2	3	3	3
ESTONIA	-	3	-	3	-	2	3
BELGIUM	2	3	4	3	2	1	4
CZECH REP.	2	2	3	2	2	3	4
FINLAND	3	2	2	2	2	2	4
IRELAND	1	2	3	3	2	1	4
MALTA	-	2	-	-		2	2
POLAND	1	2	-	2	-	3	3
SPAIN	2	2	3	1	-	1	4
AUSTRIA	4	2	-	3	2	1	4
CYPRUS	-	-	-	2	2	2	3
EU	1	2	-	3	2	2	3
LATVIA	-	2	3	2	2	2	3
NETHERLANDS	1	2	3	2	2	1	4
SLOVAKIA	1	1	-	2	-	2	2
SWEDEN	1	1	1	1	2	1	4
DENMARK	1	1	-	1	1	2	3
BULGARIA	2	2	-	2	-	2	2
LITHUANIA	3	-	1	-	-	2	3
FRANCE	1	1	-	2	1	1	4
UK	1	2	2	1	1	1	3
England & Wales	-	2	-	1	-	1	2
Scotland	-	3	-	2	-	3	4
INTERNATIONAL							
CANADA	4	3	3	2	2	3	4
ARGENTINA	2	-	-	2	-	4	3
ICELAND	2	2	3	2	1	2	4
SWITZERLAND	2	2	-	2	1	3	4
NEWZEALAND	3	2	2	2	-	2	4
SOUTH_AFRICA	1	-	-	4	2	-	4
JAPAN	4	3	-	3	1	1	3
AUSTRALIA	4	2	3	1	1	2	3
ISRAEL	2	1	-	1	1	2	3
BRAZIL	2	2	3	1	2	3	3
NORWAY	2	2	3	1	1	2	4
INDIA	-	1	-	2	-	2	4
PHILIPPINES	2	1	-	2	-	2	3
US	3	2	1	1	1	1	2
THAILAND	2	1	-	1		2	1
TAIWAN	3	2	-	1	1	1	2
SINGAPORE	3	1	1	3	2	1	1
RUSSIA	1	1	-	1	1	1	1
CHINA	1	1	-	2	-	1	1
MALAYSIA	3	1	-	1	1	2	1

Privacy International

National Privacy Ranking 2007 - Leading Surveillance Societies Around the World

	Total	Last Year's Ranking	This Year's Ranking	Change
European Union				
GREECE	3.1			
ROMANIA	2.9	-		
HUNGARY	2.9			
SLOVENIA	2.8			Improving
PORTUGAL	2.8			
LUXEMBOURG	2.8			
GERMANY	2.8			Decaying
ITALY	2.8			
ESTONIA	2.8			
BELGIUM	2.7			Deteriorating
CZECH REP.	2.5			
FINLAND	2.5			Deteriorating
IRELAND	2.5			
MALTA	2.4			Deteriorating
POLAND	2.3			Deteriorating
SPAIN	2.3			
AUSTRIA	2.3			Decaying
CYPRUS	2.3			Deteriorating
EU	2.3	-		
LATVIA	2.2			Deteriorating
NETHERLANDS	2.1			
SLOVAKIA	2.1			
SWEDEN	2.1			
DENMARK	2.0			Deteriorating
BULGARIA	2.0	-		
LITHUANIA	2.0			Deteriorating
FRANCE	1.9			Decaying
UK	1.4			
England & Wales	1.4	-		
Scotland	2.5	-		
INTERNATIONAL				
CANADA	2.9			Decaying
ARGENTINA	2.8			
ICELAND	2.7	-		
SWITZERLAND	2.4	-		
NEWZEALAND	2.3			
SOUTH_AFRICA	2.3			-
JAPAN	2.2			-
AUSTRALIA	2.2			
ISRAEL	2.2			
BRAZIL	2.1	-		
NORWAY	2.1	-		
INDIA	1.9	-		
PHILIPPINES	1.8			
US	1.5			Deteriorating
THAILAND	1.5			Deteriorating
TAIWAN	1.5	-		
SINGAPORE	1.4			
RUSSIA	1.3			
CHINA	1.3			
MALAYSIA	1.3			

Privacy International National Privacy Ranking 2007 - Leading Surveillance Societies Around the World	
GRADE	
5	no invasive policy or widespread practice/leading in best practice
4	comprehensive efforts, protections, and safeguards for privacy
3	some safeguards, relatively limited practice of surveillance
2	few safeguards, widespread practice of surveillance
1	extensive surveillance/leading in bad practice

FINAL SCORE	
4.1-5.0	Consistently upholds human rights standards
3.6-4.0	Significant protections and safeguards
3.1-3.5	Adequate safeguards against abuse
2.6-3.0	Some safeguards but weakened protections
2.1-2.5	Systemic failure to uphold safeguards
1.6-2.0	Extensive surveillance societies
	Endemic surveillance societies

CHANGE	
Improving	Country has improved since last year
Deteriorating	Country has dropped by one category
Decaying	Alarming rate of fall in protections

Tabelle 1: Privacy Ranking 2007. Quelle: http://www.privacyinternational.org/.

Kapitel 4

4 Gesetzliche Rahmenbedingungen

Die Informationstechnologie und damit die leichtere Datenverarbeitung in der Wirtschaft haben sowohl neue Chancen als auch neue Risiken bezüglich des Umgangs mit den Daten und ihrer Sammlung geschaffen. Einerseits haben die Unternehmen ein Interesse daran, diese Daten zu Wettbewerbsvorteilen zu erheben und weiterzuverarbeiten, andererseits müssen wirksame und durchsetzbare Regelungen bezüglich des Datenschutzes sichergestellt werden, um so Missbrauch zu vermeiden [BaerRud02, 439f.] und dabei ebenso rechtliche Grundsätze für die technische Ebene (vgl. dazu Kapitel 5) zu schaffen.

In diesem Beitrag werden das Datenschutzgesetz (DSG) und das Telekommunikationsgesetz (TKG) in Österreich bzw. aktuelle Entwicklungen von Privacy-Gesetzen dargestellt. Überdies werden die OECD-Richtlinien und die EU-Datenschutzrichtlinien (EU-DS-RL) kurz erläutert, die für alle Nationalgesetze eine hohe Relevanz besitzen. Anschießend beschäftigt sich die Arbeit mit der Situation innerhalb der USA. In diesem Zusammenhang wird auch auf die Problematik des E-Privacy Management im Internet eingegangen.

4.1 Datenschutzgesetz

Der Datenschutz existiert in vielen Ländern sowie in internationalen Verbünden wie der Europäischen Gemeinschaft, aber in unterschiedlicher Ausprägung. Im nachfolgenden Abschnitt wird die Entstehung des Datenschutzes in Österreich, sein Aufbau und seine Ziele dargestellt.

4.1.1 Entstehung des Datenschutzgesetzes

Obwohl ein erster Entwurf zu einem Österreichischen Datenschutzgesetz (ÖSDSG) erst 1973 vorlag, beginnt die Geschichte des modernen Datenschutzgesetzes schon Anfang der 60er Jahre des 20. Jahrhunderts in den USA. Die amerikanische Regierung plante damals, alle amerikanische Bürger und Bürgerinnen in eine Datenbank trotz der damals noch wenig entwickelten Computertechnik aufzunehmen. Viele haben diesen Tatbestand als einen schweren Eingriff in die Privatsphäre empfunden. Dadurch entstand die Datenschutzdebatte, deren Grundlage

das Recht auf Privatheit („The Right to Privacy“) von Warren und Brandeis war. Das Ergebnis der Debatte war, dass das Privatsphärengesetz („Privacy Act“)[28] in den USA verabschiedet wurde. Es besagt, dass die amerikanische Bundesregierung zur Einhaltung von Grundprinzipien zur Sicherung der Privatsphäre verpflichtet ist. Dieser Prozess löste auch entsprechende Aktivitäten in vielen Industriestaaten wie z. B. Deutschland oder Österreich aus [Garstka].

In Österreich kommt erst am 8. Juli 1969 die Frage nach dem Datenschutz zur Sprache, als die Bundesregierung einen „Bericht über den Einsatz elektronischer Datenverarbeitungsanlagen in der Bundesverwaltung“ vorlegte. Die Gesetzlage der damaligen Zeit war vollkommen ausreichend, obwohl die Probleme der Privatheit des Einzelnen erkannt wurden [Mähr99, 12f.].

Am 14. Mai 1969 wird vom Nationalrat ein Gesetz über die statistische Erfassung von Geschwulstkrankheiten (Krebsstatistikgesetz) beschlossen. Der Antrag wird positiv weitergeleitet, obwohl er, durch die Aufnahme der Namen aller Krebskranken, einen schweren Eingriff in die Privatsphäre darstellt.

In den folgenden Jahren wird festgestellt, dass durch die Entwicklung der Technologie und durch den zunehmenden Einsatz des Computers die Sammlung verschiedener Informationen von Einzelpersonen und damit die Gefahr eines Datenmissbrauches steigt. Der Gedanke nach einem Datenschutz verstärkt sich, bis am 22. Januar 1975 die Regierung eine Vorlage für ein Bundesgesetz über den Schutz personenbezogener Daten einbringt. Es dauert bis zum 18. Oktober 1978, bis der Nationalrat das Datenschutzgesetz beschließt [Egg90, 89f.]. Mit diesem am 1. Januar 1980 in Kraft getretenem Grundrecht auf Datenschutz setzt eine neue Entwicklung im Bereich der personenbezogenen Daten ein.

4.1.2 Aufbau und Ziele des DSG

In Österreich stellt der Schutz der Privatsphäre ein Grundrecht dar und ist in den Paragraphen des DSG 2000 geregelt. Die Datenschutz-RL[29] der Europäischen Union wurde in Österreich durch das Datenschutzgesetz 2000 umgesetzt. Es reguliert nicht nur die Verwendung personenbezogener Daten, die Auskunftsrechte Betroffener, die Zulässigkeit der Weitergabe von Daten und den Umgang mit Daten in Netzwerken, sondern bestimmt auch die Datensicherheit, die Kontroll- und

[28] Privacy Act vom 31. Dezember 1974; Public Law 93-579. [Hof02, 122].
[29] Näheres dazu siehe Kapitel 4.5 Privacy Richtlinien der OECD.

Rechtsschutzmaßnahmen und sieht Strafen bei einer missbräuchlichen Verwendung von Daten vor [Internet&Recht06a]. Das DSG gliedert sich in 2 Artikel mit insgesamt 59 Paragraphen [Mähr99, 14]:

Abschnitt	§§	Inhalt	Gültig für öffentlichen Bereich	Gültig für privaten Bereich
-	1-2	Grundrecht auf Datenschutz	+	+
1	3-5	Allgemeine Bestimmungen	+	+
2	6-16	Öffentlicher Bereich	+	+
3	17-31	Privater Bereich		+
4	32-34	Internationaler Datenverkehr	+	+
5	35-47	Datenschutzinstitutionen	+	+
6	48-50	Strafbestimmungen	+	+
7	51-59	Übergangs- und Schlussbestimmungen	+	+

Tabelle 2: Gliederung des ÖDSG. Quelle: [Dohr96, 84].

Artikel 1 enthält das Grundrecht auf Datenschutz sowie die Kompetenzverteilung der Gesetzgebung und Vollziehung.

Artikel 2 gliedert sich in die folgenden 7 Abschnitte:

Allgemeine Bestimmungen - Bestimmungen für den öffentlichen Bereich - Bestimmungen für den privaten Bereich - Internationaler Datenverkehr - Kontrolle des Datenschutzrates - Strafbestimmungen - Übergangs- und Schlussbestimmungen [Mähr99, 14].

Weiter teilt sich das Gesetz in Bestimmungen auf, die ausschließlich für den öffentlichen Bereich[30] – das sind Datenverarbeitungen durch Bund, Länder, Gemeinden, Kammern, Sozialversicherung, etc. – gelten, in solche, die ausschließlich für den privaten Bereich – das sind Datenverarbeitungen ausschließlich durch private Un-

[30] Vgl. §§4 und 5 ÖDSG.

ternehmen, Vereine, politische Parteien oder Religionsgemeinschaften – gelten, und in solche, die für beide Bereiche gelten [Reichmann]. Die strenge Trennung aber zwischen dem öffentlichen und dem privaten Bereich, die im österreichischen Datenschutzgesetz 1978 existiert hat, wurde schon beim DSG 2000 aufgegeben [MB06, 24]. Die oben geschilderte Abbildung 3 zeigt diese Aufteilung. Der Datenschutz wird als ein „Recht auf informationelle Selbstbestimmung“ verstanden und bezieht sich also mehr auf personenbezogene Daten bzw. Schutz von Menschen vor den Folgen missbräuchlicher Datenverwendung und nicht auf den Schutz von Daten im Allgemeinen. Für personenbezogene Daten werden nachfolgende Grundsätze festgelegt [BaerRud02, 443].

- Personendaten dürfen nur auf rechtmäßige Weise beschafft werden.
- Die Bearbeitung muss glaubwürdig und verhältnismäßig zum Anwendungszweck sein.
- Personenbezogene Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Datenerhebung explizit angegeben wurde, implizit ersichtlich war oder gesetzlich vorgesehen ist.

Bei der Verarbeitung von personenbezogenen Daten brauchen Unternehmen entweder eine Rechtsgrundlage (aus dem Datenschutzgesetz oder Telekommunikationsgesetz) oder die Einwilligung von den Benutzern. Wenn das Datenschutzgesetz nicht eingreift, dann wird die Verarbeitung durch einen Vertrag zwischen Dienstanbieter und –nutzer geregelt. In diesem Fall kommen bei Verstößen gegen vertraglich vereinbarte Regelungen zivilrechtliche Ansprüche des Betroffenen wie z. B. Unterlassung und Schadenersatz zur Geltung [Zehentner02].

Die rasanten Entwicklungen in den Bereichen Internet und Mobilkommunikation erfordern einen modernen Datenschutz, der sich in unserem Zeitalter praktisch umsetzen soll. Bäumler beschreibt vier Grundprinzipien für „E-Privacy“ [Bäu00].

- *Rechtliche Absicherung*: Ohne die gesetzlichen Rahmenbedingungen wird es keinen wirklich wirkungsvollen Schutz geben – Gesetze regeln die Rechte und Pflichten für Bürger und Wirtschaft.
- *Technische Unterstützung*: Ohne technische Lösungen ist der Datenschutz in einer hochtechnisierbaren Welt nicht durchführbar (siehe Kapitel 5)

- *Selbstschutz*: Der Staat wird in Zukunft mehr Information, Service und Beratung für seine Bürgerinnen und Bürger bieten, damit sie Entscheidungen über die Herausgabe und Verwendung ihrer Daten treffen können.
- *Marktprinzipien*: Die Datenschutzpraxis muss bei einer erhöhten Nachfrage nach Datenschutz die Produktpalette von Unternehmen ganz selbstverständlich um Angebote zum Schutz der Privatsphäre ergänzen. In einem freien Wettbewerb sollen Unternehmen den Vorteil nutzen, Datenschutz zu gewährleisten [Ka04].

Die Konsequenz aus den obigen vier Punkten ist, dass die Gesetze ständig an die technische Entwicklung angepasst werden. Missbräuche können durch die Technologie nicht verhindert werden, aber es ist viel wichtiger, dass bei einer verantwortungsbewussten Datensammlung genügend Wissen über die möglichen technischen Lösungen vorhanden ist, das dem Einzelnen hilft, den Datenschutz umzusetzen [MaLa01].

Das Ziel eines modernen Datenschutzrechtes muss daran liegen, einen Ausgleich zu finden zwischen dem rechtsgültigen Informationsbedürfnis des Staates, der auf eine zuverlässige Datengrundlage angewiesen ist und einem Privatheitsinteresse der Bürgerinnen und Bürger, das daran liegt, sich nicht zu tief in die Karten schauen zu lassen [MaLa01].

4.2 Telekommunikationsgesetz

Mit dem Aufschwung des Internets, der Digitalisierung der Telekommunikationsnetze und den rasanten Aufstieg der Mobiltelephonie haben im letzten Jahrzehnt große Veränderungen stattgefunden, die auch zu Konsequenzen für die Privatsphäre führen. Hat es früher Schwierigkeiten bei der Datenspeicherung aufgrund der Zeit, des Ortes und der mangelnden Information gegeben, können jetzt in Sekunden Daten von einem Ort an den anderen übertragen werden. Daten können in kürzester Zeit gesammelt, miteinander verglichen und analysiert werden. Die Beteiligung an dem Telekommunikationsprozess ermöglicht dem Einzelnen tief in die Sphäre der anderen einzudringen.

Im Vergleich zum DSG 2000, wo im § 4 DSG nur zwischen „Daten“ („personenbezogenen Daten“[31]) und „sensiblen Daten“ („besonders schutzwürdige Daten“) unterschieden wird, unterscheidet der TKG 2003 zwischen Stammdaten, Verkehrsdaten, Zugangsdaten, Standortdaten und Inhaltsdaten (§92 TKG 2003) [CaPeJo00, 7,18] [Hof02, 95], [Him04, 119-122] :

„Stammdaten“ (§92 (3) 3 TKG 2003): das sind alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind: a) Familienname und Vorname, b) akademischer Grad, c) Adresse, d) Teilnehmernummer, e) Bonität. Nach Beendigung der Rechtsbeziehungen der Teilnehmer sind die Stammdaten zu löschen.

„Verkehrsdaten“ (früher „Vermittlungsdaten“) (§87. (3) 5. TKG 1997 bzw. §92 (3) 4 TKG 2003): das sind alle Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Verrechnung („der Fakturierung dieses Vorgangs“) verarbeitet werden. Die Aufzählung nach TKG 1997: dies sind: a) aktive und passive Teilnehmernummern, b) Anschrift des Teilnehmers, c) Art des Endgerätes, d) Gebührencode, e) Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, f) Art, Datum, Zeitpunkt und Dauer der Verbindung, g) übermittelte Datenmenge, h) andere Zahlungsinformationen wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen, entfallen. Die Definition der Datenkategorie nach TKG 1997: „Daten, die für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich sind“ ist auch nicht mehr enthalten. Verkehrsdaten dürfen gem. §99 TKG 2003 überhaupt nicht gespeichert werden und sind unverzüglich nach der Verbindung zu löschen bzw. zu anonymisieren, außer sie werden zu Verrechnungszwecke (sog „Billing“) benutzt. Dabei bleiben die Daten bis zum Ablauf der Einspruchsfrist gegen ausgestellte Rechnungen gespeichert. Dies erfolgt aber nur mit der Zustimmung des Teilnehmers oder der Teilnehmerin, die meist in den AGB enthalten ist. Die Telekom Austria z. B. gibt an, Verkehrsdaten innerhalb eines halben Jahres nach Begleichung der Rechnung zu löschen.

[31] Bei personenbezogenen Daten ist die Identität der Betroffenen bestimmt bzw. bestimmbar ist [CaPeJo00, 7].Bestimmbar ist eine Person, wenn sie direkt oder indirekt identifiziert werden kann [Hof02, 108].

„Zugangsdaten“ (§92 (3) 4a TKG 2003): es handelt sich um eine Untermenge von Verkehrsdaten, die beim Zugang zu einem Kommunikationsnetz und für die Zuordnung der Netzwerkadressierung zum Teilnehmer notwendig ist, und zwar um die meistens dynamisch vergebenen IP-Adressen im Internet.

„Standortdaten“ (§92 (3) 6 TKG 2003): diese Daten werden mit der EK-DS-RL und dem TKG 2003 neu definiert. Das sind „Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben. Gemeint sind hier lediglich die Standortdaten mobiler Endeinrichtungen“. Standortdaten, die keine Verkehrsdaten sind, dürfen nur in anonymisierter Form bzw. mit entsprechender Einwilligung verarbeitet werden.

„Inhaltsdaten“ (§92 (3) 5 TKG 2003): das sind die Inhalte übertragener Nachrichten. Ihre Speicherung darf gem. §95 TKG 2003 nur in einem sehr eingeschränkten Maß erfolgen und zwar nur, wenn die Speichern einen wesentlichen Bestandteil des Telekommunikationsdienstes darstellt wie z. B. bei Sprachmailboxdiensten: Diese Daten werden für eine vereinbarte Zeitspanne aufgenommen. Aber auf diese Daten darf natürlich bei polizeilichen oder nachrichtdienstlichen Aktivitäten zugegriffen werden.

Die unterschiedlichen Provider in Österreich haben verschiedene Regelungen bezüglich der Speicherung dieser sensiblen Daten. Und ohne allgemeingültige Aussagen muss der Internetnutzer davon ausgehen, dass sich seine Aktivitäten im Internet unterschiedlich und auch zu längeren Zeiträumen nachverfolgen lassen. In Österreich dürfen Daten nur aufgrund gesetzlicher Regelungen an Dritte weitergegeben bzw. zugänglich gemacht werden. Das heißt aber nicht, dass in der Realität ein unberechtigter Zugriff ausgeschlossen werden kann. Die Abschnitte 4.7.1 (E-Privacy aus der Sicht des Konsumenten) und 4.7.2 (E-Privacy aus der Sicht des Unternehmens) behandeln genau diese Problematik.

In nachfolgenden zwei Abschnitten werden aktuelle Privacy-Gesetze dargestellt.

4.3 Vorratdatenspeicherungsgesetz („Data Retention“)

In Österreich besteht gem. §96 Abs 3 TKG 2003 eine Informationspflicht jedes Anbieters, „welche Daten ermittelt, verarbeitet und übermittelt werden sowie auf welcher Rechtsgrundlage, wofür und für wie lange die Daten gespeichert werden (sog.

„Data Retention“)“ [POWZu06, 216]. Das erfolgt unabhängig vom Auskunftsrecht nach dem DSG 2000. Ein Verstoß gegen die Informationspflicht ist laut § 109 Abs 3 Z 16 TKG 2003 mit einer Verwaltungsstrafe bis zu EUR 37.000,- je Verstoß bedroht [POWZu06, 216]. In Deutschland ist dieses Datenspeicherungsgesetz ab 1. Januar 2008 in Kraft getreten. Nach dem Gesetz sollen massenhafte Telefon- und Internetverbindungsdaten, die vom Telefon, SMS oder Email zustande kommen, auf Vorrat (mindestens 1 Jahr) gespeichert werden. So ist es möglich, die Tätigkeiten einer Person oder eines Unternehmens im Nachhinein zu analysieren [ARGE08b].

4.4 Polizeisicherheitsgesetz

Ähnlich wie in Deutschland ist in Österreich auch ein Gesetz in Kraft getreten, das Polizeisicherheitsgesetz heißt und ab 6. Dezember 2008[32] gilt. Dadurch wird der Polizei gestattet, ohne einen gerichtlichen Beschluss eine Inhaltsüberwachung des Internetverkehrs zu tätigen. Dabei hat sie Zugriff auf die IP-Adressen und durch die Identifizierung der IP-Adresse werden auch die öffentlichen, privaten und persönlichen Kommunikationsinhalte identifiziert, zu einer bestimmten Person zugeordnet und analysiert (wie zum Beispiel Email, Chat oder VoIP). Das ist das gleiche, als ob jemand in der Wohnung steht und unsere privaten Gespräche abhört. Es ist Tatsache, dass die personenbezogenen Daten von uns gespeichert werden und erstmals ohne Gerichtsabschluss aus bestimmtem Anlass abgehört bzw. angesehen und bewertet werden dürfen.

Um einen personenbezogenen Schutz zu gewährleisten, sind Tools vorhanden, die einigermaßen die Identität des Benutzers verstecken oder ein anonymes Surfen ermöglichen.[33]

Das Datensammeln erstreckt sich nicht nur auf Österreich, sondern wird auf globaler Ebene durchgeführt. Die Datenverarbeiter können in Staaten ihren Sitz haben, die unzureichenden Datenschutz haben. Dadurch wird der mögliche Verlust der Privatsphäre größer und es bedarf internationaler Datenschutzsysteme. Daher werden nachfolgend die internationalen Datenschutzinitiativen der OECD dargestellt.

[32] Die Überwachungsverordnung für den Telefoniebereich, aber nicht für den Internetbereich stammt noch aus dem Jahr 2003. Siehe dazu http://www.heise.de/security/news/.
[33] Mehr Informationen dazu siehe Seite https://www.datenschutzzentrum.de/rotekarte/selbstschutz.htm/ Abruf am 2008-07-05.

4.5 Privacy Richtlinien der OECD

Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ist seit den 70er Jahren im Bereich des Datenschutzes aktiv. Am 23. September 1980 wurden die „Richtlinien für den Schutz der Privatsphäre und den grenzüberschreitenden Verkehr personenbezogener Daten“ verabschiedet, deren Grundlage die im Jahr 1973 aufgestellten Fair International Practices des United States Department for Health Education and Welfare (HEW) bilden. Das Ziel ist es, die verschiedenen Nationalgesetze bei einem Datenfluss von einem Land, wo die Daten hoch geschützt sind, zum anderen, das weniger Schutz bietet, auszugleichen und einen Schutz der Privatsphäre innerhalb der Europäischen Union zu gewährleisten. Die Organisation hat acht Grundsätze zum Schutz personenbezogener Daten aufgestellt [OECD80], [APS]:

- **Grundsatz der begrenzten Datenerhebung (collection limitation):** Es sollte eine Beschränkung der Sammlung personenbezogener Daten geben. Die Erhebung der Daten soll mit der Einwilligung des Datensubjekts erfolgen.
- **Grundsatz der Datenqualität (data quality):** Personenbezogene Daten müssen dem Verwendungszweck entsprechen und in dem für diesen Zweck nötigen Ausmaß genau, vollständig und aktuell sein.
- **Grundsatz der Zweckbestimmung (purpose specification):** Die Zwecke, für die personenbezogenen Daten erhoben werden, sollen im Einzelnen angegeben werden, spätestens bei der Beschaffung der Daten. Wenn es keinen Grund für die Beschaffung gibt, werden sie gelöscht. Das ist wichtig, damit man die Kontrolle über Daten nicht verliert und damit Datendiebstahl oder Datenkopien verhindert werden können.
- **Grundsatz der Nutzungsbestimmung (use limitation):** Personenbezogene Daten dürfen nicht offen gelegt, bereitgestellt oder für einen anderen Zweck als angegeben genutzt werden, außer per Gesetz oder mit der Einwilligung des Datensubjektes.
- **Grundsatz der Sicherheit (security):** Personenbezogene Daten sollen durch angemessene Sicherungsmaßnahmen gegen Risiken wie Verlust

oder unbefugten Zugang, Zerstörung, Nutzung, Veränderung oder Datenoffenlegung geschützt werden.

- **Grundsatz der Offenheit, Transparenz (openness):** Es soll allgemein gewährleistet werden, dass Entwicklung, Praxis und Politik hinsichtlich personenbezogener Daten durchschaubar sind.
- **Grundsatz des Mitspracherechts (individual participation):** Die Person soll ein Recht auf Auskunft über die Datenerfassung und Korrektur, Löschung, Vervollständigung und Änderung haben.
- **Grundsatz der Rechenschaftspflicht (accountability):** Der Datenverantwortliche soll für die Beachtung der Maßnahmen, welche den oben genannten Grundsätzen entsprechen einstehen bzw. sind diese dem Nutzer oder eine Behörde gegenüber rechenschaftspflichtig.

Da diese Richtlinien nicht bindend sind, stehen an ihrer Stelle meistens unübersichtliche Datenschutzregelungen. Daher wurde im Jahr 1995 die EU-Datenschutzrichtlinie (EU-DS-RL, die sogenannte „Direktive“) beschlossen und im Oktober 1998 in Kraft gesetzt. Diese regelt nicht nur eine Harmonisierung der Datenschutzgesetzgebung innerhalb der EU (DSG2000 wurde an der EU-DS-RL angepasst), sondern bindet auch den Export von Daten an ein angemessenes Schutzniveau [Peissl02].

Das Ziel der Direktive liegt darin, eine Angleichung der datenschutzrechtlichen Vorschriften der einzelnen EU-Mitgliedstaaten zu erreichen, um damit ein gleichwertiges Datenschutzniveau bei der Verarbeitung personenbezogener Daten innerhalb der Europäischer Union zu schaffen.[34] Den Individuen gibt man die Möglichkeit „bisher noch nie dagewesene Eigentumsrechte und Kontrolle über ihre persönlichen Informationen...“ [Braun00c] zu haben. Diese Angleichung ermöglicht einerseits einen ungehinderten Informationsfluss zwischen den Mitgliedstaaten, andererseits verbietet die Direktive einen Datentransfer in „nicht sichere Drittländer“ (außerhalb der EU), d.h. Länder, deren Datenschutzgesetze nicht den Schutz bieten, der von der Direktive vorgeschrieben wird. Daher beginnen viele Staaten, unter anderem Argentinien, die Schweiz und Kanada, ihre eigene Ge-

[34] Innerhalb der EU wird mit dieser Richtlinie somit ein datenschutzrechtlicher Mindeststandard vorgegeben, der es den Mitgliedstaaten ermöglicht, innerhalb des Europäischeren Binnenmarktes personenbezogene Daten auszutauschen [Geis97, 289 f.].

setzgebung zu harmonisieren, damit sie von der EU-Kommission als „sicheres Drittland“ bewertet werden und somit eine Möglichkeit bekommen, an dem europäischen Informationsfluss teilzunehmen (gemäß Art. 25, 26 EU-Datenschutzrichtlinie) [Lang04]. Artikel 25 EU-DS-RL kommt zur Geltung, wenn im Drittstaat eine angemessene Schutzbestimmung für personenbezogene Daten vorhanden ist, während Artikel 26 angewendet wird, wenn das Drittland kein unangemessenes Datenschutzniveau hat und die Übermittlung auf Grund eines Katalogs von Ausnahmetatbeständen erlaubt ist [Lange05, 131-135]. Die nachfolgende Abbildung zeigt der Verlauf, nach dem die EU-Kommission und die EU-Mitgliedstaaten entscheiden, ob ein Drittland ein angemessenes Schutzniveau für personenbezogene Daten aufweist oder nicht:

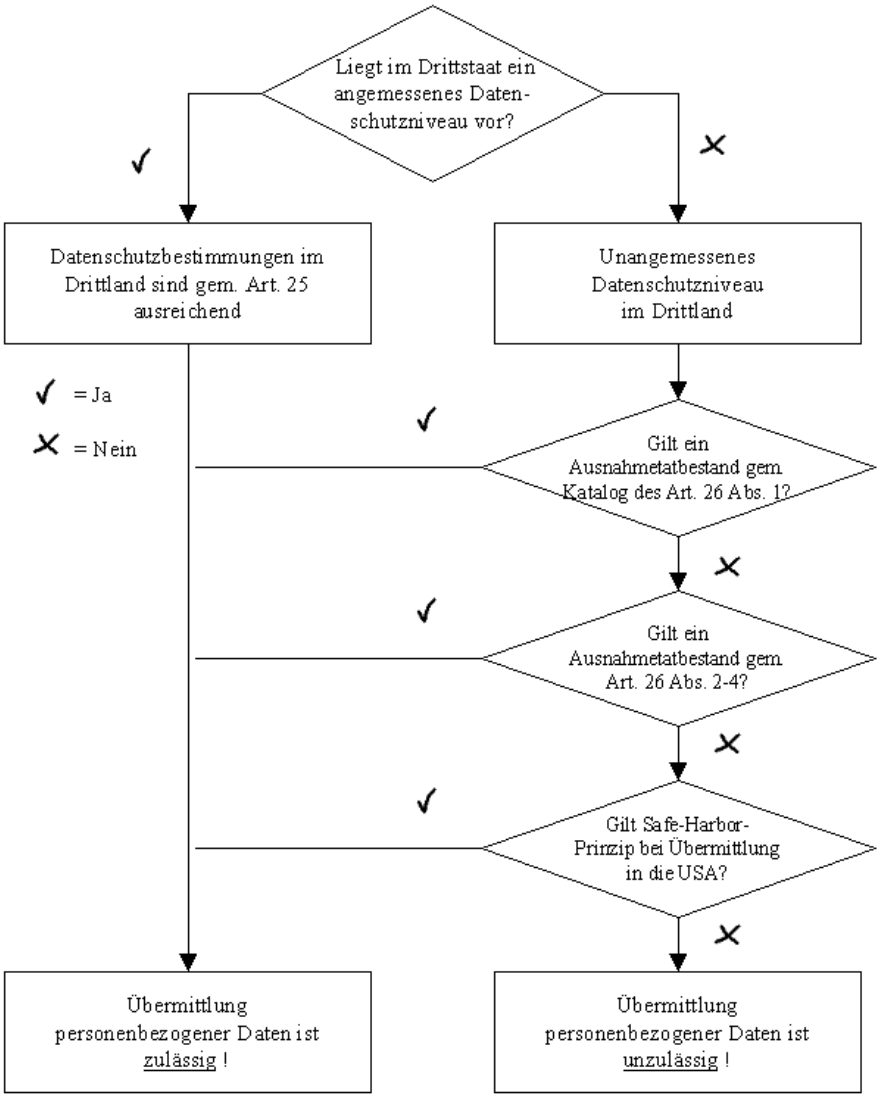


Abbildung 2: Zulässigkeit der Übermittlung personenbezogener Daten in Drittstaaten gemäß Art. 25, 26 EU-Datenschutzrichtlinie. Quelle: [Lange05, 133].

Auf den Lösungsansatz des „Safe-Harbor“ Prinzips, der zwischen den USA – als einer der größten Handelspartner der EU - und der EU im Mai 2000 entwickelt wurde, wird im nächsten Arbeitsteil noch näher eingegangen.

4.6 Situation in den USA

Im Gegensatz zu Europa, entwickelt sich in den USA das Privacy Konzept ganz anders als die Datensammlung seitens staatlicher Stellen. Die US-Regierung ist der Ansicht, dass die Wirtschaft selbstregulierend tätig werden soll, damit ein besser durchführbares System erzielbar ist, welches sich schneller und flexibler anpassen kann, was in der technologisch-dynamischen Welt von großer Bedeutung ist. Der Datenschutz dort funktioniert nach dem Prinzip „notice and choice“: Die Unternehmen legen ihre Datenverarbeitungsabsichten (Privacy Policy) offen und aufgrund dieser Erklärung kann sich jeder entscheiden, ob er bestimmte Tätigkeit abschließen will. Somit ist der Datenschutz ein Wettbewerbsvorteil und jedes Unternehmen versucht, diesen auszubauen. Infolge dieses Prozesses steigt auch das Schutzniveau enorm.

Im Vergleich zur staatlichen Regulierung bringt die Selbstregulierung erhebliche Vorteile. Sie reagiert schneller und flexibler auf die Probleme, kostet weniger und grenzüberschreitende Vereinbarungen sind leichter durchführbar. Die Selbstregulierung birgt aber auch Gefahren und Risiken in sich, da Interessen nur einseitig entwickelt werden und damit auf Kosten der öffentlichen Entscheidungsfreiheit durchgesetzt werden.[35] Es stellt sich somit die Frage, ob es einen einheitlichen gesetzlichen Datenschutz gibt, wenn ein grenzüberschreitender Datenverkehr stattfindet. Die Antwort ist die Umsetzung der erwähnten EU- Datenschutzrichtlinie aus dem Jahre 1995, in der eine Harmonisierung und Angleichung der Datenschutzbestimmungen der einzelnen EU-Mitgliedstaaten und damit ein gleichwertiges Datenschutzniveau bei der Verarbeitung der personenbezogener Daten innerhalb der Europäischen Union vorgesehen ist [Ka04], [Reichmann]. Das gilt aber nur innerhalb der EU. In den USA gibt es kein geschriebenes Recht in der Bundesverfassung außer in einigen Bundesstaaten, die sehr wohl über geschriebene Privacy- Rechte verfügen [Hof02, 117]. Dadurch, dass es wenige gesetzliche Regelungen in den USA gibt, gilt der Verstoß gegen die Privatsphäre als Bruch der Vereinbarung zwischen einem Unternehmen und einem Kunden und nicht als Ge-

[35] http://www.oeaw.ac.at/ita/ Selbstregulierung und Selbsthilfe.

setzesmissachtung. Um diese gesetzlich mangelnde Situation auszugleichen und aus EU-Sicht einen ausreichenden Schutz für den Bürger gegenüber „Drittstaaten“ wie den USA zu erreichen, wurde im Mai 2000 das „Safe Harbor“ Abkommen geschaffen. Dieses ist eine Vereinbarung, in der sich US-amerikanische Firmen zusammenschließen und verpflichten, bestimmte Datenschutzgrundsätze zu befolgen. Wenn US-Firmen mit Unternehmen in der EU personenbezogene Daten austauschen wollen, unterwerfen sie sich dabei freiwillig den EU-DS-RL. Die Federal Trade Commission soll amerikanische Unternehmen überwachen, die sich dem Safe Harbour-Abkommen unterwerfen. Durch die Bekanntmachung der Privacy Policy (Datenschutzerklärung) erklären Unternehmen, nicht nur bestimmte Datenschutzstandards einzuhalten, sondern erklären wettbewerbsrechtlich damit, Einfluss auf die Kaufentscheidungen bei Verbrauchern zu nehmen [Petri]. Unter den 192 Unternehmen bzw. Organisationen befinden sich auch Unternehmen wie TRUSTe oder BBBOnLine.[36] Nach diesem Abkommen verpflichten sich Organisationen, Informationen über die Verarbeitung von Benutzerdaten zur Verfügung zu stellen bzw. diese an natürliche Personen weiterzugeben. Demnach verpflichten sich Unternehmungen dazu, Benutzer darüber zu informieren, was mit ihren Daten passiert bzw. welche Daten zu welchem Zweck gesammelt werden und ob die Daten an Dritte weitergegeben werden oder nicht. So kann sich der Betroffene aussuchen, ob er mit der Weitergabe seiner Daten an Dritte einverstanden ist oder die Daten zu einem anderen Zweck als ursprünglich vorgesehen, verarbeitet werden dürfen. Wenn Daten an Dritte weitergegeben werden, die im Auftrag des Unternehmens die Daten verarbeiten, besteht keine Wahlmöglichkeit für den Betroffenen [Hof02, 161]. Ob die Datenschutzbestimmungen (engl. Privacy Policy) auch tatsächlich von den Unternehmen eingehalten werden wird im Kapitel 5.5 geklärt.

4.7 E- Privacy und E-Commerce

Das rapide Wachstum des Internets und seines populärsten Dienstes, dem World-Wide-Web (WWW), ermöglicht es dem Einzelnen einerseits Informationen aufzunehmen, andererseits führt uns diese enorme Möglichkeit, soziale und wirtschaftliche Vorteile zu gewinnen, in eine Welt, wo wir Informationen über uns preisgeben, indem wir neue Technologien benutzen. Ein typisches Beispiel ist E-Commerce,

[36] Mehr über TRUSTe bzw. BBBOnLine siehe Kapitel 5.8.1.

wo unzählige online Aktivitäten protokolliert, archiviert und oftmals zwecks Angebotsoptimierung analysiert werden.

Vielen Menschen ist nicht bewusst, was beim Surfen im Web passiert. Genau bei diesem „harmlosen“ Stöbern besteht eine Gefahr für die Privatsphäre.

Welche Faktoren müssen gegeben sein um zukünftig von einer sicheren Datenschutzsituation sprechen zu können?

In einer Studie „Surviving the Privacy Revolution” vom Februar 2001 begründet Forrester Research [For01], dass Privatheit einer der wichtigsten Gesichtspunkte beim Erfolg von E-Commerce ist, und dass Unternehmen, die keine Maßnahmen zum Schutz der Privatheit ihrer Kunden treffen, Nachteile erleiden könnten. Es müssen sichere Rahmenbedingungen geschaffen werden wie Rechtsregeln oder bestimmte Formen von Vertrauen (Gütesiegel), damit der Internethandel auch tatsächlich funktioniert [Spindler in MR01, 161].

Die vier Grundbausteine, die für eine Privatsphäre bei E-Commerce Umgebung unabdingbar sind, lassen anhand der nachfolgenden vier Aspekte identifizieren [Bäu00]:

- **Anonymität**: Wie kann ich meine personenbezogenen Daten verbergen bzw. nur selektiv preisgeben?
- **Vertraulichkeit**: Wie kann ich sicherstellen, dass unbefugte Dritte keinen Zugriff auf meine Daten haben? (inwieweit habe ich Kontrolle über meine Daten)
- **Transparenz**: Wie kann ich erfahren, welcher Aspekt meiner Person (Bewegungsmuster, Diskussionsbeiträge, etc.) zu irgendeinem Zeitpunkt überwacht wird, und unter welchen Umständen (d.h. Grund der Überwachung, Dauer der Datenspeicherung, Empfänger der Daten, etc.) dies geschieht? Oder anders formuliert: Wofür werden Informationen benötigt und wie werden diese verwendet und von wem?
- **Vertrauen und Absicherung**: Wem kann ich vertrauen und wer kann mir im Konfliktfall helfen?

Die Transaktionen im E-Commerce benötigen eine enorme Menge von personenbezogenen Informationen, die entweder für eine bestimmte Aktion benötigt (z. B. Kreditkarteninformation, Lieferungsangaben) oder vom E-Business verlangt wer-

den: der Zugang zu diesen Informationen ermöglicht es Daten zu analysieren, neue Trends herauszufinden und somit die Effizienz von den E-Commerce-Aktivitäten zu optimieren. Die Konsumenten erfahren meistens, dass durch ihre Onlinetätigkeiten potentiell ihre Privacy verletzt werden kann, ohne dass sie diesem Vorgang zugestimmt haben. In der Neuen Welt des Informationszeitalters und des E-Commerce eröffnet sich die Notwendigkeit bzw. die Möglichkeit, einen Ausgleich zwischen dem öffentlichen Interesse und den „Privacy"-Aspekten zu finden. Das ist jene schon bereits erwähnte Möglichkeit, bei der das Individuum seine Privacy maximal aufrechterhält, und gleichzeitig aber seine preisgegebenen personenbezogenen Daten, die es nach außen gegeben hat, kontrollieren kann.

E-Privacy zielt nach Datensparsamkeit, es wird genau soviel Wissen über Personen gesammelt und gespeichert, wie für die Zusammenarbeit notwendig ist. E-Commerce optimiert im Gegensatz dazu die Kundenbindung. Diese erzielt man nur, wenn man mehr Vertrauen und Wissen von ihren Kunden gewinnt. Vor diesem Hintergrund führt der Mangel an E-Privacy dazu, dass das Wachstum von E-Commerce behindert wird. Und am Ende könnte es weder E-Privacy noch E-Commerce geben [GLN00]. Eine Entwicklung, die ebenfalls von niemanden gewünscht wird.

4.7.1 E-Privacy aus der Sicht des Konsumenten

Im Internet geben immer mehr Nutzer, meistens freiwillig, ihre Intimität preis. Die Videoplattform YouTube[37] z. B. lockt Millionen von Menschen mit dem Slogan „Broadcast yourself". Auf der Videoplattform können Benutzer Heimvideos online veröffentlichen, in denen private Einzelheiten wie der komplette Lebenslauf, bisherige Arbeitsgeber, Hobbys etc. public werden. Diese privaten Daten stellen wertvolle Ressourcen für die Werbeindustrie dar. Dabei verlieren die Konsumenten nicht nur vollständig die Kontrolle über diese Daten, sondern sie werden zudem auch ihrer Privatsphäre beraubt.

Bei der Erhebung personenbezogener Daten sollte nicht nur aus datenschutzrechtlichen Gründen behutsam vorgegangen werden. Wenn der Internetanbieter den Nutzer sofort nach Name, Adresse begrüßt, wird der Kunde schnell abgeschreckt. In einem realen Geschäft zeigt man auch nicht gleich den Personalausweis, nur

[37] http//www.youtube.com/.

weil man eine Umkleidekabine betritt. Für den Kunden müssen die größtmögliche Anonymität, Vertrauen, und persönliche Vorlieben fragt, um diesen beim nächsten Besuch mit einem personalisierten Angebot zu Transparenz und Sicherheit gewährleistet werden. Vor dem Hintergrund dieses Zusammenhangs, werden im nachfolgenden Kapitel die wichtigsten Begriffe in Bezug auf diesen Forschungsaspekt geklärt.

4.7.1.1 Anonymität und Vertraulichkeit

In einer Welt, wo der Mensch viele seiner Entscheidungen und Handlungen dem Computer überlässt, gibt er automatisch einen Teil seiner Autonomie auf. Es funktioniert wie ein Tauschhandel: der Nutzer sucht etwas, er bekommt durch die Suchmaschine seine Antwort und im Gegensatz dazu - bewusst oder unbewusst – gibt er Information über seine eigene Person preis. Dadurch, dass jeder Computer im Internet durch eine IP-Adresse[38] bis zu einem bestimmten Grad identifizierbar ist, lassen sich Nutzer leicht online verfolgen. Besteht dadurch eine Personenbezogenheit? „Nach Art 2 lit. a DS-RL sind unter personenbezogenen Daten all jene Informationen über eine (natürliche) Person zu verstehen, durch die eine Person bestimmt oder bestimmbar ist. Bestimmbar ist eine Person, sofern sie direkt oder indirekt identifiziert werden kann, insbesondere durch die Zuordnung zu einer Kennnummer… “. Die Identifizierbarkeit des Nutzers hängt somit von den eingesetzten Mitteln ab [Hof02, 108]. Die IP-Adresse des Computers zählt zu diesen Kennnummern. Heißt dies aber, dass ein- und dieselbe Person durch die IP-Adresse zu identifizieren ist? Ob IP-Adressen personenbezogene Daten sind, hängt davon ab, ob der Datenverarbeiter in der Lage ist, den Bezug zu einer Person mit den ihm zur Verfügung stehenden Mitteln herzustellen. Was unter eingesetzten Mitteln zu verstehen ist, ist in den Richtlinien nicht zu erfahren. Nach Hofer [Hof02, 109] nimmt man bei dynamischen IP-Adressen die Herleitung des Personenbezugs aufgrund dessen, dass der Benutzer bei jeder neuen Verbindung eine neue Nummer bekommt, aber mit der Zunahme von Breitbandzugängen, die meistens mit statischen IP-Adressen arbeiten, ist die Identifizierung von PCs über die IP-Adresse sehr leicht. Deswegen wurden Anonymisierungstools geschaffen, um die IP-Adressen zu verbergen. So wird es technisch aufwändiger zu beobachten,

[38] IP-Adresse: Jeder Computer besitzt eine Nummer zum Zentralrechner (Domain) im Internet. Man unterscheidet zwischen statischen (dieselbe Adresse bei der Einwahl in das Internet) und dynamischen Adressen (aus einem Pool vergebene Adresse) [Hof02, 109].

wer mit wem im Internet kommuniziert. Dagegen besteht bei dynamischen IP-Adressen ohne Zusatzinformationen keine Möglichkeit, die Identität des Nutzers zu erfahren, da die IP-Adresse aus einem Pool von Adressen immer wieder neu vergeben wird. Ein Personenbezug dieser Daten allein ist zu verneinen, außer der Nutzer stellt diesen selbst her.

Keine personenbezogenen Daten sind anonyme Daten. Aber in der E-Welt verschwimmt langsam die Grenze zwischen der Anonymisierung und Personenbezogenheit. Aktivitäten, die vielfältige Datenspuren hinterlassen, werden zu einem Profil zusammengefasst. Die Frage ist, wie vertraut werden diese Profile behandelt, werden sie zu einem anderem als dem angegebenen Zweck verwendet und werden sie an Dritte weitergeleitet. Solche Aktivitäten erfolgen sehr oft ohne Wissen und Wollen des Betroffenen und geraten in Konflikt mit der informationellen Selbstbestimmung, die als zentrales Grundrecht der Informationsgesellschaft gilt [Ross07, 9,11]. Damit der Einzelne geschützt wird und sich frei entfalten und entwickeln kann, muss er die Preisgabe von Angaben über sich kontrollieren können, d.h. die betreffenden Daten bei Bedarf korrigieren, löschen oder bezüglich des Verwendungszwecks Beschränkungen aussprechen können.

4.7.1.2 Transparenz

Ein großes Problem stellt die fehlende Transparenz dar. Für die Konsumenten ist es meistens nicht nachvollziehbar, wem sie ihre Daten hinterlassen. Wenn sie ihre personenbezogenen Daten sehr detailliert angeben, dann nur wenn sie eine entsprechende Gegenleistung oder Zusatznutzen an Produkten und Leistungen bekommen, wie z. B. Rabatte oder personalisierte Services [CaPeJo00, 16]. Jupiter Research 2002 zeigt, dass sogar Personen, die sehr besorgt in Bezug auf ihre Privacy sind, bereit sind, mehr Informationen über sich preiszugeben, wenn sie im einen bestimmten Nutzen daraus ziehen [AG04]. Eine internationale Studie [HaHuLeePng03] ermittelte sogar, für wieviel Bequemlichkeit (Zeitersparnis) oder welche Geldsumme die befragten Studenten ihre personenbezogenen Daten preisgeben würden. Aufgrund der Ergebnisse konnten die befragten Personen in die drei nachfolgenden Gruppen unterteilt werden.

„Privacy guardians“: 72% der Befragten in den USA und 84% der Befragten in Singapur lassen sich die Vertraulichkeit ihrer Daten nur schwer abkaufen,

„Information seller“: Unter diese Gruppe fallen 20% der US-Teilnehmer und 8% der Singapur-Teilnehmer. Sie geben ihre Daten ohne Probleme preis, wenn man ihnen genug bietet. (z. B. Geld)

„Convenience seekers“: Unter diese Gruppe fallen 7% der Befragten aus beiden Ländern. Die Gruppe dieser Befragten tauscht ihre Daten gegen Bequemlichkeit. Wenn man z. B. beim nächsten Webseitebesuch schneller Online-Einkäufe erledigen kann, ist man dazu bereit seine persönlichen Daten preiszugeben.

Eine absolute Anonymität im Internet ist unmöglich, aber auch nicht immer sinnvoll. Bei Online-Transaktionsplattformen wie z. B. Online-Shops benötigt man die Eingabe kundenbezogener Information wie die Angabe der Lieferadresse, damit die bestellte Ware an den richtigen Platz geliefert werden kann. Damit der Datenschutz gewährleistet wird, ist eine sichere Datenübertragung erforderlich und der Grundsatz der Transparenz ist zu befolgen. Jedem soll die Möglichkeit gegeben werden, sich über die Herausgabe personenbezogener Daten und deren Bearbeitung zu informieren. Daher muss sich der Benutzer im Internet über die möglichen Folgen vor seiner Zustimmung informieren. Einen Hinweis darauf stellen die publizierten Datenschutzregeln dar, die sogenannten Privacy Policy[39], die auf der Webseite des Anbieters publiziert werden, um dem Nutzer Informationen darüber zu geben, was mit seinen personenbezogenen Daten geschieht. Es werden im Allgemeinen Namen, E-Mail-Adresse, die zu Werbezwecken genutzt werden, angefordert. Über das Netzwerk sind Daten wie IP-Adresse, Information über den benutzten Browser und ISP (Internet Service Provider) ersichtlich. Manche Unternehmen geben bekannt, dass sie finanzielle Information hinsichtlich über den Endbenutzern über Dritte wie z. B. der SCHUFA AG einholen, die prüft, ob jemand kreditwürdig ist oder nicht. Wenn keine personenbezogenen Daten gespeichert werden, greift das DSG nicht und das Unternehmen befindet sich auf unsicherem Terrain [CaPeJo00; MaLa01].

Eine Hilfestellung zur Kontrolle und Transparenz des Nutzers im Netz wird durch die vom World Wide Web Consortium (W3W) unterstützte Platform for Privacy Preferences (P3P)[40] erreicht, die es dem Benutzer ermöglicht, das eigene Profil bzw. die eigenen Privacy Präferenzen mit den Privacy Policies eines Unternehmens zu

[39] näher dazu im Kapitel 5.7 Definition und Bestimmung einer E-Privacy Policy aus der Unternehmensseite.
[40] näher über P3P siehe Kapitel 5.1 Plattform for Privacy Preferences Project (P3P).

vergleichen. Die Bereitschaft des Benutzers, persönliche Daten im Netz zur Verfügung zu stellen, wird letztendlich nicht nur vom Nutzen des Dienstanbieters abhängen, sondern auch, inwieweit durch die Transparenz der Datenverarbeitung das notwendige Vertrauen der Nutzer gewonnen werden kann. Mit P3P kann zusätzlich Transparenz erreicht werden. Der Nutzer muss nicht jedes Mal die Privacy Policy jeder Webseite studieren, da dieser Schritt von P3P automatisiert wird. Damit er dem Internetdienstanbieter vertrauen kann, lassen Unternehmen ihr Verhalten von unabhängigen Organisationen wie TRUSTe[41] und BBBOnLine[42] untersuchen. Die dort angebotenen Zertifizierungen oder Gütesiegel vermitteln glaubhaft die Qualität des Produktes und bauen damit die Voraussetzung für das nötige Vertrauen beim Endbenutzer auf, das im Internet so wichtig ist [Spindler in MR01, 169].

4.7.1.3 Vertrauen und Absicherung

Bei der Zustimmung zur Privacy Policy eines Unternehmens weiß der Kunde im E-Commerce meistens nicht, ob diese wirklich eingehalten wird und kann auch nicht verhindern, dass die Privacy Policy später geändert wird. Einmal eingewilligt, kann er auch nicht durch eine technische Unterstützung zurücktreten, was ihm eigentlich nach dem Datenschutzgesetz zusteht. Daher spielt Vertrauen im E-Commerce eine wichtige Rolle, insbesondere im Privatkundengeschäft bzw. B2C-Bereich[43]. Das könnte durch technische Unterstützung ausgeglichen werden, auf die im Kapitel 5 „Privacy Enhancing Technologien“ näher eingegangen wird. Vertrauensinstitutionen, die bestimmte Gütesiegel anbieten, sollen die Privacy Policy vom Unternehmen überprüfen und sicherstellen, dass sie auch tatsächlich eingehalten wird. Dadurch wird die Sicherheit erhöht, das Vertrauen verstärkt und somit der E-Commerce gefördert. Interessant sind die Aussagen einer Umfrage von Economic and Social Research Council [Eco07] im November 2007, bei der Internet Nutzer online beobachtet wurden und deren Ergebnisse mit ihren Aussagen über die Privacy verglichen wurden. Unternehmen, die bestimmte personenbezogene Daten von Benutzer verlangen und dabei mehr Vertrauen bei ihnen gewinnen als andere, bekommen mehr Details über die entsprechende Person als üblich. Sogar Leute, die einen hohen Grad an Interesse am Schutz ihrer Privacy aufzeigen, sind einver-

[41] http://www.truste.org/, mehr dazu Kapitel 5.6.1.
[42] http://www.bbbonline.org/, mehr dazu Kapitel 5.6.1.
[43] Abkürzung für Business to Customer = Privatkundengeschäft.

standen, Privacy Verluste zu akzeptieren, wenn sie dem Empfänger ihrer Daten vertrauen. Ungefähr 56% Prozent gaben an, Bedenken über ihre Privatsphäre zu haben, wenn sie online sind. Das Verhalten online hängt davon ab, ob sie die Seite als vertrauenswürdig einstufen oder nicht. Wenn die Seite vertrauenswürdig erscheint, sind die Benutzer eher bereit, ihre Privatsphäre preiszugeben, als wenn sie nicht so sicher wirkt. Dann verhalten sich Kunden vorsichtiger als sonst [Eco07].

Der Grad wie viel Privacy offenbar wird, wird von dem Design der Formulierung von Fragen und Antworten auf der Seite beeinflusst. Wenn die Antwort „Ich würde lieber nichts sagen“ ganz oben von den Wahloptionen steht, sind die Nutzer eher bereit, mehr personenbezogene Information preiszugeben, als wenn ihnen die Möglichkeit gegeben wurde, nicht genaue Information anzugeben wie zum Beispiel ein Gehalt zwischen £10.000- £50.000 p.a [Eco07].

Ein interessanter Aspekt ist, dass Benutzer, die beunruhigt über ihre Privacy sind, online genau gegensätzlich zu ihren Aussagen reagieren, wenn diese unter bestimmten Konditionen gestellt wurden. Daher spielt das Empfinden der Nutzer eine wichtige Rolle und ermöglicht es den Erfolg einer angebotenen Leistung zu steigern [Eco07].

4.7.2 E-Privacy aus der Sicht des Unternehmens

Unternehmen erhöhen durch eine personalisierte Behandlung die Zufriedenheit und Treue ihrer Kunden und damit letztendlich den eigenen Umsatz und Gewinn [Sack07]. Meistens aber ergibt sich eine Vertrauenslücke seitens der Kunden. Daher sind Daten gegenüber Kunden als Wertgegenstand zu verstehen, welcher von den Unternehmen als Wettbewerbsvorteil genutzt und der vor unbefugten Zugriffen geschützt werden soll. Das spiegelt sich in den dargestellten Privacy Policies des Unternehmens wider, die das Ziel haben, einerseits die Konsumenten zu überzeugen, dass ihre Daten gesetzkonform aufbewahrt werden und andererseits das Unternehmen von anderen unterscheiden soll, um Vertrauen aufzubauen. Beispiel dafür ist IBM, das seine Privacy Policy als Markendifferenzierer („brand differentiator“) nutzt [APS].

Meistens aber ergeben sich Probleme im Unternehmen seitens unvorsichtiger Mitarbeiter, die unbewusst Auskünfte weiterleiten. Daher benötigt man Mechanismen

des Datenschutzes, die einen Schutz vor Missbrauch Dritter (Mitarbeiter, Lieferanten, Konkurrenzunternehmen) schaffen sollen. [BaerRud02, 447]

Die Grenze zwischen Missbrauch und Gebrauch von Daten aus Unternehmenssicht ist sehr oft nicht klar. Das betrifft vor allem viele internationale Firmen, die unterschiedliche nationale Gesetze haben. Die globale Harmonisierung der Gesetzgebung, die Anforderungen in Bezug auf das Sammeln, die Nutzung, Speicherung und Weitergabe personenbezogener Information verlangen von Unternehmen, dass sie diese Bestimmungen befolgen. Ob das der Realität entspricht, hängt von jedem Unternehmen einzeln ab.

Die Federal Trade Commission (FTC)[44] in den USA legte 2001 eine erfolgreiche Klage gegen dem Online-Spielzeughändler Toysmart ein. Der Verkauf der Kundendaten sei gegen den Privacy Policies des Unternehmens gewesen, die den Kunden zugesichert haben, dass Daten an keine Dritten verkauft werden sollten. Dies zeigt, dass angegebene Datenschutzerklärungen (Privacy Policies) auch eingehalten werden müssen [Pilz01]. Denn die Anwendung nationaler Gesetze in grenzüberschreitendem Internet ist oft sehr problematisch [Bäu00]. Dazu kommt die unübersichtliche Platzierung der Privacy Policies, die mit zahlreichen rechtlichen Begriffen dargestellt werden und schwierig zu verstehen sind. Im nachfolgenden Abschnitt werden Technologien dargestellt, die das Management der Privacy Policies erleichtern und mehr Transparenz schaffen.

[44] http://www.ftc.gov/.

Kapitel 5

5 Privacy Enhancing Technologien

Wie bereits erwähnt, ist der moderne Datenschutz auf zahlreiche Technologien angewiesen: Produkte, Instrumente, Strategien und auch Infrastrukturen, die datenschutzrechtliche Anforderungen erfüllen sollen, damit elektronische Kommunikation reibungslos funktioniert. Meistens aber weiß niemand, wie weit der Mensch in Bezug auf die Herausgabe personenbezogener Daten gehen kann, damit seine Privatsphäre geschützt bleibt [CaPe02; AdTu05]. Gerade hier entstehen Probleme, die mithilfe der Technik beseitigt oder zumindest teilweise behoben werden können. Daher wurden die sogenannten „Privacy Enhancing Technologies" (PETs)[45] entwickelt. Eine technisch sichere Umgebung, v. a. ihre Bedienungsfreundlichkeit, weckt beim Nutzer Vertrauen. Und Vertrauen ist eine Grundvoraussetzung für seine Teilnahme an elektronischen Transaktionen [MR01, 195-197].

Bei PETs geht es vorrangig um die anonyme und pseudonyme Nutzung von Diensten, wobei der Nutzer in der Wahrung seiner Privatsphäre unterstützt wird [Sack07]. Möglichkeiten zum Einsatz von PETs unterteilen sich in folgende Gruppen: Verschlüsselung, Anonymisierungsdienste und Einsatz von Datenschutzsoftware („Privacy Tools" bzw. „Privacy Policy Frameworks") [CaPe02]. Die letztere Gruppe nimmt bei dieser Arbeit eine wichtige Rolle ein. Sie wird dazu benutzt, die Sammlung und Verarbeitung personenbezogener Daten zu überwachen und den Nutzer über mögliche Erhebungen zu informieren. Ein wichtiger Vertreter hiervon ist das Plattform for Privacy Preferences Project (P3P)[46].

Laut Adomavicius und Tuzhilin müssen PETs jedoch „zwangsläufig versagen", da eine Datenvermeidung durch technische Schutzmechanismen nicht weiter garantiert werden kann [AdTu05]. Sie sprechen von einem „Zwang zur Transparenz", d.h. die Menschen akzeptieren die Vorteile neuer Technologien und damit die Preisgabe ihrer personenbezogenen Daten, aber ihre Privacy wird dabei nicht tatsächlich bewahrt. Deswegen ist es für Konsumenten wichtig zu erfahren, was mit ihren Daten passiert. Dadurch wächst die Transparenz und damit auch die Kontrollmöglichkeit über die von ihnen weitergegebenen Daten. Denn ein Verzicht auf

[45] In dieser Arbeit wird der englische Begriff PETs benutzt.
[46] Näheres hierzu in Kapitel 5.1 Plattform for Privacy Preferences Project (P3P).

die Herausgabe personenbezogener Daten bedeutet gleichzeitig Verzicht auf personalisierte Dienste - und dies führt damit letztlich zum Verzicht von Kundenvorteilen. Das folgende Kapitel beschäftigt sich eingehender mit PETs, insbesondere P3P.

5.1 Plattform for Privacy Preferences Project (P3P)

P3P (Plattform for Privacy Preferences Project)[47], auf Deutsch „Plattform für Datenschutzpräferenzen“, ist eine technische Plattform zum Austausch von Datenschutzinformationen. Es handelt sich um einen vom W3C (World Wide Web Consortium) entwickelten Standard zum Schutz der Privatsphäre des Anwenders bei der Nutzung des Internets. Hierbei waren u. a. Firmen wie AOL, IBM und Microsoft beteiligt. Nach seiner Verabschiedung im Jahr 2002 soll dieser Standard nach Beendigung seines Entwicklungsstadiums in alle Browser und Websites implementiert werden. Mithilfe von P3P wird die Privacy Policy[48] eines Websitebetreibers in einem vorgegebenen Format (z. B. XML)[49] so dargestellt, dass sie von einem P3P-fähigen Browser oder P3P-Agent automatisch gelesen und mit den Privacy-Einstellungen des Nutzers verglichen werden kann.

P3P ist so konzipiert, dass jeder Internetbenutzer vor dem Surfen seine Präferenzen angibt, d.h. er bestimmt, welche seiner personenbezogenen Daten preisgegeben und wie verwendet werden dürfen, und kann so seine Privatsphäre optimal schützen [Mey02, 27 ff.]. Ziel dieses Standards ist es, eine einheitliche Sprache für die Schutzanforderungen persönlicher Daten festzulegen [FHW01]. Es ist für den Benutzer wichtig zu wissen, wer seine Daten erhält bzw. sammelt (bleiben sie beim Webseitenbetreiber oder werden sie an Dritte weitergegeben), welche Informationen genau gespeichert werden, zu welchem Zweck sie erhoben werden (zum Beispiel zu Marketingzwecken) und ob er später seine Daten ändern bzw. löschen kann. Anwender benutzen P3P, um ihre eigenen Richtlinien bzgl. der Verwendung ihrer persönlichen Daten festzulegen. Die Betreiber von WWW-Servern können mithilfe von P3P ihre eigene Politik in Bezug auf die personenbezogenen Daten ihrer Anwender einheitlich beschreiben [Lang02].

[47] http://www.w3.org/p3p/.
[48] Näheres zu Privacy Policy siehe Kapitel 5.4 E-Privacy Policy auf Unternehmensseite.
[49] Die Extensible Markup Language (XML) ist eine Metasprache für Dokumentbeschreibungen, die vom W3C (World Wide Web Consortium) betreut wird. Sie ist strukturiert und maschinenlesbar.

Der Browser vergleicht nun die vom Benutzer eingestellten „Datenverarbeitungskriterien“ mit der Datenschutzerklärung („Privacy Policy“) des Websitebetreibers. Entspricht diese den Vorstellungen des Benutzers, wird die Webseite angezeigt. Falls nicht, wird die Aktion abgebrochen und der Benutzer kann die Seite nicht besuchen. Es sei denn, er entscheidet sich, nachdem er die Browserwarnung gelesen hat, explizit dafür, die Seite trotzdem zu sehen.

Benutzer wollen sich in den seltensten Fällen eingehender mit der Privacy Policy einer Webseite beschäftigen. Mittels P3P können sie sich die Datenschutzpraktiken, übersichtlich zusammengefasst ansehen und selbst entscheiden, ob sie ihre personenbezogenen Daten preisgeben wollen. Dass dieses Prozedere automatisch abläuft, vereinfacht das Ganze. Dadurch werden sowohl Transparenz als auch Datenschutz verbessert, da es dadurch selbst für einen Laien möglich wird, zu erkennen, ob die Behandlung seiner personenbezogenen Daten tatsächlich mit seinen Vorstellungen übereinstimmt [Lang02; Hof02, 139]. Die folgende Grafik zeigt, wie P3P genau funktioniert:

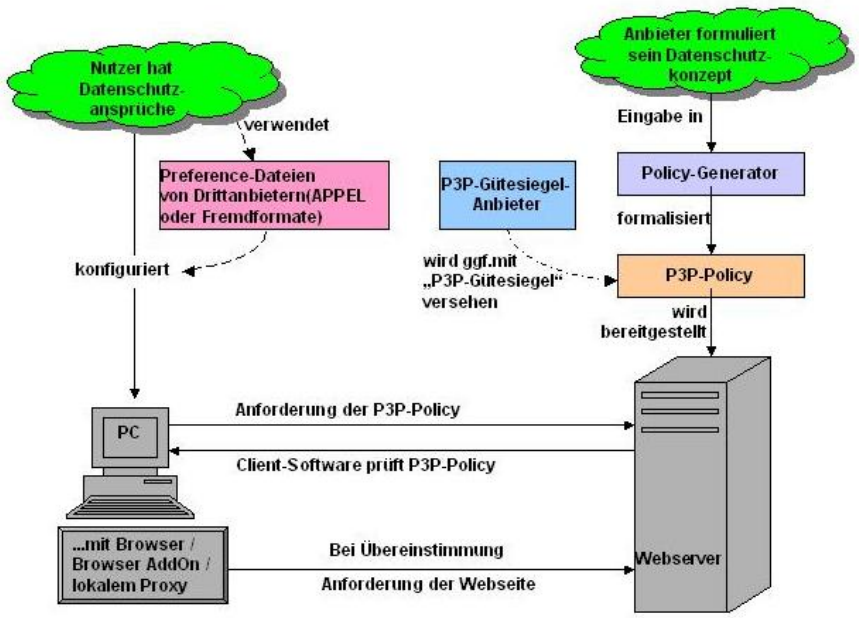


Abbildung 3: Funktionsweise von P3P. Quelle: https://www.datenschutzzentrum.de/selbstdatenschutz/p3p/grafiken/p3p_flow_1.jpg.

Noch deutlicher wird die Funktionsweise von P3P anhand der nächsten Graphik:

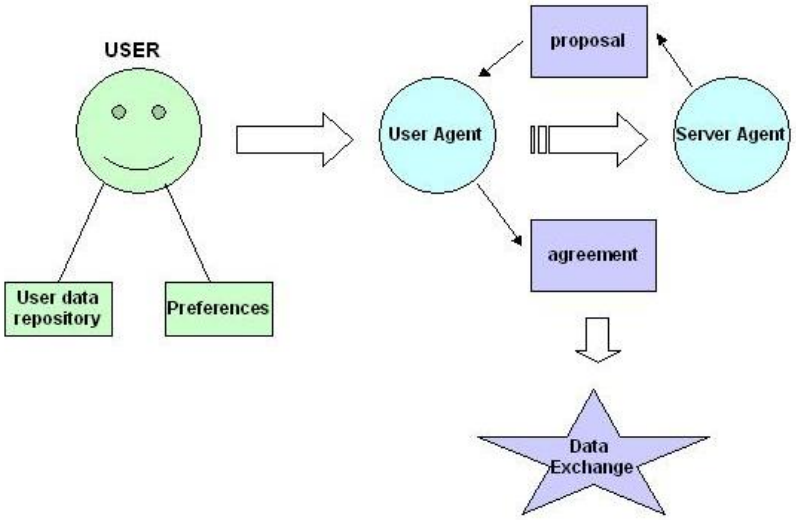


Abbildung 4: P3P. Quelle: [Wäll00].

Eine P3P-Transaktion funktioniert im Einzelnen wie folgt: Der Benutzer (User) speichert seine Präferenzen in einem „User Agent“ wie z. B. dem Internet Explorer. Beim Abruf einer Webseite mit einem P3P-fähigen Browser bzw. einem P3P-Agenten nimmt dieser „User Agent“ vor der Datenübertragung Kontakt mit einem Agenten des in Anspruch genommenen Dienstes („Server Agent“) auf. Er vergleicht die Einstellungen des Benutzers mit der Privacy-Politik des Unternehmens. Diese wird ihm von einem P3P-Agent auf der Serverseite in maschinenlesbarer Form bereitgestellt. Die Privacy-Politik wird in einer sogenannten „safe zone“ aufgerufen und in den Cache[50] geladen. Der Server Agent sendet sodann einen sog. Vorschlag (proposal) an den User Agent. In diesem ist angegeben, welche Daten abgerufen oder gespeichert werden sollen, was der Agent mit diesen Daten machen möchte und welche Konsequenzen dies für den Anwender hat. Der User Agent antwortet darauf mit einer Vereinbarung (agreement). Stimmen die Präferenzen des Benutzers (Users) und die Privacy-Politik des Unternehmens überein, kommt es zu einem Datenaustausch. Bei jedem Besuch dieser Seite überprüft der Agent die Privacy-Politik auf Änderungen. Stellt er keine Veränderungen fest, wird automatisch die Datenübermittlung eingeleitet, falls doch, beginnt der gesamte Prozess von neuem [Wäll00]. Das Vertrauen des Benutzers wird gestärkt, weil er mittels P3P die Weitergabe seiner Daten vollständig kontrollieren kann: Der Benut-

[50] Cache bedeutet in der EDV einen schnellen Puffer-Speicher. Mehr dazu unter http://de.wikipedia.org/wiki/Cache/.

zer kann seine Präferenzen überprüfen, ändern oder löschen und ist damit immer über einen möglichen Datenaustausch informiert [Grill06].

Allerdings kann der P3P-Agent nicht garantieren, dass die von einem Unternehmen publizierten Datenschutzerklärungen auch tatsächlich eingehalten werden. Eine Verifizierung dieser Angaben kann er schlichtweg nicht leisten. In Kapitel 5.6 (Einhaltung von Privacy Policy) wird näher auf diese Problematik eingegangen.

5.1.1 Plattform for Privacy Preferences Project (P3P) User Agents

Wie bereits oben erwähnt, ist der User Agent dafür zuständig, die Privacy Policy eines Unternehmens und den Präferenzen eines Benutzers zu vergleichen und entsprechend zu reagieren. Er hilft dem Benutzer dabei, die Weitergabe seiner Daten besser zu kontrollieren. Manche User Agents liefern eine Zusammenfassung der Privacy Policy, andere teilen mit, dass ein Privacy Seal (siehe Kapitel 5.6.1) vorhanden ist, dritte stellen einen Button bereit, der ohne umständliches Suchen direkt zur (menschenlesbaren) Privacy Policy der Webseite führt, ohne dass sich der Benutzer die Mühe geben muss, diese auf der Seite zu suchen. Das W3C gibt zurzeit vier User Agents/Proxies an, die verwendet werden könnten [W3Cb]:

- Internet Explorer 6.0
- Netscape 7.0
- JRC P3P Proxy
- AT&T Privacy Bird

Im Microsoft Internet Explorer (ab Version 6.0) und Netscape 7 sind P3P User Agents bereits integriert [GolLe01]. Andere User Agents wie zum Beispiel Privacy Bird (siehe Kapitel 5.1.1.4) sind als Add-ons im Internet kostenfrei verfügbar.

Im nachfolgenden Abschnitt wird auf die P3P User Agents näher eingegangen.

5.1.1.1 Internet Explorer

Die P3P-Datenschutzrichtlinien finden sich beim Internet Explorer ab Version 6.0 (IE6) im Menüpunkt „Ansicht“ → „Datenschutzbericht...“. So kann die Datenschutzrichtlinie jeder abgerufenen Webseite, sofern eine solche existiert, in natürlicher Sprache angesehen werden. In einem sog. Container-Element wird die P3P-

Policy zusammengefasst und anhand bestimmter Fragen und Antworten dargestellt (siehe Abbildung 5). Typische Fragen sind z. B.:

- Welche Arten von Daten werden gesammelt?
- Zu welchem Zweck werden die Daten gesammelt?
- Wer erhält Zugriff auf die gesammelten Daten?
- Wie lange werden die gesammelten Daten gespeichert? [vgl.Buck03]

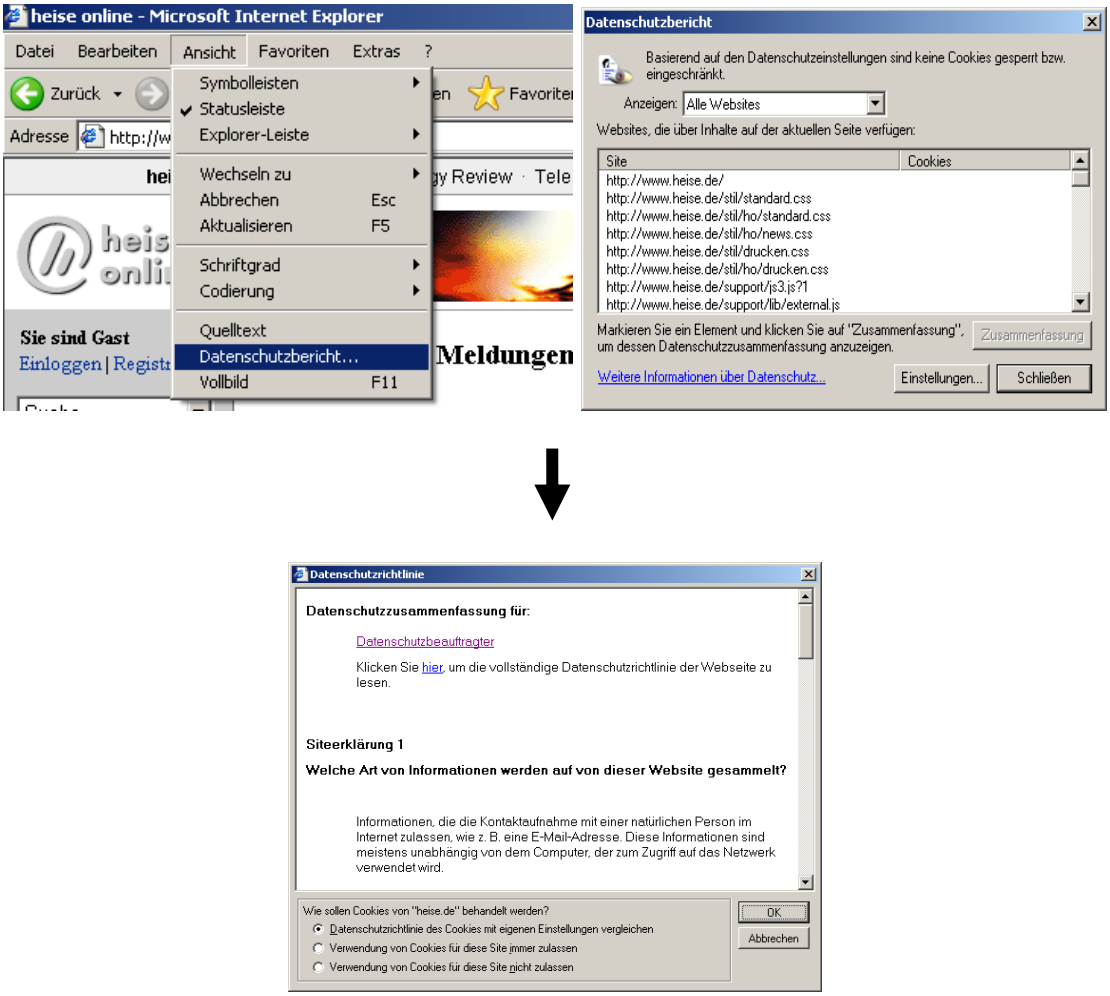


Abbildung 5: P3P-Privacy Policy Internet Explorer 6.0 (Screenshot).

Der Internet Explorer 6.0 wurde so konfiguriert, dass er eine begrenzte Benutzung von P3P ermöglicht. Durch das Anlegen sog. Cookies[51] wird der Webserver darüber informiert, ob der Benutzer eine aufgerufene Webseite in der Vergangenheit bereits aufgesucht hat.

[51] Cookies sind kleine Textdateien, die die Webseite auf der Festplatte eines Computers speichert. Sie verwalten Zustandsinformationen, wenn Benutzer verschiedene Seiten auf einer Webseite durchsuchen und später zu der Webseite zurückgehen. Das hilft der Webseite, die Ansicht für den nächsten Besuch des Benutzers anzupassen.

Der Benutzer kann auswählen, ob er Cookies zulässt, blockiert oder im Bedarfsfall gefragt werden möchte, was zu tun ist.[52] Diese Einstellungen können im Menüpunkt „Extra“ → „Internetoptionen“ über die Registerkarte „Datenschutz“ (engl. Privacy, siehe Abbildung 6) vorgenommen werden:

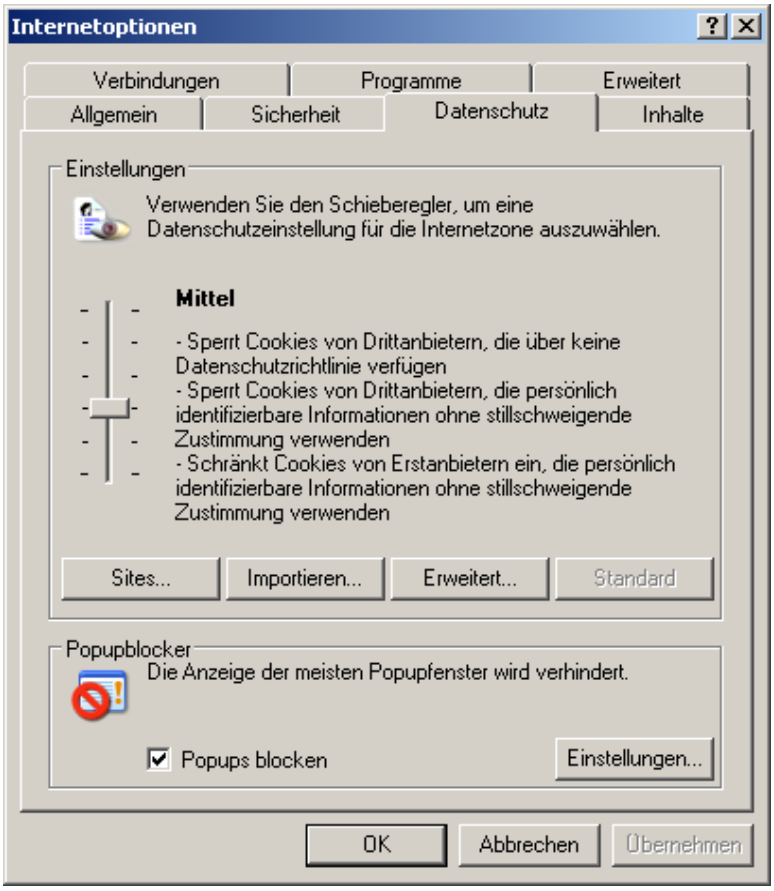


Abbildung 6: Die Privacy-Einstellungen im Internet Explorer 6.0 (Screenshot).

Es besteht auch die Möglichkeit, statt der vordefinierten Privacy-Einstellungen eine Konfigurationsdatei zu importieren (siehe Abbildung 7). Die im folgenden dargestellten Konfigurationsdatei lässt den IE sämtliche Cookies für die aktuelle Sitzung automatisch akzeptieren. Nach der jeweiligen Sitzung werden sie gelöscht, sodass bei einem wiederholten Besuch der Webseite die Cookies nicht mehr wiedererkannt werden. Die Coolkiesverwaltung wird ausschließlich über die Angaben in der jeweiligen Datei gesteuert [vgl. JAP01]:

[52] Mehr dazu unter Seite http://support.microsoft.com/kb/508948/de/.

```
<!-- Internet Explorer - Privacy configuration file  -->
<!--                  JAP-Team jap@inf.tu-dresden.de  -->
<!--                   http://anon.inf.tu-dresden.de  -->
- <MSIEPrivacy>
  - <MSIEPrivacySettings formatVersion="6">
    - <p3pCookiePolicy zone="internet">
        <firstParty noPolicyDefault="forceSession" noRuleDefault="forceSession" alwaysAllowSession="yes" />
        <thirdParty noPolicyDefault="reject" noRuleDefault="reject" alwaysAllowSession="no" />
      </p3pCookiePolicy>
    </MSIEPrivacySettings>
    <flushCookies />
  </MSIEPrivacy>
```

Abbildung 7: Datenschutz-Konfigurnationsdatei im IE. Quelle: [JAP01].

5.1.1.2 Netscape 7.0

Bei Netscape 7.0 unterscheidet man zwischen den Schutzniveaus „niedrig“ (low), „mittel“ (medium), „hoch“ (high) und „benutzerdefiniert“ (custom). Der P3P-Agent kann auch auf Cookies der Website oder von dritten Websites reagieren. Besitzt die Webseite keine Privacy Policy, fehlen auch dem P3P-Agent die Informationen über die Datenverarbeitungspraktiken der Website.

Für den Fall, dass eine Website Benutzerdaten ohne dessen Zustimmung verarbeitet, sollten Cookies per Privacy-Einstellung abgelehnt werden, um dem Benutzer eine bessere Kontrolle über seine personenbezogenen Daten zu gewährleisten. Die dritte Einstellungsmöglichkeit „hoch“ (high) stützt sich auf die weiter oben erwähnte „Opt-out“-Methode, mittels derer der Benutzer einer Verarbeitung seiner personenbezogenen Daten widersprechen kann. Die vierte Option „benutzerdefiniert“ (custom) erlaubt eine Datenverarbeitung nur dann, wenn der Benutzer vorher ausdrücklich zugestimmt hat (sogenanntes „Opt-in“) [ULDb].

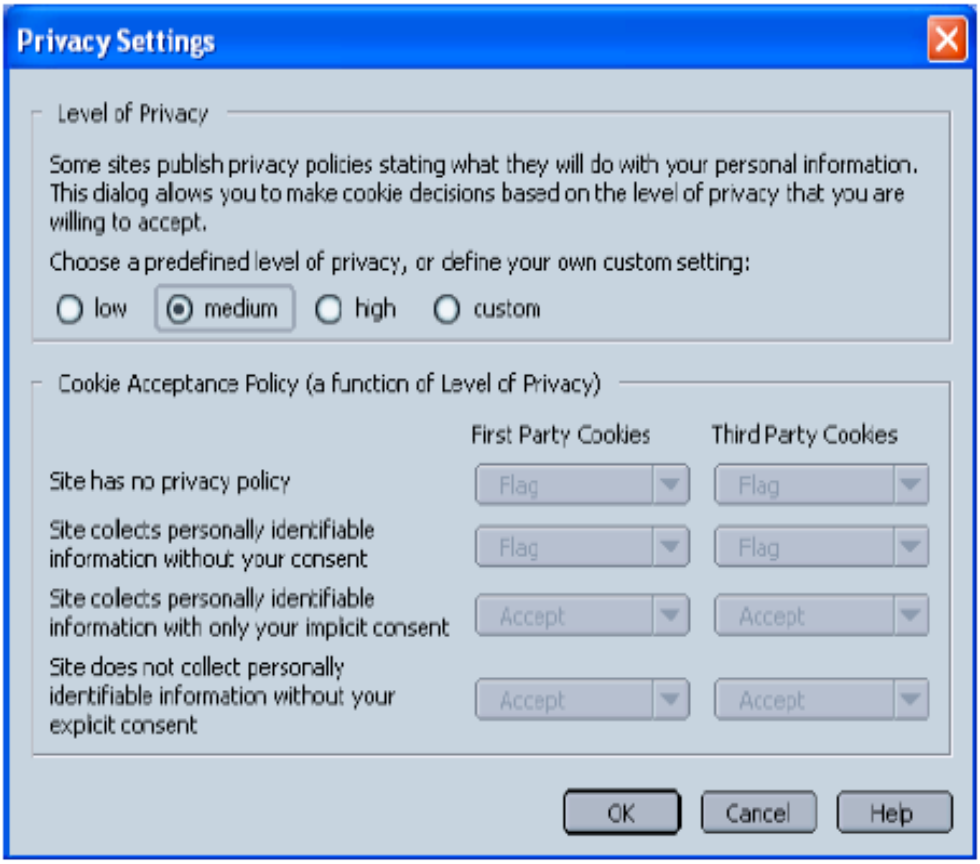


Abbildung 8: Privacy-Einstellungen bei Netscape 7.0. Quelle: [JAP01].

5.1.1.3 JRC P3P Proxy

JRC P3P Proxy ist ein weiterer User Agent, der Privacy-Präferenzen des Benutzers kontrolliert und dementsprechend den Zugriff auf eine Website entweder erlaubt oder verweigert. Man kann zwischen sechs vordefinierten Sicherheitsniveaus wählen. Auch hier ist ein Import von Privacy-Einstellungen möglich. Diese werden auf dem Proxy-Server von JRC gespeichert. Mittels eines Privacy-Buttons besteht darüber hinaus die Möglichkeit, diese Einstellung zu aktivieren oder zu deaktivieren. Aktiviert man sie, erfolgt die Verbindung zum Server, auf dem die Privacy-Einstellungen gespeichert sind, automatisch [vgl. Mey02, 75].

5.1.1.4 AT&T Privacy Bird

Der Privacy Bird (in Form eines Vogels) wurde von der AT&T Corporation entwickelt und ist ein P3P User Agent, der die Datenschutzerklärungen des Users und die Privacy Policy der Webseite vergleicht, um dabei dem Benutzer die Entscheidung zu erleichtern, ob er einen Datenaustausch erlauben soll oder nicht. Er ist als

ein Add-on[53] für den Mirosoft Internet Explorer (IE) (ab Version 5.01) realisiert, der nach der Privacy Policy auf einer Webseite sucht und diese liest. Falls eine solche existiert, stellt er dem Benutzer in leicht verständlicher Form Informationen über die Benutzung seiner Daten zur Verfügung. Dabei ändert der Privacy Bird je nach Suchfunktion seine Farbe: Der grüne Vogel zeigt, dass die Privacy Policy mit der Benutzer-Einstellung übereinstimmt, der gelbe Vogel gibt Auskunft darüber, dass auf der Webseite keine Privacy Policy gefunden wurde und der böse rote Vogel weist darauf hin, dass die Privacy Policy der Webseite nicht den Einstellungen des Benutzers entspricht. Außerdem macht ein schlafender grauer Vogel den Benutzer darauf aufmerksam, dass das Tool ausgeschaltet ist (Abbildung 9). Das Ganze kann optional auch akustisch unterstützt werden. Klickt der Benutzer das Vogel-Symbol an, erhält er zusätzliche Informationen über die aktuelle Privacy Policy der Webseite und kann seine Präferenzen definieren bzw. verändern (Abbildung 10).

Abbildung 9: AT&T Privacy-Bird-Symbole (Screenshot).

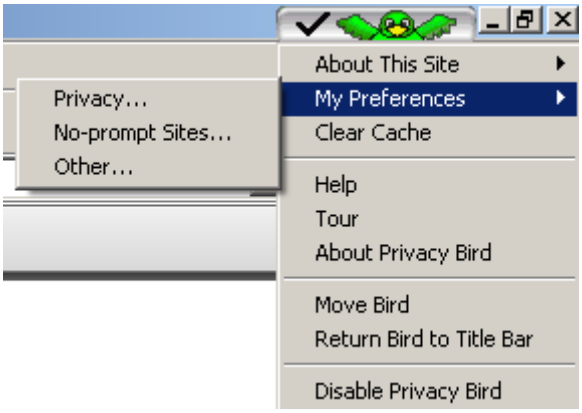


Abbildung 10: Privacy Bird Menü (Screenshot).

[53] Ein Add-on ist ein Erweiterungspack oder optionales Modul, das ein Programm oder Spiel ergänzt. Mehr dazu unter http://www.microsoft.com/austria/windowsxp/sp2/sp2_addonmanager.mspx/.

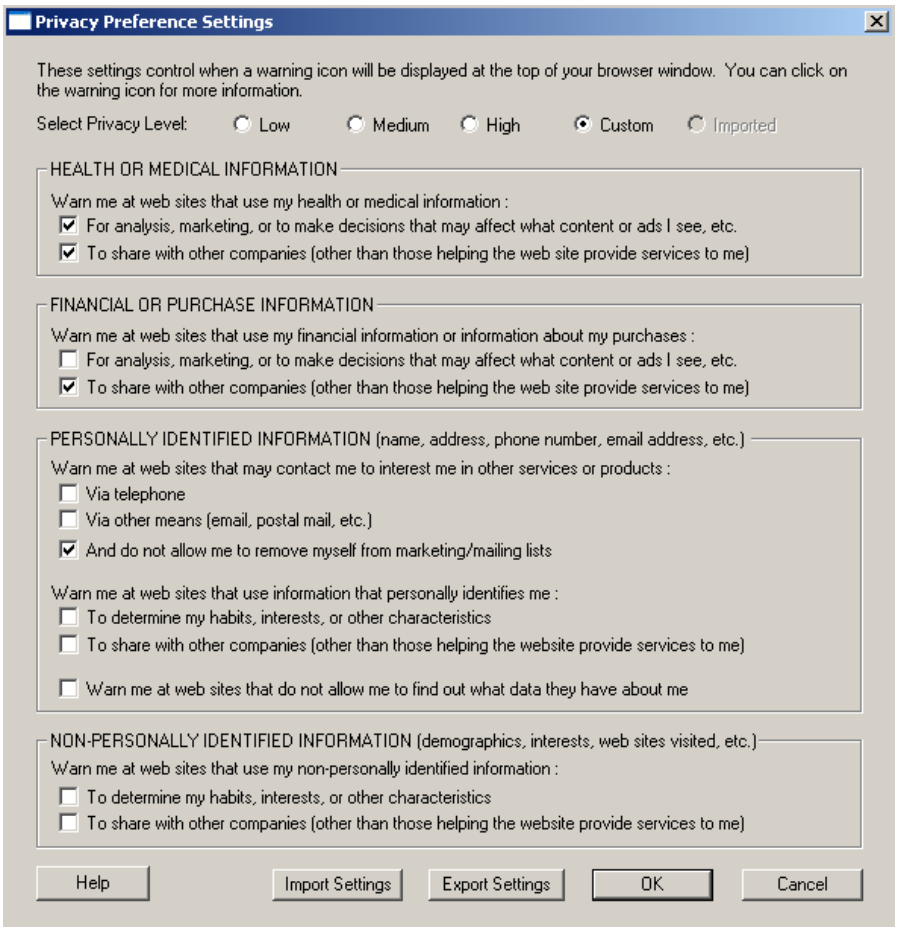


Abbildung 11: AT&T Bird: Bestimmung von Privacy-Präferenzen (Screenshot).

Für den Mozzilla Firefox existiert das Add-on „PrivacyFox“. Es verfügt über ähnliche Funktionen wie Privacy Bird [CAG05].

5.2 A P3P Preference Exchange Language (APPEL)

APPEL steht für „A P3P Preference Exchange Language“ (deutsch: „Eine Austauschsprache für P3P-Präferenzen“) und ergänzt P3P. „APPEL erweitert P3P um die Möglichkeit zur Beschreibung von Datenschutzpräferenzen eines Benutzers und spezifiziert einen Mechanismus zur Auswertung, ob die Datenschutzrichtlinien einer Webseite konform zu den Datenschutzpräferenzen des Benutzers sind“ [Buck03]. Dadurch, dass APPEL in der Praxis nur selten eingesetzt wird,[54] wird in dieser Arbeit nicht näher darauf eingegangen [W3Ce].

[54] Es findet keine Unterstützung von APPEL in den verbreiteten Internet-Browsern wie Internet Explorer, Netscape/Mozilla [Buck03, 57] statt.

5.3 Enterprise Privacy Authorization Language (EPAL)

Ein vom W3C anerkannter internationaler Standard ist die IBM EPAL. EPAL steht für „Enterprise Privacy Authorization Language" und ist eine formalisierte Sprache. EPAL ergänzt P3P und ermöglicht es Unternehmen zu überprüfen, ob die veröffentlichte Privacy Policy innerhalb ihrer Informationssysteme durchsetzbar ist [Kobsa07]. EPAL wurde entwickelt, um eine P3P Privacy Policy innerhalb eines Unternehmens und unternehmensübergreifend darstellen und durchsetzen zu können, was mit P3P alleine nicht möglich ist. Während P3P durch die Darstellung der Datenschutzbestimmungen einer Webseite den Internetnutzer darüber aufklärt, wie Unternehmen ihre Daten verarbeiten, besteht die Aufgabe von EPAL darin, diese Bestimmungen umzusetzen. Mittels EPAL haben Unternehmen die Möglichkeit, ihren Kunden glaubhaft darzustellen, dass „die tatsächliche Verwendung der Daten mit der Datenschutzerklärung übereinstimmt" [Sac07]. EPAL bestimmt den detaillierten Ablauf der Datenverarbeitung. Während P3P nur kurz mitteilt: „Wir veröffentlichen keine Daten", liefert EPAL ein feingranulares Privacy-Policy-Model und schildert den kompletten personenbezogenen Datenfluss, der im Unternehmen verarbeitet wird [W3Cd].

5.4 E-Privacy Policy auf Unternehmensseite

Eine Folge der fehlenden internationalen Gesetzgebung sind die Datenschutzerklärungen im Internet. Sie wurden aufgrund der Selbstregulierung des Marktes geschaffen. Eine elektronische Datenschutzerklärung (engl. Privacy Policy) ist eine Art Kommunikationsform für den Benutzer, die auf der Website publiziert wird und erklärt, wie ein Unternehmen personenbezogene Information des Benutzers verwendet. Die Unternehmen publizieren unterschiedliche Privacy Policies, mit verschiedenem Umfang. Diese sind öffentlich, d. h. sie können von jedem jederzeit eingesehen werden [TRUSTe07a].

Die Privacy Policy ist eine Sammlung von Regelungen, die bestimmte Rechte und Pflichten für die Benutzer und Dienstanbieter enthält. Hinter der Idee einer öffentlichen Darstellung der Privacy Policy steht, die Betreiber von Websites zu verpflichten, ihre dargestellte Politik tatsächlich einzuhalten und sie so zu gestalten, dass sie benutzerfreundlich ist, also auch in verständlicher Form gelesen werden kann. Weiters können die Benutzer selbst entscheiden, ob sie die Seite besuchen und

damit bewusst ihre personenbezogenen Daten zu den in der Policy angegebenen Konditionen preisgeben. Die Theorie aber entspricht nicht immer der Realität [Cio07]. Laut einer Umfrage [PZ06] lesen viele Online-Käufer die Privacy Policy gar nicht. Die meisten gehen davon aus, dass sich Unternehmen damit ihrer Verpflichtungen entledigen wollen bzw. dass sich Datenschutzerklärungen im Internet sowieso alle ähneln. Sicher, das Lesen langer Datenschutzpraktiken ist oft mühsam. Trotzdem stärkt das Publizieren der Privacy Policy (sogenanntes „Privacy Statement“) das Vertrauen der Benutzer gegenüber den jeweiligen Webseitenbetreibern. Dieser Effekt verstärkt sich noch, wenn Datenschutzpraktiken von Vertrauensinstitutionen wie TRUSTe und BBBOnLine überprüft werden[55]. Bevor auf die Einhaltung von Privacy Policy eingegangen wird, wird im nachfolgenden die Bestimmung einer E-Privacy Policy im Unternehmen näher erklärt.

5.5 Erstellung einer E-Privacy Policy im Unternehmen

Wie wird die Privacy Policy im Unternehmen erstellt? Die Unternehmenspolitik in Bezug auf die Privacy wird zuerst skizziert. Sie wird vom sogenannten Chief Privacy Officer (CPO) definiert, wobei die Bestimmungen über das Sammeln und die Verarbeitung personenbezogener Daten vom Unternehmen festgelegt werden. Der CPO sollte daher mit den gesetzlichen Bestimmungen und Strukturen sowie der Strategie im Unternehmen vertraut sein [ASP].

Meistens ist auf einer Website nicht nur eine Privacy Policy vorhanden, sondern es werden verschiedene Policies für unterschiedliche Bereiche benötigt [W3Cb]. Man kann z. B. zwischen Benutzern unterscheiden, die nur auf der Website surfen, und solchen, die mit der Absicht kommen, etwas zu kaufen (Online-Käufer). Dies muss in der Gestaltung der Privacy Policy ebenfalls berücksichtigt werden. Im nächsten Schritt wird entschieden, welcher P3P-Generator für die Formulierung der Privacy Policy in Frage kommt. Unter den zahlreichen Editoren seien hier nur drei genannt:

- IBM Privacy Policy Editor[56],
- PrivacyBot.com[57],
- P3Pedit[58].

[55] Dieser Sachverhalt wird in Kapitel 5.6.1 näher beschrieben.
[56] http://www.alphaworks.ibm.com/tech/p3peditor/.
[57] http://www.privacybot.com/.
[58] http://www.p3pedit.com/.

Der einzige kostenfreie Editor, der im Rahmen dieser Arbeit auch eingehender erklärt wird, ist der IBM Privacy Policy Editor (Abbildung 13). Alle anderen Editoren sind kostenpflichtig und konnten wegen fehlender Vorab-Testmöglichkeit nicht getestet werden.

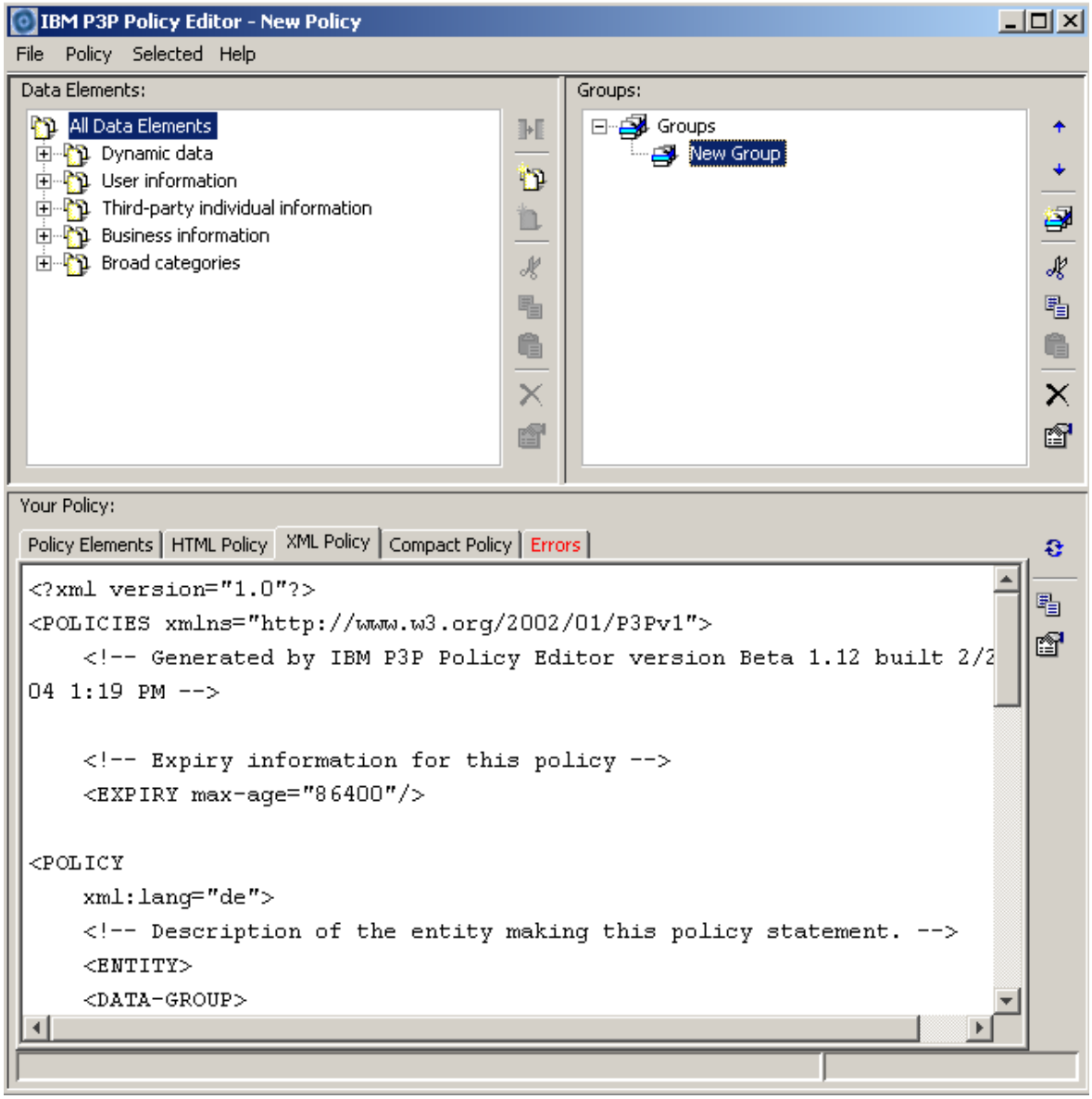


Abbildung 12: Benutzeroberfläche IBM Privacy Policy Generator (Screenshot).

Der IBM Privacy Policy Editor teilt die Eingabe in zwei Bereiche auf:

- Policy Properties (Abbildung 13) und
- Data Properties (Abbildung 14).

Im Bereich „Policy Properties“ geht es um:

- Organisation (Daten zum Websitebetreiber wie Name, E-Mail-Adresse, Homepage-URL, Telefonnummer, Postadresse),
- Website (In einem Verzeichnis wird die menschenlesbare Privacy Policy dargestellt.),
- Assurances (Wer überwacht die Policy? Hier können verschiedene Gesetze oder Institutionen eingegeben werden.),
- Access (Hat man hier Zugriff auf die Daten? Außerdem wird der User angewiesen, wie er seine gespeicherten Daten betrachten bzw. pflegen kann.),
- Expiry (Wie lange ist die Privacy Policy gültig?).

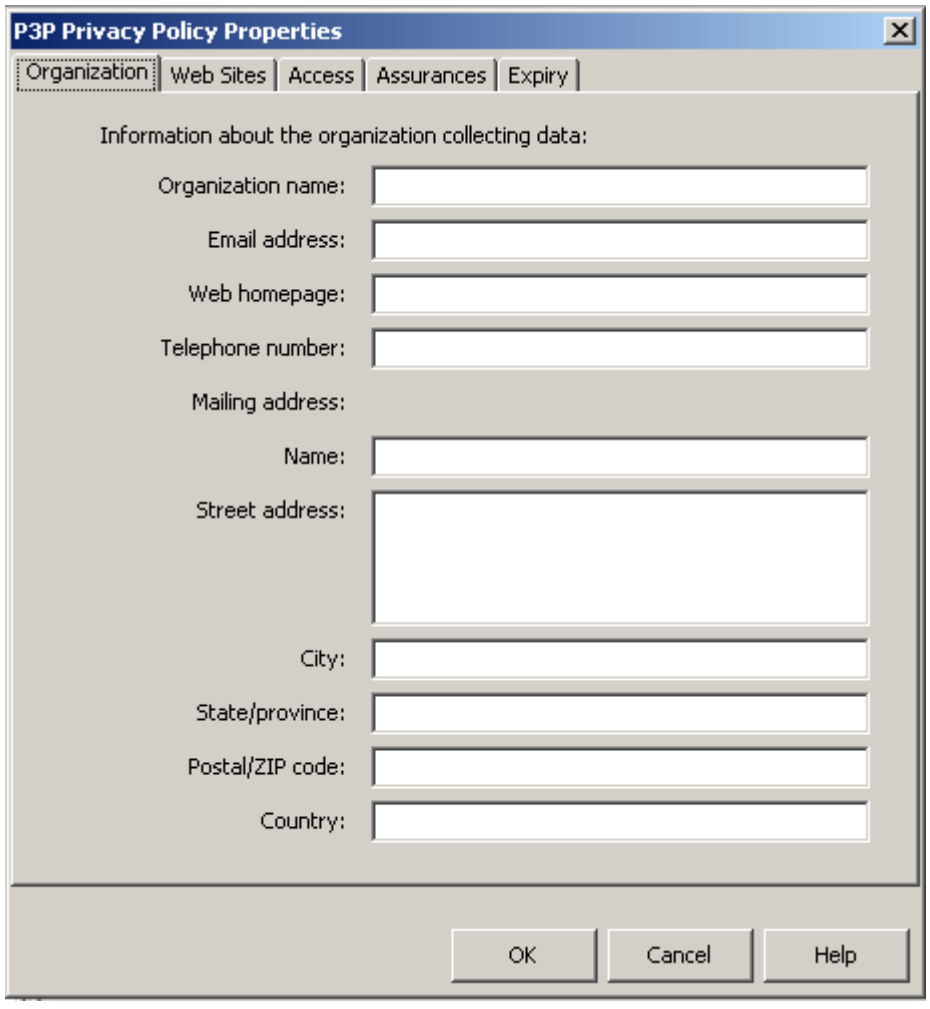


Abbildung 13: Eingabeoberfläche Privacy Properties (Screenshot).

Bei der Eingabeoberfläche „Data Properties“ werden zuerst alle Daten, die vom Unternehmen verarbeitet werden, eingegeben. Das sind: Dynamic Data, User Information, Third-party individual Information, Business Information und Broad

Categories (Abbildung 12). Diejenigen Daten, die eine einheitliche Privacy Policy enthalten, werden durch die „drag and drop“[59]-Methode in Datengruppen zusammengefasst und so als die „Data Properties“ spezifiziert. Diese Datengruppe unterteilt sich dann in:

- General (Bezeichnung und Erklärung, wieso diese Daten benötigt werden und was passiert, wenn die geforderten Daten nicht preisgegeben werden. Zusätzlich kann man angeben, ob sich die Identität des Benutzers durch die Preisgabe bestimmen lässt.),
- Purpose (Zu welchem Zweck werden die Daten erhoben?),
- Recipient (Wer ist der Empfänger der Daten?),
- Retention (Wie und warum werden die Daten gespeichert?).

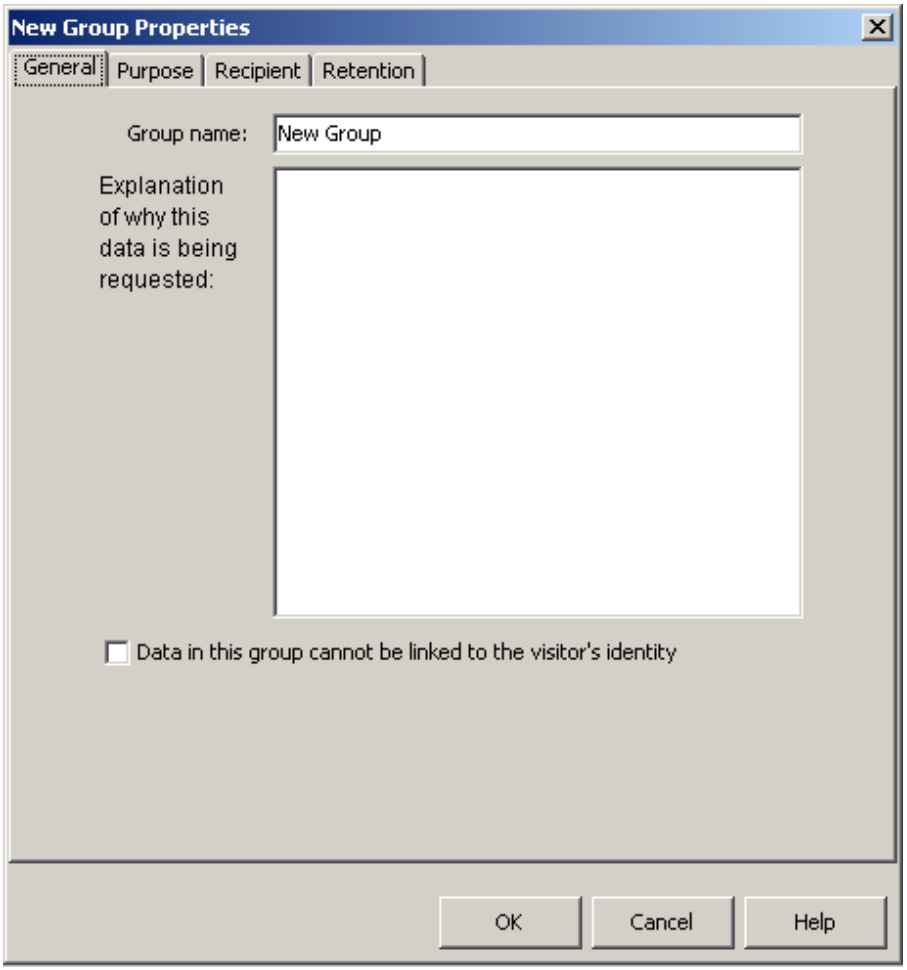


Abbildung 14: Data Properties (Screenshot).

[59] Durch „Ziehen“ und „Einfügen“ werden Daten von der linken Seite zur rechten verschoben.

Nach Eingabe obiger Informationen erstellt der Privacy Policy Editor neben einem XML-Code der Policy (maschinenlesbare Policy) auch eine HTML[60]-Version. Dies ist dann die menschenlesbare Policy[61], die möglichst verständlich und kurz dargestellt wird, damit sie der Benutzer direkt zur Kenntnis nimmt. Der XML-Code ist unter dem Namen „privacy1.xml“ zu speichern. Gibt es mehrere Privacy Policies auf einer Website, sind diese entsprechend (z. B. „privacy2.xml“, „privacy3.xml“ etc.) zu benennen. Darüber hinaus ist es eine Referenzdatei „p3p.xml“ zu erstellen. Diese gibt dem WWW-Browser bekannt, wo sich die Policy-Datei befindet. Als letzter Schritt wird mittels eines sog. Validator die Privacy Policy auf mögliche Fehler überprüft [W3Cf].

Danach werden die Datenschutzpraktiken auf der Website veröffentlicht und das Unternehmen verfügt somit über eine P3P Privacy Policy[62] [W3Cc]. Die nachfolgende Grafik veranschaulicht den eben beschriebenen Gesamtprozess in einem Unternehmen:

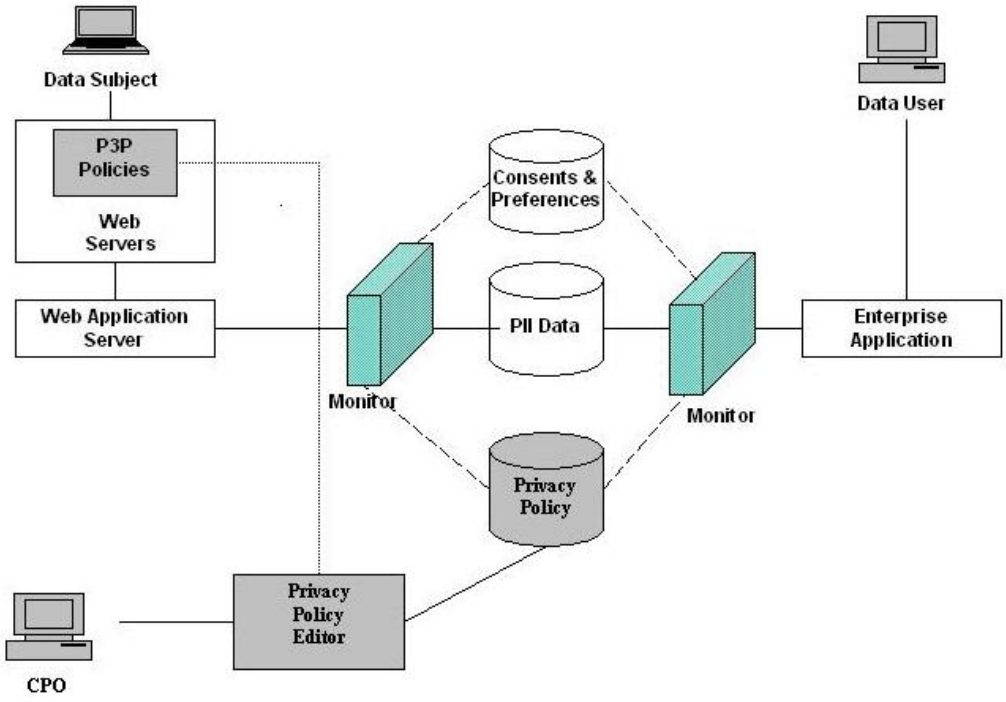


Abbildung 15: Privacy Management und Durchführung im Unternehmen. Quelle: [APS].

[60] HyperText Markup Language.
[61] Siehe Abbildung 5.
[62] Zur genaueren Information über die Bestimmung von Privacy Policy siehe [Bloom02].

Auf der linken Seite befindet sich der Internetbenutzer, „Data Subject“ genannt. Er ist derjenige, dessen personenbezogene Information (PII)[63] vom Unternehmen erfasst werden. Auf der rechten Seite ist der „Data User“, der interne Angestellte, der PII verwendet (zum Beispiel zu Marketingzwecken).

Das Hauptmanagement besteht aus dem Privacy Management Server (ersichtlich in der Mitte der Graphik). Dort befindet sich der Kern der Privacy-Managementtechnologie, welche alle Abläufe untereinander steuert und reguliert.

Die Hauptkomponenten des Privacy Management Servers sind die „Privacy Monitors“, die PII aufbewahren und bestimmte Ressourcen schützen. Sie sind dafür zuständig, die Daten zu überwachen und zu schützen, die vom Überwachungssystem (den sogenannten „Monitors“) transportiert werden.

Liefert der Benutzer („Data Subject“) bestimmte personenbezogene Informationen zum Unternehmen, wird der gesamte Prozess vom Monitor nachverfolgt: Die Sammlung von PII, die Zustimmung des Benutzers, seine Daten zu sammeln und zu verarbeiten, und die Privacy Policy.

Wenn der „Data User“ versucht, die Daten aufzunehmen, überprüft der Monitor zuerst, ob der Zugriff den Anforderungen entspricht: Die Regelungen anhand der Privacy-Politik einerseits und die Zustimmung des Benutzers andererseits müssen gesetzeskonform sein.

Ein Unternehmen sollte auch Privacy Management Services für Benutzer anbieten. Diese sind meistens auf dem Web-Application-Server vorhanden, auf welchen die Benutzer direkt zugreifen können. Zur Verfügung stehen Dienstleistungen wie:

- die gespeicherten personenbezogenen Daten anschauen und/oder ändern,
- die Privacy Policy überprüfen und ihr zustimmen,
- Privacy-Benachrichtigung erhalten und Privacy-Berichte anzeigen, wenn der Benutzer Informationen vom Unternehmen verlangt wie z. B., welche Daten von ihm aufgenommen wurden, wer sie und zu welchem Zweck bekommen hat [ASP].

[63] Die Abkürzung „PII“ wird hier als jede personenbezogene Information eines Individuums verstanden.

Um das Vertrauen von Internetbenutzern zu erhöhen, müssen viele Unternehmen künftige Konsumenten davon überzeugen, dass die personenbezogenen Daten, die sie bei ihrem Webseitenbesuch hinterlassen, sicher behandelt werden. Um dies zu erreichen, haben Websitebetreiber verschiedene Methoden entwickelt. Einige davon (Privacy Policy und die Gütesiegel) werden im nachfolgenden Arbeitsabschnitt erklärt.

5.6 Einhaltung von Privacy Policy

Unternehmen sollte bewusst sein, dass eine nicht eingehaltene Privacy Policy das Unternehmensimage empfindlich schädigen und damit seine Wettbewerbsfähigkeit schwächen kann. Daher sollte die Privacy Policy auf der Website den Internetbenutzern versichern, dass sie sich auf sie verlassen können. Dadurch steigt bei Internetbenutzern das Vertrauen und das Unternehmen stärkt seine Marktposition, was automatisch zu steigenden Kundenzahlen führt [Cio07], [Wörndl03], [PZ06].

In der Realität aber sieht es so aus, dass die bloße Veröffentlichung einer Datenschutzerklärung den Benutzern keine Garantie gibt, dass die Privacy Policy eines Unternehmens auch tatsächlich mit dieser übereinstimmt [ABNT07].

Wieso sind das Posting und die Einhaltung der Privacy Policy so wichtig für ein Unternehmen? Wieso sollen Kunden darauf reagieren und den Datenschutzpraktiken der Unternehmen mehr Aufmerksamkeit schenken? Alle diese Fragen sollen in den nachfolgenden Arbeitsabschnitten geklärt werden. Überdies werden Vertrauensinstitutionen dargestellt, die für die Überprüfung der Privacy Policy zuständig sind.

5.6.1 TRUSTe und BBBOnLine

Eine der einfachsten Methoden für einen Benutzer, eine Entscheidung zu treffen, ob er einer Webseite vertrauen soll oder nicht, ist, sich an den sogenannten Datenschutzgütesiegeln (engl. „Privacy Seal“) zu orientieren. Von den vielen Organisationen, die Gütesiegel anbieten, besitzen „TRUSTe“ und „BBBOnLine“ („Better Business Bureau OnLine“) die meisten registrierten Mitgliedern (2.241 Mitglieder bei TRUSTe und 43.207 Websites bei BBBOnLine)[64]. Sie sind ein typisches Bei-

[64] Siehe http://www.bbbonline.org/business/ und http://www.truste.org/about/fact_sheet.php?PHPSESSID=bf8ce52e55700246ca8f3f74d0749205/.

spiel für die Selbstregulierung des Datenschutzes der US-Wirtschaft und können in P3P integriert sein und Bestandteil der Datenschutzerklärung werden.

TRUSTe

Gegründet 1997 von Elektronic Frontier Foundation (EFF) und CommerceNet Consortium, nimmt TRUSTe eine besondere Stellung ein. Es steht als Beispiel für ein Gütesiegelprogramm, mit dessen Hilfe Konsumenten erkennen sollen, welchen Webseiten sie vertrauen können. Hauptziel von TRUSTe ist, das Vertrauen von Benutzern im Internet zu erhöhen [Ben99; Hof02, 134].

TRUSTe legt bestimmte Datenschutzrichtlinien fest, die durch das Handelsministerium der USA und FTC (Federal Trade Commission) anerkannt sind [SmSh07, 109]. Alle Unternehmen, die sich zu den TRUSTe-Richtlinien verpflichten und daran festhalten, sollen die in den USA vorherrschenden Standards erfüllen: eine „Privacy Policy“ auf ihrer Website implementieren, die in Form eines „Privacy Statements“ sichtbar ist, welche wiederum von TRUSTe überprüft wird: der Benutzer muss über die Datensammlung und -verarbeitung im Unternehmen informiert sein und es soll ihm die Möglichkeit gegeben werden, über seine Daten zu bestimmen, indem er einwilligt oder nicht. Des Weiteren soll er Zugang zu seinen Daten haben. Wenn ein Unternehmen diese Voraussetzungen erfüllt, wird es berechtigt, nach Zahlung einer Registrierungsgebühr, das Gütesiegel[65] von TRUSTe auf seiner Website zu platzieren (Abbildung 16):

Abbildung 16: TRUSTe-Logo. Quelle: http://www.truste.org/.

Es verpflichtet sich gleichzeitig dazu, das Gütesiegel an einem gut sichtbaren Platz anzubringen. Und TRUSTe versichert dabei, dass diese Unternehmen die Privacy-Politik auch tatsächlich einhalten [SmSh07, 109], indem in periodischen Abständen die Websiten kontrolliert werden, ob tatsächlich die Standards eingehalten werden

[65] Das TRUSTe-Logo hat sich innerhalb seiner zehnjährigen Existenz verändert, siehe Abbildung 16.

oder ob sich das „Privacy Statement“ geändert hat. Manchmal schickt die Organisation sogar von sich aus Daten an die Website, um zu sehen, wie die Daten tatsächlich verarbeitet werden.

Damit kein unautorisierter Eingriff stattfindet, hat TRUSTe das Gütesiegel „Click to Verify“ implementiert, das jedes von TRUSTe anerkanntes „Privacy Statement“ enthalten soll. Dieses Gütesiegel leitet dann zur Bestätigung sofort zum Server der Organisation um [Gri04]. Besteht ein konkreter Verdacht des Missbrauchs, kontrolliert ein Wirtschaftsprüfer (bspw. KPMG oder Pricewaterhouse), ob gegen die Regeln von TRUSTe gehandelt wird. Falls sich dies bestätigt, wird das Unternehmen von TRUSTe in seinem prinzipienwidrigen Verhalten gestoppt, ansonsten wird es verwarnt und letztlich wird ihm die Erlaubnis zur Verwendung der „Trustmark“ entzogen [Hof02, 135].

Ebenfalls wichtig zu erwähnen ist, dass das Gütesiegel für sich alleine keine Webseiteninformationen speichert, TRUSTe liefert auch keine Technologie an die bei ihm registrierten Unternehmen, um personenbezogene Informationen zu verwalten, sondern die Organisation besitzt lediglich eine legislative Funktion [GaSp02, 598].

BBBOnLine

BBBOnLine ist eine hundertprozentige Tochtergesellschaft von Council of Better Business Bureaus. Ähnlich wie TRUSTe ist das Ziel von BBBOnLine, das Vertrauen im Internet durch ihre BBBOnLine-„trustmark“zu stärken. Die Organisation hat drei Gütesiegel-Programme: „BBBOnLine Reliability“, „BBBOnLine Privacy“ und „BBBOnLine Kid’s Privacy“(Abbildung 17):

Abbildung 17: BBBOnLine’s Gütesiegel: „BBB Reliability Programm[66]“, „BBB Privacy Programm“ und „Kid’s Privacy Seal“ (Screenshot).

[66] BBB hat das Gütesiegel von der „BBBOnLine Reliablity mark“ zur „Accredited Business trustmark“ gewechselt. Beides kann auf Webseiten von Unternehmen erscheinen. Näheres hierzu siehe http://www.bbbonline.org/.

„BBB Reliability"-Programm: Das Gütesiegel zeigt, dass das Mitglied mindestens ein Jahr Unternehmer ist, die BBB-Richtlinien befolgt und sich verpflichtet, dabei mit BBB zu kooperieren, um die Probleme der Konsumenten zu lösen, die in Verbindung mit den dargestellten Waren und Dienstleistungen auf der Website auftreten[67].

„BBBOnLine Kid's Privacy"-Programm: Das Gütesiegel kann auf Webseiten platziert werden, die mit den Richtlinien der COPPA (Children's Online Privacy Protection Act)[68] übereinstimmen und von dem „BBBOnLine Kid's Program" akzeptiert werden. Die Mitgliedschaft verlangt ein Zertifikat, dass Webseite der Organisation und die Privacy Policy den Anforderungen der BBBOnline's Website entsprechen[69].

„BBB Privacy"-Programm: Das Gütesiegel kann von jedem Unternehmen benutzt werden, das daran interessiert ist und auch von dem „Privacy-Programm" aufgenommen wird. Wie bei beiden zuvor genannten Programmen verpflichten sich auch hier die Webseitenbetreiber dazu die Vorschriften des „Privacy-Programms"[70] einzuhalten [GaSp02, 599].

Die Benutzer einer Webseite können jederzeit Beschwerden gegenüber BBBOnLine wie auch TRUSTe vorbringen. Bei BBBOnLine heißt dieses Forum „dispute resolution", das jedes Unternehmen bei der Registrierung anerkennt. Beim TRUSTe erfolgt dies im Rahmen eines standardisierten Verfahrens (sogenanntes Watchdog) [Hof02, 255].

Obwohl einige „Big-Player" wie AOL, Microsoft, Yahoo, Altavista Mitglieder von TRUSTe und BBBOnLine sind, finden sich trotzdem einige Schwächen bei den Programmen. Erstens ist die Zahl der registrierten Mitglieder im Verhältnis zu den vielen amerikanischen kommerziellen Websites ziemlich gering[71]. Zweitens ist eine Kontrolle durch die Gütesiegelanbieter bei einem Verstoß gegen die Privacy Policy eines Unternehmens gar nicht möglich, da die internen Praktiken der Unternehmen nie ohne deren Einwilligung nach außen treten werden. Sogar die Gütesiegelorga-

[67] Weitere Informationen finden sich unter http://www.bbbonline.org/reliability/requirement.asp/.
[68] Children's Online Privacy Protection Act = Gesetz zum Schutz von der Privatsphäre von Kindern im Internet.
[69] Mehr Informationen unter http://www.bbbonline.org/privacy/kid_require.asp/.
[70] Mehr Informationen unter http://www.bbbonline.org/privacy/threshold.asp/.
[71] Siehe Anfang Kapitel 5.6.1 TRUSTe und BBBOnLine.

nisationen selbst befolgen nicht immer die eigene Privacy Policy wie bei dem Fall TRUSTe und Thecounter.com [vgl. Hof02, 136 f.].

5.6.2 European Privacy Seal (EuroPriSe)

Da die oben erwähnten Möglichkeiten zur Einhaltung der Privacy Policy nur in den USA gelten, wird in diesem Abschnitt ein europäisches Datenschutz-Gütesiegel (EuroPriSe) vorgestellt.

EuroPriSe (European Privacy Seal) ist ein Projekt im Rahmen des eTEN-Programms, welches von der Europäischen Kommission gefördert wird. Es besteht aus acht europäischen Organisationen und Unternehmen aus acht Ländern, unter der Leitung des Unabhängigen Landeszentrums des Datenschutzes (ULD)[72]. Ziel ist, einen einheitlichen Zertifizierungsprozess für Produkte und Dienstleistungen in der Informationstechnik einzuführen, der sicherstellen soll, dass die IT-Produkte und Dienstleistungen den europäischen Datenschutzrechtsnormen entsprechen. Dies führt nicht nur zu einer besseren Marktpositionierung und zu einem Wettbewerbsvorteil der Produkte und Dienstleistungen der Unternehmen gegenüber solchen, die kein Gütesiegel anbieten, sondern auch zu mehr Vertrauen zu diesen Produkten seitens der Anwender und Käufer, da diese Produkte tatsächlich den europäischen Anforderungen entsprechen [ITA08].

Motivation für das Projekt war das Datenschutz-Gütesiegel von Schleswig-Holsteins, das seit dem Jahr 2000 vor allem auf dem deutschen Markt etabliert ist und bisher das einzige europaweite Datenschutz-Gütesiegel[73] ist, das an ca. 40 Produkte verliehen wurde.

Das erste Unternehmen, das mit dem EuroPriSe-Gütesiegel ausgezeichnet wurde, ist Ixquick[74], eine Meta-Suchmaschine, die am 14. Juli 2008 als erste nach dem EU-Datenschutzrecht geprüft und zertifiziert wurde [EPIC08a].

Abbildung 18: European Privacy Seal. Quelle: http://www.european-privacy-seal.eu/.

[72] http://www.datenschutzzentrum.de/.
[73] Mehr Informationen auf http://www.oeaw.ac.at/ita/ und http://www.datenschutzzentrum.de/.
[74] http://www.ixquick.com/.

5.6.3 Direct Marketing Association (DMA)

Die Direct Marketing Association (DMA), die größte Interessenvertretung für Direktmarketingunternehmen[75], gab 1997 ein Datenschutzversprechen, dass alle Mitglieder der DMA ab dem 1. Juli 1999 bestimmten Datenschutzbestimmungen, die die DMA für ihre Mitglieder entworfen hat, folgen werden. Dabei wurden als Basis die FTC-Bestimmungen (notice, choice, access und security) herangezogen. Die Mitglieder sollen auch die Robinsonliste[76] der DMA berücksichtigen, die den Kunden bei Eintrag in der Liste vor unerwünschter Werbung schützt [Hof02, 137].

Hält ein Direktmarketingunternehmen seine Privacy Policy nicht ein und führt dies zu Kundenbeschwerden, wendet sich das „DMA Committee on Ethical Business Practice“ an das entsprechende Unternehmen. Falls der Hinweis, die DMA-Grundsätze einzuhalten, nicht beachtet wird, wird der Fall an das „DMA Board for appropriate action“ geleitet und es werden weitere Sanktionen eingeleitet.

Die DMA bietet auch einen eigenen „Privacy Policy Generator“, mit dem alle Mitglieder ihre Datenbestimmungen festlegen sollen. Diese werden dann automatisch in eine eigene Privacy Policy integriert. Dabei sollen auch die speziellen Bestimmungen von Daten von Kindern berücksichtigt werden, um die Vorgaben von COPPA nicht zu verletzen [Hof02, 137 f.].

Im nächsten Abschnitt wird OPA erläutert, eine von vielen Organisationen, die gegründet wurde, um das Vertrauen der Benutzer im Internet zu erhöhen.

5.6.4 Online Privacy Alliance (OPA)

Die Online Privacy Alliance (OPA)[77] ist ein Zusammenschluss aus mehr als 40 weltweit tätigen Online-Unternehmen. Ziel dieser Vereinigung ist es, die Kunden davon zu überzeugen, dass ihre Privatsphäre im Internet in sicheren Händen ist. Sie handeln nicht auf gesetzlicher Basis, sondern stellen die Selbstregulation in den Vordergrund. Dadurch, dass die OPA nur Richtlinien vorgibt, aber die Einhaltung nicht garantiert, werden diese von bereits genannten Vertrauensinstitutionen (TRUSTe und BBBOnLine) kontrolliert.

[75] http://www.dma.org.uk/.
[76] Eine „Robinsonliste“ ist eine Liste, die aufgrund des Verbraucherschutzgesetzes entsteht und enthält Adressen von Privatpersonen, die keine adressierte Werbung per Post wünschen. Siehe dazu [Mähr99, 47f].
[77] http://www.privacyalliance.org/.

Vertreter der OPA sind große Unternehmen wie Doubleklick, IBM, Microsoft u. a., Websitebetreiber wie AltaVista und Lycos sind hingegen nicht Mitglied dieser Vereinigung [Hof02, 135].

Kapitel 6

6 Privacy-Missbrauch

“As nightfall does not come at once, neither does oppression. It is in such twilight that we all must be aware of change in the air – however slight – lest we become victims of the darkness.”

William O. Douglas, Richter am obersten US-Bundesgericht, 1898-1980

Die Informationswelt erleichtert in vielen Punkten den Alltag. Aber hinter diesem Vorteil verbirgt sich auch ein gewisses Risiko: der Verlust unserer Privatsphäre.

Es gibt viele Unternehmen, die viel mehr über uns wissen als wir selbst. Ob es um Videoüberwachung, Bewertung von Kunden anhand von Scoringverfahren[78], die Überwachung am Arbeitsplatz, die Nutzung personenbezogener Daten durch öffentliche Stellen oder die Überflutung unseres E-Mail-Postfachs mit unerwünschter Werbung (SPAM) geht, eines ist sicher: Durch die Informatisierung unserer Gesellschaft ergeben sich erhebliche Probleme. Die Aufgabe des Staates ist es, durch Gesetze und Kampagnen (z. B. BigBrotherAwards)[79] die Unternehmen zu zwingen, bestimmte Regelungen nicht nur auf ihren Websites zu präsentieren (in Form von Privacy Policies), sondern diese auch zu befolgen. Der Privacy-Missbrauch muss reduziert werden, damit das Vertrauen der Konsumenten nicht verloren geht [Tan06].

Durch die dauerhafte Internetnutzung werden personenbezogene Daten aufbewahrt, vernetzt und zu einem einzigen Profil gebündelt. Es werden manchmal falsche Profile einer bestimmten Person zugeordnet, Daten werden für einen komplett anderen Zweck, als angegeben, benutzt, Identitäten (Username und Passwort) werden durch Phishing[80] gestohlen. Dies kann für die Zukunft eines Menschen beträchtliche Folgen nach sich ziehen und führt langsam zum Verlust unserer Privatsphäre und zu einem sukzessiven Verlust des Vertrauens des Benutzers.

[78] Durch eine Kombination einer Vielzahl von persönlichen Daten (Alter, Stadt, Adresse, Nachbarschaft, Anzahl Umzüge u. a.) wird eine Bewertung der Kreditwürdigkeit einer Person mittels einer Zahl (Score) ermittelt.
[79] Durch die Verleihung von BigBrotherAwards = „Oscars für Überwachung“ soll die Öffentlichkeit darauf aufmerksam gemacht und auf die Nominierten Druck ausgeübt werden, ihr Handeln (Verletzung von Datenschutz, Privatsphäre usw.) zu ändern. Siehe weitere Informationen in [Tan06].
[80] Beim Phishing (engl.fishing/angeln) versucht der Täter, mittels einer gefälschten E-Mail vertrauliche Informationen wie Zugangsdaten und Passwörter zu bekommen.

Der nachfolgende Arbeitsabschnitt wird sich auf einige Privacy Risiken konzentrieren.

6.1 Verkauf von Daten

Laut § 8 (2) DSG gelten in Österreich „bei der Verwendung von zufälligerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten …schutzwürdige Geheimhaltungsinteressen als nicht verletzt“ [DSG00]. Die durch das Gesetz erstandene Rechtslücke ist eine willkommene Gelegenheit für Datenhändler [ARGE08a]. Im Gegensatz dazu bringt diese Gesetzeslücke dem Internetbenutzer in Bezug auf den Schutz seiner Privatsphäre nur Nachteile. Seine personenbezogenen Daten werden mittels verschiedener Methoden gesammelt und/oder missbraucht. Eine Methode ist z. B. das Auffangen von E-Mails im Internet durch Spammer. Denen geht es meistens um das schnelle Sammeln und Versenden von E-Mail-Adressen und der Anwender ist dagegen meist hilflos. Eine andere Variante ist, die Daten eines Kundenstammes (z. B. durch Rabattkundenkarten) eines Unternehmens zu sammeln und zu verkaufen (wie z.B. im Fall von Tchibo[81]). Die Kundendaten von Tchibo werden von der AZ Direkt GmbH[82] nach bestimmten Kriterien selektiert (Alter, Wohnadresse, Einkaufsverhalten usw.) und verkauft. Obwohl im Jahr 2004 im Tchibo-Prospekt stand: „Alle persönlichen Daten werden vertraulich behandelt“, stand ganz unten bei der Telefonnummer in kaum lesbarer Schrift geschrieben: „Gelegentlich geben wir die Anschriften unserer Kunden an Unternehmen weiter, deren Produkte für Sie von Interesse sein könnten. Bitte teilen Sie uns mit, falls Sie das nicht möchten.“ Es bestand jedoch nicht einmal die Möglichkeit einer Abbestellung. Also sollten sich die Kunden, die diesen Hinweis evtl. gelesen hatten, schriftlich bei Tchibo melden. Im Internet stand dazu: „Die Weitergabe Ihrer im Internet eingegebenen persönlichen Daten an unberechtigte Dritte außerhalb des Unternehmens Tchibo ist grundsätzlich ausgeschlossen.“ Tchibo hat „die Verbraucherinnen und Verbraucher nicht darüber informiert, was mit ihren Daten geschieht“ und „verletzt mit dieser besonders dreisten Weitergabe der Kundendaten auf grobe Weise die Privatsphäre seiner Kunden“ [Tan06, 109 ff.]. Nachdem viele Tchibo-Kunden durch den verliehenen BigBrotherAward[83]

[81] http://www.tchibo.com/.
[82] http://www.az-direct.com/.
[83] BigBrotherAwards ist eine oscarähnliche Verleihung in Bezug auf die Datenschutzverletzung verschiedener Bereiche.

in der Kategorie Verbraucherschutz im Jahr 2004 auf dieses Geschäftsgebahren aufmerksam gemacht wurden und ihre Geschäftsbeziehungen mit dem Unternehmen aufkündigten, hat sich Tchibo in punkto Privatsphärenschutz gebessert. Mittlerweile können Kunden auf der Website bei der Privacy-Politik des Unternehmens der Nutzung und Übermittlung ihrer Daten zu Marketing-Zwecken schriftlich wie auch per Email widersprechen.

Aber wie Rainer Kuhlen festgestellt hat [Kuhl04], wird die Privatsphäre nicht als selbstverständliche Voraussetzung für E-Commerce betrachtet, und solange bestimmte Vorteile wie Rabatte durch Kundenkarten und Preisnachlässe bei Autoversicherungen nur gegen Weitergabe von persönlichen Daten existieren, werden immer mehr Menschen freiwillig auf ihre Privacy verzichten.

6.2 Weitergabe von Benutzerdaten durch gesetzliche Bestimmungen

Der US-Medienkonzern Viacom[84] hat den Suchmaschinenbetreiber Google[85] wegen Urheberrechtsverletzung auf über eine Milliarde Dollar verklagt. Das Gericht entschied Anfang Juli 2008, dass Google alle YouTube-Nutzerdaten[86] (Benutzerdaten und IP-Adressen) an Viacom übergeben muss, trotz Googles Argumentation, das Urteil verstoße gegen seine Datenschutzbestimmungen. Im März 2007 beschuldigte Viacom Google, dass auf der YouTube-Plattform mehr urheberrechtlich geschützte Inhalte vorhanden seien als selbstgedrehte Videos. Mit den in verschlüsselter Form von Google gelieferten Daten konnte Viacom die Tatsache beweisen, dass die Videoplattform YouTube aufgrund dieser urheberrechtlich geschützten Videos erfolgreich geworden war [Comp08]. Laut der stellvertretenden Datenschutzbeauftragten aus Schleswig-Holstein kann dieser Fall dazu führen, dass die Daten der Nutzer, die Viacom erhält, ausgewertet und an Unternehmen weiterverkauft werden können. Auch die Sicherheitsbehörden können Vorteile aus dem Urteil gewinnen, indem sie personenbezogene Profile erstellen, die bei der Entscheidung helfen, ob einer bestimmten Person ein Visum gegeben oder verweigert werden soll [RP08].

[84] http://www.viacom.com/.
[85] http://www.google.com/.
[86] Die Videoplattform YouTube gehört seit 2006 Google.

Da Google eine marktführende Stellung in Deutschland (mit einem Marktanteil von 89,3%), in den USA (57%[87]) [Matt08] und dem Rest der Welt hat, ist die Möglichkeit von Privacy-Missbrauch sehr groß, insbesondere durch die Integration von Google Analytics[88] in Webseiten. Google Analytics ist ein Webanalysedienst der Google Inc. („Google"), der Cookies verwendet. Mit dem Einsatz von Google Analytics können Webseite-Betreiber beispielsweise untersuchen, wo und wie lange sich Benutzer auf ihren Seiten verweilen. Die Benutzerdaten inklusive ihrer vollständigen IP-Adresse werden dann an einen Server von Google in den USA übertragen und dort gespeichert. Datenschutzrechtlich ist der Einsatz dieses Tools problematisch, da fast niemand weiß, dass das Benutzer-Online-Verhalten von Google ausgewertet und mit anderen Daten aggregiert wird. So werden Benutzer-Profile erstellt, die dann für Marketingzwecke benutzt werden können [ORF08].

Die Online-Suche ist ein wichtiger Weg zur Wissensbeschaffung geworden, ohne die wir nicht leben können. Dass die Aufzeichnungen von Suchmaschinen missbraucht werden, scheint daher nur eine Frage der Zeit zu sein.

Was auch die Zukunft bringt, mit der Digitalisierung unseres Wissens steigt die Notwendigkeit, eine Suchmaschine zu benutzen. Denn „mit der Speicherung von Wissen in digitalen Dokumenten sind wir zum ersten Mal seit Erfindung der Schrift darauf angewiesen, Maschinen zu nutzen, die in der Lage sind, uns Zugang zum gespeicherten Wissen zu verschaffen" [Plaß05] - und damit steigt auch unumgänglich das Risiko des Privacy-Missbrauchs.

6.3 Risiken bei sozialen Netzwerken

Immer mehr Menschen stellen eigene Inhalte ins Internet und vernetzen sich miteinander. Im Rahmen dieses Phänomens sind „Social Networking Sites" entstanden. Das sind Portale, in denen sich angemeldete Benutzer und Benutzerinnen treffen, Freundschaften schließen, Filme, Fotos und Nachrichten austauschen. Viele Benutzer nutzen „Social Networking", um Kontakte zu knüpfen. Sie laden ihre personenbezogenen Informationen selbst in die Internetportale, und damit erhalten Privatpersonen einen umfassenden Zugriff auf die Personendaten anderer. Dadurch erweisen sich diese Netzwerke als Tummelplatz für Verletzungen der Privat-

[87] Stand der Daten: September 2007.
[88] Google Analytics ist ein kostenloser Webanalysedienst der Google Inc („Google"), der Cookies verwendet und welcher der Analyse von Zugriffen auf Webseiten dient. Damit kann man ein umfassendes Nutzerprofil von Webseiten-Besuchern anlegen [ORF08].

sphäre ihrer Benutzer. Eines der beliebtesten Netzwerke ist Facebook[89]. Mit diesem großen aus den USA stammenden „Social Network“ wird sich auch das folgende Unterkapitel beschäftigen. Insbesondere sollen im Rahmen der Auseinandersetzung auch Privacy-Risiken für Social Network User diskutiert werden.

6.3.1 Facebook

Bei einer Studie an der Carnegie Mellon Universität (CMU)[90] wurde festgestellt, dass viele Facebook-Benutzer ziemlich ahnungslos sind bzw. sich gar nicht dafür interessieren, welchem Privacy-Risiko sie sich aussetzen, wenn sie persönliche Daten auf der Seite von Facebook veröffentlichen. Gross und Acquisti zeigen in ihrem Artikel, dass Benutzer fremden Menschen Zugang zu ihren persönlichen Informationen erlauben, weil sie keine Ahnung von der enormen Zahl derer haben, die ihre Daten einsehen können [AGr05].

Das Publizieren persönlicher Daten im Internet kann Gefahren mit sich bringen, die die Benutzer nicht einschätzen können. Dies sind z. B. Stalking, Re-Identifikation von Gesichtern, demographische Identifikation, Identitätsdiebstahl, das Erstellen von digitalen Dossiers und Benutzermanipulationen.

Bei **Stalking-Attacken** kann der potenzielle Feind den Aufenthaltsort seines Opfers anhand von personenbezogenen Daten bestimmen, da das Facebookprofil Informationen wie Wohnsitz, Stundenplan (welche Vorlesungen besucht werden) und Ort des letzten Logins beinhaltet. An der CMU waren außerhalb des Semesters 15,7% der weiblichen und 21,2% der männlichen Nutzer von Stalking-Attacken betroffen [AGr05].

Viel größer ist die Gefahr beim Online-Stalking, wenn Internetbenutzer den sogenannten AOL instant messenger (AIM) nutzen. Er erlaubt das Hinzufügen sogenannter „buddies“ zur eigenen Liste, ohne dass diese „buddies“ vorher wissentlich zustimmen müssen. Das bedeutet, dass der potenzielle Feind seine „buddies“ (die Facebook-Benutzer) anhand seiner Liste immer im Blickfeld hat und sehen kann, ob diese online sind. Somit kann er diese spielend leicht verfolgen. Von den 3.400 Benutzern der CMU hatten 77,7% einen AIM (AOL instant messenger) im Einsatz.

Bei der **Re-Identifikation** geht es darum, Verknüpfungen zwischen bekannten Eigenschaften und Tatsachen wie Name und Adresse herzustellen. Durch die Ein-

[89] http//www.facebook.com/.
[90] http://www.cmu.edu/.

gabe von Geburtsdatum, Geschlecht und Postleitzahl kann eine Person mit hoher Gewissheit identifiziert werden [Swe04]. Durch die Angabe des Wohnsitzes kann die Postleitzahl festgestellt werden und ein potenzieller Feind kann so an sensitive Daten dieser Person herankommen, die dann bestimmungsfremd genutzt werden können [Swe02]. So können Fotos von Personen mit zugeordnetem Namen auf der Social-Network-Homepage mit einer speziellen Gesichtserkennungs-Software identifiziert und mit dem Lebenslauf auf einer Firmenwebseite in Verbindung gebracht werden. Mittels CBIR (content based image retrival) ist es möglich, Objekte und Merkmale wie Häuser im Hintergrund eines Bildes zu identifizieren und dadurch die betreffende Person geografisch zu lokalisieren. So kann die Adresse der entsprechenden Person herausgefunden und diese physisch verfolgt werden.

Wenn die Angaben von Geburtsdatum, Heimat, aktuellem Wohnsitz und Telefonnummer gleichzeitig öffentlich ersichtlich sind, kann die persönliche Sozialversicherungsnummer herausgefunden werden und dadurch ein **Identitätsdiebstahl** erfolgen. Facebook-Benutzer, die beobachtet werden und ihre persönlichen Daten angeben, laufen Gefahr, dass jemand ein Profil mit ihrem Namen anlegt und ihren Ruf schädigt.

Das Beobachten des Netzwerkes und seiner Benutzer, kann zu einem **digitalen Dossier**[91] führen. Studenten, die sich im Moment noch keine Sorgen über ihre Online-Aktivitäten machen, können später z. B. Berufs- oder Bewerbungsprobleme bekommen, wenn sie im Netz kompromitierende Fotos aus ihrem Privatleben zugänglich machen. Obwohl viele Netzwerke die Möglichkeit anbieten, das eigene Profil komplett zu löschen, bleiben peinliche Kommentare an anderer Stelle oder eigene Bilder auf fremde Profile immer noch bestehen.

Das Internet vergisst nichts und es kann sich auf die oben beschriebene Art und Weise sehr negativ auf die Karriere eines Menschen auswirken. Die unzähligen Profile, Diskussionen oder Beiträge, die meist sehr unüberlegt ins Netz gestellt werden, können leicht eine interessante Quelle für zukünftige Arbeitsgeber werden. Die Unternehmen setzen Suchmaschinen ein, um potenzielle Arbeitnehmer zu überprüfen, und sehr oft nutzen sie für ihre Recherchen Plattformen wie

[91] digitale Archivierung von personenbezogenen Informationen. So können sämtliche Benutzerinformationen (z. B. verschiedene Profilseiten und Online-Beiträge von Webseitenbenutzer) gespeichert und verknüpft werden, und dadurch wird ein digitaler Dossier persönlicher Daten zusammengestellt.

MySpace[92] oder Xing[93], wo unzählige Informationen verfügbar sind, die bei einem Bewerbungsinterview nicht gefragt werden dürfen wie z. B. provokative Meinungen über Alkohol oder Drogen [Fin06].

Facebook-Benutzer können leicht von jemandem getäuscht werden, der nicht tatsächlich angemeldet ist. Normalerweise überprüft das Unternehmen die Registrierung seiner Benutzer durch Senden einer E-Mail, die eine zufallsgenerierte Kennzahl enthält. Da zwischen Registrierung und der Zusendung der Bestätigungsmail einige Minuten vergehen, kann der potenzielle Feind in dieser Zeit in das Netzwerk eindringen [AGr05]. So können persönliche Informationen gestohlen werden und Gefahren wie Phishing oder Spearing[94] (siehe Kapitel 6.4.2 Phishing und Kapitel 6.4.3 Spearing) entstehen.

6.3.2 MySpace

MySpace ist genauso wie Facebook eines der erfolgreichsten „Social Networks". Es besitzt mittlerweile weltweit über 100 Millionen Profile. Und jeden Tag kommen 270.000 Neuregistrierungen von Internetnutzern hinzu [RosenD07]. Obwohl sich MySpace als ziemlich sicheres Netzwerk etablieren konnte, haben sich im Laufe der Zeit die Zielgruppen und damit auch die Bedeutung der Privacy verändert. Beunruhigend ist die Tatsache, dass die Webseite ihre Benutzer warnt, dass die Kommunikation mit Freunden schwieriger wird, falls die Privacy-Standardeinstellungen von „public" auf „private" geändert werden.

Eine andere Gefahr stellen die großen Medienkonzerne wie die News Corporation, eine Muttergesellschaft von Fox, die dieses Netzwerk für Marketingzwecke nutzen, dar. Es werden die Interessen und Wünsche von Generationen manipuliert. Auf der anderen Seite aber zieht dieses Netzwerk Kritik auf sich, weil sich darin pubertierende Teenager allzu offenherzig präsentieren, oder minderjährige Mitglieder mit sexuellen Angeboten konfrontiert werden. Kürzlich hat eine 14-Jährige eine Klage in Höhe von 30 Mio. US-Dollar gegen MySpace eingereicht, mit der Behauptung, ein 19-Jähriger habe sie sexuell angegriffen, nachdem sie über die Webseite Kontakt mit ihm aufgenommen habe. Solche Tatsachen zeigen, zu welchen gefährlichen Konsequenzen Online-Aktivitäten führen können [RosenD07].

[92] http//www.myspace.com/.
[93] http://www.xing.com/.
[94] Näheres dazu in Kapitel 6.5

Aus diesem Grund beabsichtigt MySpace, den Kontakt Fremder oder über 18-Jähriger zu unter 16-Jährigen Nutzern zu erschweren. Obwohl MySpace die Jugendlichen unter 16 ermutigt, ihre Profile im Privatmodus zu erstellen, sind Nutzerprofile von unter 16-Jährigen weiterhin allen MySpace Usern zugänglich.

6.4 Diebstahl von Benutzerdaten

Der nächste Abschnitt wird sich auf einige Privacy-Fälle, vor allem auf unerwünschte elektronische Werbemails (SPAM), Pishing und Spearing konzentrieren, die dadurch ermöglichen, dass persönliche Daten im Internet gestohlen werden.

6.4.1 Spam-Send Phänomenal Amount of Mail (SPAM)

Spam-Send Phänomenal Amount of Mail (SPAM), was u. a. unerwünschte Massen-E-Mails bedeuten, die schon in Kapitel 3.2 näher erklärt wurden, sind in der Informationsgesellschaft ein besonderes Problem, sowohl am Arbeitsplatz wie auch privat. Es ist nicht selten, dass SPAM betrügerische Angaben beinhaltet und leider reagieren viele Internetnutzer darauf. Laut der Europäischen Kommission haben 7% der Nutzer im Jahr 2004 aufgrund einer SPAM-E-Mail eine Bestellung getätigt und 33% auf einen Link in einer SPAM-E-Mail geklickt [KOM04]. Eine aktuelle Studie von Sophos[95] vom 15. Juli 2008 zeigt jene zwölf Länder, aus denen der meiste SPAM kommt und in denen daher dringender Handlungsbedarf besteht:

[95] http://www.sophos.com/.

Platz	Land	Anteil
1	USA	14,9%
2	Russland	7,5%
3	Türkei	6,8%
4	China (mit Hongkong)	5,6%
5	Brasilien	4,5%
6	Polen	3,6%
6	Italien	3,6%
8	Südkorea	3,5%
9	Großbritannien	3,2%
9	Spanien	3,2%
11	Deutschland	3,0%
12	Argentinien	2,9%
Sonstige		37,7%

Tabelle 3: SPAM-Versand. Quelle: [SOPHOS08].

SPAM ist nicht nur eine Belästigung per E-Mail, sondern versucht oft, den Empfänger auf eine betrügerische Webseite weiterzuleiten. Die meisten Spammer sind Profis und oft mit Kriminellen vernetzt, die den Diebstahl personenbezogener Daten wie z. B. Kreditkartennummern ermöglichen, um damit später Identitätsmissbräuche zu betreiben. Bei Phishing-Mails nimmt z. B. der Absender die Identität einer Online-Einrichtung an (z. B. Bank, Web-Shop) und verlangt von dem Opfer, Daten wie Passwörter, TANs[96] auf einer gut gefälschten Webseite preiszugeben. Daher sind die Maßnahmen gegen SPAM ein wichtiger Schutz nicht nur für Private, sondern auch für Unternehmen. Besonders für Unternehmen ist eine Aufklä-

[96] Eine Transaktionsnummer, die im elektronischen Bankengeschäft (Online-Banking) benötigt wird.

rung ihrer Mitarbeiter über den richtigen Umgang mit sensitiven Daten sehr wichtig, weil dadurch verhindert werden kann, dass Unternehmensdaten durch Spammer oder Phishing-Aktionen (siehe Kapitel 6.4.2 Phishing) aufgefangen werden. Ein Datenschutzproblem stellt auch Spähsoftware, sog. „Spyware“, dar, welche sich per E-Mail oder Gratissoftware verbreitet, das Verhalten des Benutzers und sowie seine Zugangsdaten ausspionieren, um diese dann weiterzuleiten bzw. zu verkaufen.

6.4.2 Phishing

Phishing ist eine Form von Privacy-Betrug, wo der Betrüger versucht, besonders sensitive Daten (wie Kreditkartennummer, Passwörter usw.) vom Benutzer zu erlangen und dabei eine vertrauenswürdige Instanz verkörpert. Normalerweise werden Benutzer angelockt, indem der Phisher z. B. E-Mails einer Bankinstitution, Auktions- und Verkaufsplattformen fälscht, damit die Benutzer ihre geheimen Zugangsdaten wie PINs, TANs usw. angeben, die dann über eine gefälschte Internetseite im Postfach des Betrügers landen. Diese Daten werden betrügerisch benutzt, um Überweisungen zu tätigen.

Bei einer Studie von Gartner Group [Gartner04] haben 19% auf den Link in einer Phishing-Mail geklickt und 3% sogar finanzielle und persönliche Information weitergegeben.

6.4.3 Spearing

Eine andere Form von Phishing ist **Spearing** (Spear Phishing) oder Context aware phishing [Jak05].

Unter Spear Phishing vesteht man gezielte Attacke auf einen bestimmten Benutzer. Bei dieser Form des Betruges setzen die Angreifer sogenannte Social-Engineering-Techniken ein, stellen sich als „neuer Freund“ dar und versuchen das Vertrauen des Benutzers zu gewinnen, indem er persönliche Daten von sich in den sozialen Netzwerken preisgibt. Es kann sein, dass die Daten durch einen Small-Talk in der Kaffeeküche, eine einfache Internetrecherche oder eine fingierte Umfrage entnommen werden. Mit diesen Daten senden die Phisher legitim wirkende E-Mails an den Benutzer in dem Unternehmen, wo er arbeitet, um ihn zu täuschen, diese E-Mails kommen von dem jeweiligen Chef und/oder dem Administrator, die z. B. eine neue Login-Adresse verkünden. Der angefragte Benutzername und das

Passwort werden bei entsprechendem Anklicken auf dem gefälschten Link zu der Betrügerwebseite übermittelt [Val08].

Daher sollte man bei den in den vorigen Kapiteln erwähnten Internetnetzwerken wie Facebook, MySpace u.a. besonders vorsichtig mit der Preisgabe persönlicher Informationen sein. Der Phisher braucht nur einen Einblick in einige soziale Netzwerke wie MySpace, Facebook oder LinkedIn[97], um eine Menge vertrauenswürdiger Informationen für seine Angriffe zu sammeln.

[97] http://www.linkedin.com/.

Kapitel 7

7 Fallstudie

Im Rahmen dieser Diplomarbeit wurde eine Befragung mittels Fragebogens durchgeführt. Die Erhebung erfolgte ausschließlich auf elektronischem Weg unter dem Link http://www.wu-wien.ac.at/usr/h97d/h9752159/fragebogen.html/. Es wurden 107 Menschen befragt, unter ihnen Studenten und Vollzeit-Berufstätige, wobei die Gewichtung auf Studenten mit 51,4% lag. Die Fragen basieren auf fünf Hypothesen, wobei zu jeder Hypothese Indikatoren gebildet wurden.

Sinn und Zweck dieser Untersuchung ist es herauszufinden, inwieweit Konsumenten ihre Privatsphäre wahrnehmen und vorhandene Risiken für diese vermeiden. Anschließend werden verbesserte Handlungsmöglichkeiten für Konsumenten, Unternehmen und Gesetzgeber dargestellt.

Hypothese 1:

Die Etablierung von Informationssystemen führt dazu, dass die Benutzer sich vernetzen und mehr elektronische Dienste im Anspruch nehmen.

Indikatoren für Hypothese 1:

1. Anzahl, Häufigkeit, Dauer und Ort der Internetbenutzung (Frage 1; 2; 3; 4).
2. Die Einstellung zum Internet (Frage 5).
3. Zweck der Internetnutzung (YouTube; Facebook, StudiVZ, Onlinekauf, Surfen), (Frage 6).

Hypothese 2:

Die Benutzer sind über ihre Electronic Privacy beunruhigt.

Indikatoren für Hypothese 2:

1. Die Preisgabe der persönlichen Daten im Internet (Angst, Zweifel): (Frage 7; 8; 9).
2. Je sensitivere Daten verlangt werden, desto weniger persönliche Daten werden preisgegeben (Frage 9).
3. Das Wissen von der Sammlung persönlicher Daten durch Dritte (Frage 10).
4. Den meisten Nutzern ist die Datensammlung nicht bewusst (Frage 10).

Hypothese 3: Je höher die Kontrolle des Benutzers über die Speicherung und Verwendung persönlicher Daten des Benutzers (persönlich oder durch technologische Unterstützung), desto mehr persönliche Information gibt dieser preis.

Indikatoren für Hypothese 3:

1. Die Kenntnis bestimmter Möglichkeiten von Kontrolle persönlicher Daten gibt dem Benutzer mehr Sicherheit (inwieweit haben die Benutzer Kontrolle über ihre Daten): (Frage 13; 14; 16; 17; 18).
2. Grad der Schutzmaßnahmen, wie wichtig ist mir der Schutz meiner persönlichen Daten bzw. meiner Privatsphäre (Frage 11; 12; 15; 17; 18; 19; 20).

Hypothese 4: Die Benutzer haben keine ausreichende Information über mögliche Risiken bezüglich ihrer Electronic Privacy.

Indikatoren für Hypothese 4:

1. Phishing, Spearing, SPAM (Frage 21; 22; 23; 29).
2. Online-Banking (Frage 24).
3. Newsgroups (YouTube, Facebook, StudiVZ, MySpace): (Frage 25; 26; 27; 28).
4. Missbrauch persönlicher Daten (Frage 27; 28; 30; 31; 34; 35; 36).

Hypothese 5: Das Vorhandensein und das Durchlesen einer Privacy Policy erhöht das Vertrauen der Benutzer.

Indikatoren für Hypothese 5:

1. Die meisten Benutzer lesen die Privacy Policy (Datenschutzerklärung) nicht (Frage 37; 38).
2. Es gibt eine Beziehung zwischen der Datenschutzerklärung und dem Risiko. Je höher das Risiko, desto mehr erhöht sich das Vertrauen gegenüber dem Unternehmen, wenn die Privacy Policy existiert und durchgelesen wird (Frage 39).
3. Das Vorhandensein eines Gütesiegels macht die Webseite eines Unternehmens vertrauenswürdiger (Frage 40; 41; 42; 43).

Eine Auswertung der ersten Hypothese hat ergeben, dass die Benutzer (51,43% Studenten und 44,76% Vollzeit-Berufstätige) sehr stark das Internet mindestens

einmal täglich (88,79%) und meistens von zu Hause (94,39%) seit mehr als 5 Jahren (84,91%) benutzen. Die meisten sehen das Internet als Mittel zum Surfen (93,46%) und zur Kommunikation mittels E-Mails und soziale Netzwerke (89,72%). 71,03% kaufen online Produkte und 70,09% benutzen Online-Aktivitäten wie Online-Banking. Die Benutzer bilden sich mit 65,42% online weiter, beruflich ist der Computer ein unvermeidliches Instrument geworden (76,64%).

Bezüglich Privacy glauben 67,3% der Befragten, dass jemand verfolgen kann, was sie online machen und dass ihre persönlichen Informationen online gestohlen werden können (59,8%). 69,1% sind der Meinung, dass Daten, die online preisgegeben werden, missbraucht werden und zu unerwünschten Folgen führen können (70,1%).

Die zweite Hypothese hat bestätigt, dass Konsumenten weniger persönliche Informationen preisgeben, je sensitiver die Daten werden. So haben Konsumenten Bedenken, ihre Kreditkartennummer (90,5%), Sozialversicherungsnummer (74,29%) und Telefonnummer (66,67%) online preiszugeben. Der Name, das Geburtsdatum, bevorzugte Produkte und Hobbys geben Konsumenten preis, ohne dabei viel nachzudenken (jeweils 26,6%, 19,1%, 10,5%, 4,8%).

Es hat sich herausgestellt, dass den meisten Benutzern die Datensammlung durch Dritte eher unbekannt ist. 68,9% wissen nicht, wer ihre persönlichen Informationen online sammelt. Hinzu kommt die Tatsache, dass nur 17% der Befragten sich Gedanken über mögliche Risiken machen, wenn persönliche Informationen über sie im Internet stehen. Ein großer Anteil (56,6%) macht sich nicht immer Sorgen darüber und realisiert die Gefahren damit nicht. Viele Benutzer aber haben Angst, jemand könnte ihre Daten online einsehen. Diese haben auch wenig Vertrauen in Webseiten verschiedener Unternehmen (69,2%). Sie geben dann weniger persönliche Daten über sich selbst preis.

In Bezug auf die dritte Hypothese versuchen 73,6% der Benutzer eine gewisse Kontrolle über ihre persönlichen Daten zu gewinnen, indem sie weniger personenbezogene Daten online (die E-Mail-Adresse, die Telefonnummer oder das Geburtsdatum) preisgeben. Nur 17,9% interessieren sich nicht dafür, wie viel sie davon online weitergeben. Leider kennen sehr viele nichts (72,6%) Technologien wie P3P, Privacy Bird, EPAL und APPEL zur Kontrolle der persönlichen Daten. Nur 18,3% wissen, dass P3P im Internet Explorer integriert ist und den Schutz der Pri-

vatsphäre des Benutzers verbessern kann, wenn diese Option aktiviert ist. Darüber hinaus wissen mit 68,9% der Befragten nichts über den „Datenschutzbericht“ im Internet Explorer, und sie interessieren sich auch nicht dafür, wie das Ganze funktioniert (nur 26,7%).

Bei der Befragung wurde festgestellt, dass Konsumenten sehr viel Wert auf ihre Privatsphäre legen und nur 0,9% sie als nicht wichtig einstufen. Aber gleichzeitig haben die meisten Befragten wenig Kontrolle darüber, wie viele von ihren personenbezogenen Daten eine Webseite sammelt, und wenn sie online einkaufen, wissen sie auch nicht, wer ihre Daten speichert. Dafür erwarten sie aber, dass ihre Privatsphäre durch den Staat und Technologien geschützt werden soll.

Bezüglich vorhandener Risiken hat sich ergeben, dass die Benutzer sehr wohl über mögliche Gefahren im Internet wie Phishing, Spearing, Spyware und SPAM informiert sind. Die meisten (98,1%) haben von dem Begriff SPAM gehört, gefolgt von Spyware (80,8%), Phishing (73,1%), und am wenigsten kannten die Befragten den Begriff Spearing (9,6%). Obwohl solch eine hohe Zahl der Befragten diese Risiken schon als nicht fremd einstuft, haben trotzdem 13,2% mehr als einmal auf eine Internetattacke reagiert und dabei Schaden in Höhe von 500-1.000 Euro (2,9%) bzw. ab 1.000 Euro (1,9%) erlitten.

Viele Befragte meinen, dass Online-Banking ziemlich sicher sei, und 41,5% haben volles Vertrauen in ihr Bank-Unternehmen. Im Gegensatz dazu sind viele der Meinung, dass die persönlichen Daten im Internet nicht sicher seien und durch unautorisierte Dritte gesammelt werden könnten (72,9%).

Die sozialen Netzwerke sind auch beliebige Kommunikationsmittel. 61% der Befragten nutzen die Dienste von YouTube, Facebook, MySpace und StudiVZ, wobei das „Social Network“ YouTube mit 97,2% das beliebteste Kommunikationsmittel darstellt.

Bei der Benutzung sozialer Netzwerke akzeptieren 76,5% der Befragten keine Fremden als ihre „Online-Freunde“, was bedeutet, dass sich die Benutzer sehr vorsichtig im Internet verhalten und sich Gedanken über mögliche Risiken machen. Sie wissen mit 52,4%, dass die hinterlassene persönliche Information auf diesen Webseiten von anderen wie Spammern oder Hackern aufgefangen werden kann. Und man stellt fest, dass SPAM immer noch ein aktuelles Bekämpfungsthema ist. 38,3% bekommen 1 bis 5 SPAMs pro Tag.

Den meisten Benutzern ist die Weitergabe ihrer persönlichen Daten beim Abschluss eines Geschäftes wie z. B. bei Kundenkartenangeboten diverser Unternehmen (BILLA, BIPA) bewusst, und trotzdem würden 57% der Befragten dieser Weitergabe auf keinen Fall zustimmen.

Viele davon interessieren sich, wie viel persönliche Informationen über sie im Internet vorhanden sind und 78% haben bereits etwas über sich gefunden. Das zeigt auf, dass trotz der Aufmerksamkeit bezüglich der Weitergabe personenbezogener Daten eine enorme digitale Datenmenge im Internet über die meisten Personen verbleibt. Schlechte Erfahrungen aufgrund vorhandener elektronischer Spuren hatten nur 3,7% gemacht.

Erstaunlicherweise wissen 27,1% der Berufstätigen nicht, ob ihre E-Mail-Korrespondenz von Dritten gelesen werden darf, und 24,3% glauben, dass ihr Unternehmen sie nicht durch ihre E-Mails überwachen kann.

Bei dem letzten Teil der Befragung ergab sich, dass die Benutzer bei Onlinegeschäften nicht immer die Datenschutzerklärung (6,6% immer und 64,2% ab und zu) lesen, und nur 5,7% glauben, dass das Privacy Statement verständlich auf der Webseite dargestellt ist. Bei einem höheren Risiko, wie z. B. Kreditkartennummerneingabe, liest aber ein größerer Anteil der Benutzer (35,5%) immer die Privacy Policy. Obwohl viele der Befragten vorhandene Gütesiegel kennen (62,6%), interessieren sich 67,3% der Benutzer überhaupt nicht dafür, ob eine Webseite ein Gütesiegel hat. Ebenso wenig beeinflusst deren Vorhandensein sie bei ihrer Entscheidung bezüglich des Abschlusses eines elektronischen Geschäfts.

Kapitel 8

8 Schlussfolgerung

“You have zero privacy anyway – get over it“

Scott McNealy, Chef von Sun Microsystems, 1999

1999 behauptete der Chef von Sun, dass es keine Privatsphäre gäbe. Fünf Jahre später ändert er seine Meinung, indem er sagt: „IT ohne Privacy wird sich in Zukunft nicht mehr verkaufen lassen“.

In dieser Diplomarbeit wurde die Problematik „Electronic Privacy Management“ erläutert. Es wurde gezeigt, wie sich die Privatsphäre im Laufe der Zeit verändert hat und wie die Benutzer sie langsam verlieren. Die Chancen und Risiken, die in der zunehmenden Informationsgesellschaft beim Sammeln personenbezogener Daten entstehen, verändern das Bewusstsein der Bevölkerung bezüglich des Umgangs mit ihrer Privatsphäre. Dieser Prozess ist aber erst der Anfang.

Basierend auf den theoretischen Grundlagen wurde anhand eines Fragebogens im Kapitel 7 untersucht, wie wichtig den Benutzern die Privatsphäre ist, ob sie sich mit ihr auseinandersetzen, ob sie die entstehenden Risiken wahrnehmen und wie sie sich dabei schützen.

Im Allgemeinen lässt sich feststellen, dass viele Benutzer, unter ihnen meist Studenten, die elektronischen Dienstleistungen sehr gerne in Anspruch nehmen. Sie realisieren sehr wohl die möglichen Gefahren und Risiken dabei, nutzen Onlineaktivitäten wie Online-Banking (70,9%), vertrauen dem Unternehmen blind und machen sich dabei nicht viele Gedanken über die negativen Folgen, die daraus entstehen können. Gleichzeitig aber haben sie Angst, jemand könnte online in ihre Daten einsehen und ihre persönlichen Daten missbrauchen. Daher versuchen sie, ihre Daten durch einfache Methoden zu kontrollieren, wie z. B., dass sie ihre E-Mail-Adressen in geringerem Umfang online angeben.

Wenn es um eine technische Unterstützung des Schutzes ihrer Privatsphäre geht, sind die Benutzer weniger informiert. Zwar ist ihnen die Privatsphäre sehr wichtig, sie lesen aber selten die Datenschutzerklärungen der Unternehmen, wenn sie Onlinedienstleistungen in Anspruch nehmen. Die Benutzer sind der Überzeugung, dass sie selbst für ihre Privatsphäre verantwortlich sind, interessieren sich aber

nicht viel für vorhandene Schutzmaßnahmen. Dadurch besteht die Gefahr, dass die Benutzer große Teile ihrer Privatsphäre dauerhaft verlieren, ohne sich dessen bewusst zu sein.

Aus diesem Grund werden an dieser Stelle Handlungsvorschläge für Konsumenten, Unternehmen und Gesetzgeber angeführt, die das Ausmaß der Risiken minimieren und dabei helfen, einen besseren Schutz der Privatsphäre zu gewährleisten. Die Empfehlungen beziehen sich auf die Theoriegrundlage dieser Arbeit, die Analyse der Fallstudie und basieren auf dem International Working Group on Data Protection in Telecommunications „Rom Memorandum“ [vgl. IWG08]:

<u>Konsumenten:</u>

- Informationen, welche z. B. durch Teilnahme an einem Gewinnspiel abgegeben werden, werden meist zu einem anderen Zweck gesammelt. Zu beachten ist in diesem Fall, an wen die Informationen weitergegeben werden und ob es eine Opt-out-Möglichkeit gibt.
- Auf SPAM sollte in keinem Fall geantwortet werden, da sich danach die Werbeflut enorm vergrößert. Man kann aber versuchen, durch SPAM-Filter Nachrichten mit ähnlichem Inhalt dauerhaft zu sperren.
- Da beim Arbeitsplatz eine sehr große Wahrscheinlichkeit besteht, dass Online-Aktivitäten überwacht werden, sollten persönliche Postings oder E-Mails vom Computer zu Hause geschickt werden.
- Um weitergegebene persönliche Informationen besser zu kontrollieren, sollte der Browser entsprechend konfiguriert werden. Eine der Möglichkeiten, die Privatsphäre zu schützen, ist, einen P3P-fähigen Internet Explorer zu benutzen.
- Privacy Policies informieren über die Datenschutzpolitik des Unternehmens. Gütesiegel, die von Unternehmen wie TRUSTe, BBBOnLine etc. ausgestellt sind, verleihen diesen Richtlinien eine größere Glaubwürdigkeit. Daher sollten bei elektronischen Transaktionen solche Gütesiegel auf der Webseite beachtet werden.
- Die Verwendung einer anonymen E-Mail-Adresse und Pseudonyme bei Postings und sozialen Netzwerken helfen bei der Kontrolle unerwünschter Werbemails (SPAM). Wenn eine Adresse verlangt, aber kein Passwort per

E-Mail zugeschickt wird, ist die Angabe einer „echten“ Adresse nicht notwendig.

- Die Privatsphäre Dritter soll respektiert werden, daher sollen Personendaten wie Fotos mit Zusatzangaben wie Namensbeschriftung vermieden werden. Auch bei der Veröffentlichung eigener Daten soll man sich zuvor Gedanken machen, ob diese in einem Bewerbungsgespräch zu unerwünschten Folgen führen können.
- Fremden sollten z. B. im Chat oder auf der persönlichen Homepage bei YouTube oder MySpace keine persönlichen Informationen wie Adresse, Telefonnummer und Ähnliches bekannt gegeben werden.
- Der Benutzer entscheidet selbst, welche persönliche Information er weitergibt. Das Schlimmste, was bei der Angabe falscher Daten passieren kann, ist, dass die gewünschte Dienstleistung nicht weiter benutzt werden darf bzw. verboten wird.

<u>Unternehmen:</u>

- Unternehmen können bessere Kontrolle für Benutzer anbieten, indem sie ihnen die Möglichkeit geben, komplett seine Daten zu löschen, selbst zu entscheiden, welche seiner Daten in der Suchfunktion von sozialen Netzwerke erscheinen und was mit seinen Profildaten passieren soll.
- Unternehmen sollen die Benutzerdaten als wertvolles Kapital ansehen, das sie nur bzw. mehr bekommen, wenn sie das Vertrauen von Benutzer gegenüber dem Unternehmen verstärken.
- Eine Verbesserung der Möglichkeit für Benutzer, Missbrauch auf der Webseite zu melden, z. B. mittels eines Buttons auf jeder Seite.
- Die Privacy Policy (Datenschutzerklärung) möglichst verständlich und benutzerfreundlich zu gestalten und auf der Webseite so zu platzieren, dass sie leicht auffindbar ist.
- Unternehmen sollen Mitarbeiter über die E-Mail-Korrespondenz, SPAM-Bekämpfung und Weitergabe geschäftlicher Daten informieren.

- Durch entsprechend ersichtliche Platzierung und Erklärung eines Gütesiegels auf der Webseite könnte das Vertrauen der Konsumenten gegenüber dem Unternehmen erhöht werden.

Gesetzgeber:

- Aufgrund zunehmender Benutzung des Internets durch Jugendliche und Kinder gehört der Datenschutzunterricht unbedingt an die Schulen.
- Datenschutzerklärungen müssen unter die Lupe genommen werden und Korrekturen sind anzuregen. Die Benutzer sollten über Datenbearbeitungszwecke entsprechender Webseiten die Weitergabe der persönlichen Daten oder die Geltendmachung des Auskunftsrechts Bescheid wissen.
- Durch Kampagnen bezüglich der Gefahren im Internet sollen die Benutzer sensibilisiert werden.

9 Anhang: Fragebogen

Hier werden der Fragebogen, der im Kapitel 7 erklärt wurde, und seine Ergebnisse dargestellt:

Fragebogen: Electronic Privacy Management

Diese Umfrage ist Teil meiner Diplomarbeit.

Ich werde mich freuen, wenn Sie sich nur 10 Min Ihrer Zeit in Anspruch nehmen und mir dabei sehr helfen. Vielen Dank.

1. Haben Sie Computer zu Hause?

a) ☐ ja b) ☐ nein

2. Wie oft benutzen Sie das Internet bzw. wie häufig surfen Sie im Internet?

a) ☐ Mindestens einmal täglich
b) ☐ Mindestens einmal in der Woche
c) ☐ Mindestens einmal im Monat
d) ☐ Weniger als einmal im Monat
e) ☐ Ich benutze nie das Internet

3. Seit wann benutzen Sie das Internet?

a) ☐ Seit mehr als 5 Jahren
b) ☐ Seit 3-5 Jahren
c) ☐ Seit 1-3 Jahren
d) ☐ Seit circa einem Jahr
e) ☐ Erst seit kurzem
f) ☐ Ich benutze nie das Internet

4. Wo benutzen Sie das Internet? (mehrfache Benennung)

a) ☐ Zu Hause
b) ☐ An der Universität
c) ☐ Beim Arbeitsplatz
d) ☐ Nirgendwo

5. Beurteilen Sie die folgenden Aussagen über Internet:

	trifft voll zu	trifft eher zu	trifft weniger zu	trifft nicht zu	trifft überhaupt nicht zu
Es ist schwierig das Internet zu benutzen	☐	☐	☐	☐	☐
Es ist schwierig das zu finden was ich will	☐	☐	☐	☐	☐
Jemand kann verfolgen was ich online mache	☐	☐	☐	☐	☐
Ich bekomme zuviel SPAM (junk E-mail)	☐	☐	☐	☐	☐
Meine persönliche Information kann online gestohlen werden	☐	☐	☐	☐	☐
Jemand kann meine persönliche Information, die ich preisgebe, missbrauchen	☐	☐	☐	☐	☐
Die preisgegebene Information kann später zu unerwünschten Folgen führen	☐	☐	☐	☐	☐
Ich bin skeptisch was das Internet angeht	☐	☐	☐	☐	☐
Ich finde, das Internet ist eine tolle Sache	☐	☐	☐	☐	☐

6. Zu welchem Zweck nutzen Sie das Internet? (mehrfache Benennung)

a) ☐ Onlinekauf

b) ☐ Online-Banking

c) ☐ Surfen/Hobby

d) ☐ Kommunikation/Chat/ E-Mail/ Newsgroup

e) ☐ Beruflich

f) ☐ Zu Weiterbildung

7. Falls Sie im Internet persönliche Daten preisgeben müssen, um z. B. ein Konto zu errichten oder online einzukaufen, bei welchen Daten haben Sie Bedenken, diese preiszugeben? *(mehrfache Benennung)*

a) ☐ Name

b) ☐ Adresse (E-Mail, Post)

c) ☐ Kreditkartennummer

d) ☐ Geburtsdatum

e) ☐ Sozialversicherungsnummer

f) ☐ Telefonnummer

g) ☐ Bevorzugte Produkte, die Sie einkaufen

h) ☐ Hobbies

8. Wie würden Sie die Preisgabe folgender personenbezogenen Daten an eine Webseite beurteilen?

	sehr gefährlich	1	2	3	4	5	6	7	gar nicht gefährlich
Name		☐	☐	☐	☐	☐	☐	☐	
Adresse (E-Mail, Post)		☐	☐	☐	☐	☐	☐	☐	
Kreditkartennummer		☐	☐	☐	☐	☐	☐	☐	
Geburtsdatum		☐	☐	☐	☐	☐	☐	☐	
SozialversicherungsNr		☐	☐	☐	☐	☐	☐	☐	
Telefonnummer		☐	☐	☐	☐	☐	☐	☐	
Bevorzugte Produkte, die sie einkaufen		☐	☐	☐	☐	☐	☐	☐	
Hobbies		☐	☐	☐	☐	☐	☐	☐	

9. Haben Sie es jemals abgelehnt, persönliche Information an Unternehmen oder eines Geschäftes preiszugeben (z. B. kein Online-Banking errichtet), weil Sie gedacht haben, es sei zu persönlich bzw. Sie hatten Angst? *(mehrfache Benennung)*

a) ☐ Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil ich Angst hatte, jemand könnte in meine Daten einsehen

b) ☐ Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil sie mir zu persönlich waren

c) ☐ Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil mir die Seite nicht sicher erschien

d) ☐ Nein, ich gebe meistens meine Daten preis

e) ☐ Nein, ich habe im Internet nie ein Geschäft abgeschlossen

f) ☐ Ich weiß es nicht/ habe keine Meinung

10. Wenn ich meine persönlichen Daten im Internet preisgebe, bin ich mir nicht sicher, wer diese sammelt

a) ☐ trifft voll zu
b) ☐ trifft eher zu
c) ☐ trifft weniger zu
d) ☐ trifft nicht zu
e) ☐ trifft überhaupt nicht zu

11. Sind Sie darüber besorgt, wieviel Information über Sie im Internet verfügbar ist?

a) ☐ Ja, ich mache mir immer Sorgen
b) ☐ Ja, ich mache mir ab und zu Sorge
c) ☐ Nein, ich mache mir keine Sorgen
d) ☐ Ich weiß es nicht/ habe keine Meinung

12. Haben Sie irgendwann mal versucht, Ihre persönliche Information im Internet zu reduzieren oder nicht? (z. B. wenn Sie Ihre E-Mail, Telefonnummer, Geburtsdatum usw. weniger preisgeben)

a) ☐ Ja, ich habe es versucht
b) ☐ Nein, ich mache das nicht
c) ☐ Ich weiß es nicht/ habe keine Meinung

13. Welche der folgenden Dienste, die zur Kontrolle Ihres Datenschutzes dienen, kennen Sie? (*mehrfache Benennung*)

a) ☐ P3P (Plattform for Privacy Preferences Project)
b) ☐ Privacy Bird
c) ☐ EPAL
d) ☐ APPEL
e) ☐ Keine

14. Kennen Sie im Internet Explorer den „Datenschutzbericht“ unter dem „Ansicht“-Menü?

a) ☐ Ja
b) ☐ Nein

15. Haben Sie sich jemals dafür interessiert, wie die Datenschutzeinstellung im Internet Explorer durch das Menü „Ansicht-Datenschutzbericht“ funktioniert?

a) ☐ Ja
b) ☐ Nein
c) ☐ Ich weiß es nicht/ habe keine Meinung

16. Wissen Sie, dass P3P (Plattform for Privacy Preferences Project) im Internet Explorer schon integriert ist und automatisch Ihre persönlichen Daten kontrolliert und dadurch Ihre Privatsphäre schützt, wenn Sie dieses aktivieren?

a) ☐ Ja
b) ☐ Nein
c) ☐ Ich weiß nicht was P3P ist

17. Wenn ich im Internet surfe, kann ich nicht kontrollieren, wieviel Information die Webseite über mich sammelt?

stimme voll zu	1	2	3	4	5	6	7	stimme überhaupt nicht zu
	☐	☐	☐	☐	☐	☐	☐	

18. Wenn ich im Internet etwas kaufe, kann ich nicht kontrollieren, wer meine persönlichen Daten sammelt?

stimme voll zu	1	2	3	4	5	6	7	stimme überhaupt nicht zu
	☐	☐	☐	☐	☐	☐	☐	

19. Inwieweit ist der Schutz Ihrer persönlichen Daten wichtig?

sehr wichtig	1	2	3	4	5	6	7	überhaupt nicht wichtig
	☐	☐	☐	☐	☐	☐	☐	

20. Wer, glauben sie, soll Ihre Privatsphäre schützen? *(mehrfache Benennung)*

a) ☐ Regierung
b) ☐ Jeder Benutzer ist für sich selbst verantwortlicht (durch Technologien)
c) ☐ Unternehmen
d) ☐ Jeder (der Schutz ist durch bestimmte Verhaltensnormen garantiert)
e) ☐ Keiner
f) ☐ Ich weiß es nicht

21. Kennen Sie einige von den unten aufgezählten Begriffen?

(mehrfache Benennung)

a) ☐ Phishing
b) ☐ Spearing
c) ☐ Spyware
d) ☐ SPAM
e) ☐ Ich kenne keine

22. Haben Sie irgendwann auf eine Phishing-Attacke/Spearing/SPAM reagiert bzw. was bestellt?

a) ☐ Ja, einmal
b) ☐ Mehr als nur einmal
c) ☐ Nie
d) ☐ Ich weiß nicht was Phishing/Spearing bzw. SPAM bedeutet

23. Ist Ihnen dadurch ein Schaden entstanden?

a) ☐ Nein
b) ☐ 1 - 100 EUR
c) ☐ 100 - 500 EUR
d) ☐ 500 - 1000 EUR
e) ☐ ab 1000 EUR
f) ☐ Ich weiß nicht was Phishing/Spearing bzw. SPAM bedeutet

24. Beurteilen Sie inwieweit Online-Banking Ihrer Meinung nach sicher ist?

Ich habe volles Vertrauen	1	2	3	4	5	6	7	ich habe überhaupt kein Vertrauen
	☐	☐	☐	☐	☐	☐	☐	

25. Welche der folgenden sozialen Netze kennen Sie? *(mehrfache Benennung)*

a) ☐YouTube
b) ☐Facebook
c) ☐MySpace
d) ☐StudiVZ
e) ☐Ich kenne keine

26. Haben sie ein Konto bei irgendwelchen in der vorigen Frage dargestellten sozialen Netzwerken?

a) ☐Ja
b) ☐Nein (überspringen Sie die nächste Frage)

27. Akzeptieren Sie auch Leute, die Sie nicht kennen, als Ihre online „Freunde“?

a) ☐Ja
b) ☐Nein
c) ☐Keine Ahnung

28. Wenn sie Ihre persönlichen Daten bei so einer Website (z. B. Facebook) online hinterlassen, wer, glauben Sie, kann in Ihre private Information einsehen?

a) ☐Nur ich
b) ☐Ich und meine Freunde
c) ☐Niemand
d) ☐Spammer, Hacker
e) ☐Ich weiß es nicht

29. Wieviel SPAM haben Sie im letzten Monat circa pro Tag bekommen?

a) ☐Keine
b) ☐1-5
c) ☐5-10
d) ☐10-20
e) ☐über 20
f) ☐Keine Ahnung

Verschiedene Firmen bieten Kundenkarten (Billa, BIPA, Tchibo) an.

30. Wissen Sie, dass beim Abschluss dieses Geschäftes Ihre persönlichen Daten (z. B. Ihr Name, Adresse, Einkaufsverhalten) nur mit Ihrer Zustimmung gesammelt und an Dritten (zu Marketingzwecken) weitergegeben werden?

a) ☐Ja
b) ☐Nein

31. Nehmen Sie an, Sie hätten gern so eine Kundenkarte. Würden Sie dieser Bedingung (Weitergabe Ihrer persönlichen Daten an Dritten) zustimmen?

a) ☐ Ja
b) ☐ Vielleicht
c) ☐ Nein, auf keinen Fall
d) ☐ Ich weiß es nicht

32. Haben Sie mittels einer Suchmaschine (z. B. Google) Informationen über sich selbst gesucht (z. B Ihr Name), um zu sehen, was für persönliche Information über Sie im Internet steht?

a) ☐ Ja
b) ☐ Nein (nächste Frage überspringen)
c) ☐ Ich weiß es nicht

33. Wenn Sie im Internet nach Ihrem Namen gesucht haben, haben Sie dabei was gefunden oder nicht?

a) ☐ Ja
b) ☐ Nein

34. Hatten sie jemals schlechte Erfahrungen damit gehabt, dass personenbezogene Informationen über Sie im Internet stehen? (z. B. kein Job bekommen, weil Sie was im Internet publiziert haben, das dem zukünftigen Arbeitgeber nicht passt)

a) ☐ Ja
b) ☐ Nein
c) ☐ über mich gibt es nichts im Internet

35. Glauben sie, dass Ihre Daten im Internet nicht sicher sind und von unautorisierten Dritten oder Organisationen gesammelt werden können?

stimme voll zu	1	2	3	4	5	6	7	stimme überhaupt nicht zu
	☐	☐	☐	☐	☐	☐	☐	

36. Wissen Sie, ob in dem Unternehmen in welchem Sie arbeiten, Ihre Emailkorrespondenz gelesen werden darf?

a) ☐ Ja, meine Emails dürfen gelesen werden
b) ☐ Nein, es wird nichts überwacht
c) ☐ Ich weiß es nicht
d) ☐ Ich bin nicht berufstätig

37. Lesen Sie die Privacy Policy (Datenschutzerklärung) einer Webseite, wenn Sie ein elektronisches Geschäft abschließen?

a) ☐ Immer b) ☐ Ab und zu c) ☐ Nein

38. Glauben sie, dass die Privacy Policy (Datenschutzerklärung) meistens unverständlich, voll mit gesetzlichem Jargon ist?

a) ☐ Ja b) ☐ Teilweise c) ☐ Nein d) ☐ Ich weiß es nicht

39. Wenn Sie sensitive Daten übermitteln sollen, wie ihre Kreditkartennummer, lesen Sie dann die Datenschutzerklärung des Unternehmens?

a) ☐ Ja, Immer b) ☐ Nicht immer c) ☐ Nein d) ☐ Ich weiß es nicht

40. Sagt Ihnen der Begriff „Gütesiegel“ etwas?

a) ☐ Ja b) ☐ Nein c) ☐ Ich weiß es nicht

41. Die folgenden Unternehmen/Gütesiegel beschäftigen sich mit der Einhaltung des Datenschutzes, was auf einer Webseite in Form einer Datenschutzerklärung dargestellt wird. Welche von den aufgezählten Unternehmen/Gütesiegel kennen Sie?

a) ☐ TRUSTe
b) ☐ BBBOnLine
c) ☐ Web Trust
d) ☐ EuroPriSe = European Privacy Seal
e) ☐ Ich kenne keine

42. Wenn Sie ein elektronisches Geschäft abschließen, achten Sie darauf, ob die Webseite ein Gütesiegel hat?

a) ☐ Ja b) ☐ Nicht immer c) ☐ Nein d) ☐ Ich weiß es nicht

43. Beeinflusst Sie das Vorhandensein eines Gütesiegels auf der Webseite, wenn Sie die Absicht haben, online was zu kaufen?

mit zehr großer Wahrscheinlichkeit	1	2	3	4	5	6	7	mit gar keiner Wahrscheinlichkeit
	☐	☐	☐	☐	☐	☐	☐	

44. Darf ich Sie abschließend um ein paar Angaben bitten. Ihre Angaben werden anonym behandelt.

44. Ihr Geschlecht?

a) ☐Weiblich b) ☐Männlich

45. Ihr Alter?

a) ☐Unter 22 b) ☐22-30 c) ☐31-45 d) ☐46-60 e) ☐60+

46. Ihr höchster Ausbildungsstand?

a) ☐HAK
b) ☐Gymnasium
c) ☐Technische Schule
d) ☐Abgeschlossene Lehre
e) ☐Matura
f) ☐Akadem. Grad
g) ☐Anderes

47. Welchen Beruf über Sie aus?

a) ☐Studentln
b) ☐Angestellte/r
c) ☐Arbeiterln
d) ☐Wissenschaftlicher Mitarbeiterln
e) ☐Management
f) ☐Selbständig
g) ☐Arbeitslos
h) ☐Anderes

48. Wo wohnen Sie?

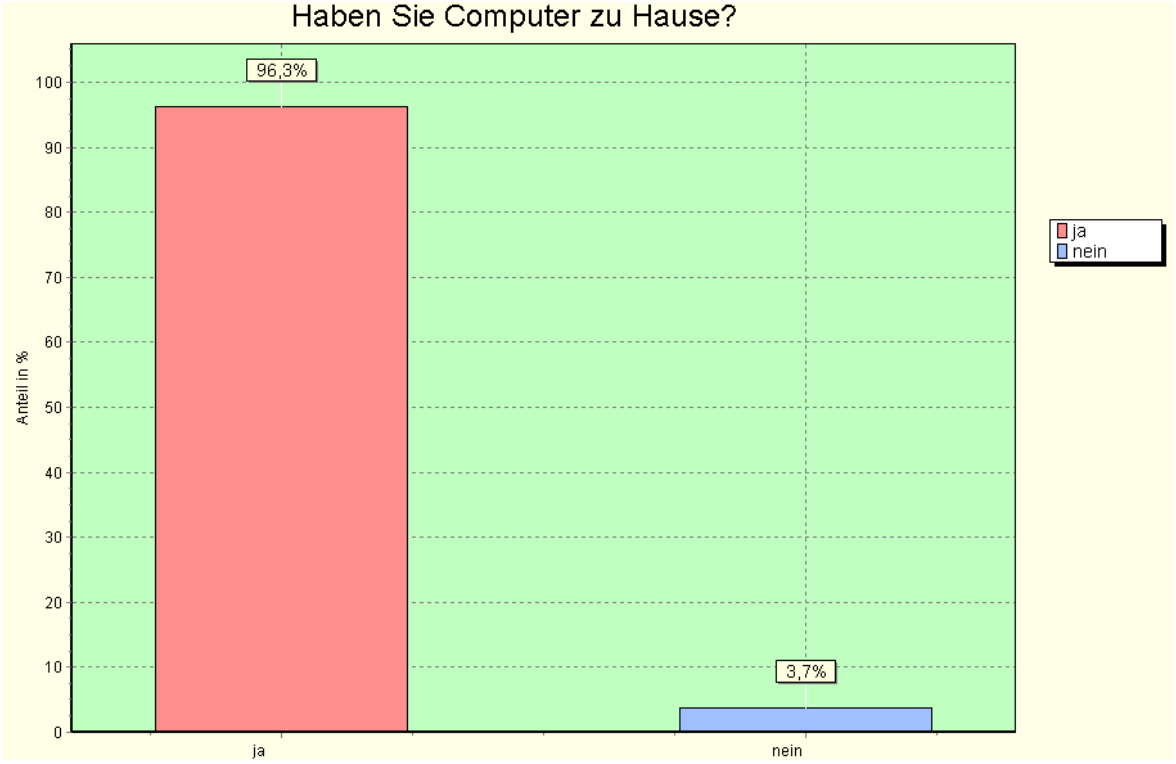
a) ☐Europa
b) ☐Nordamerika
c) ☐Südamerika
d) ☐Asien
e) ☐Afrika
f) ☐Australien, Neuseeland

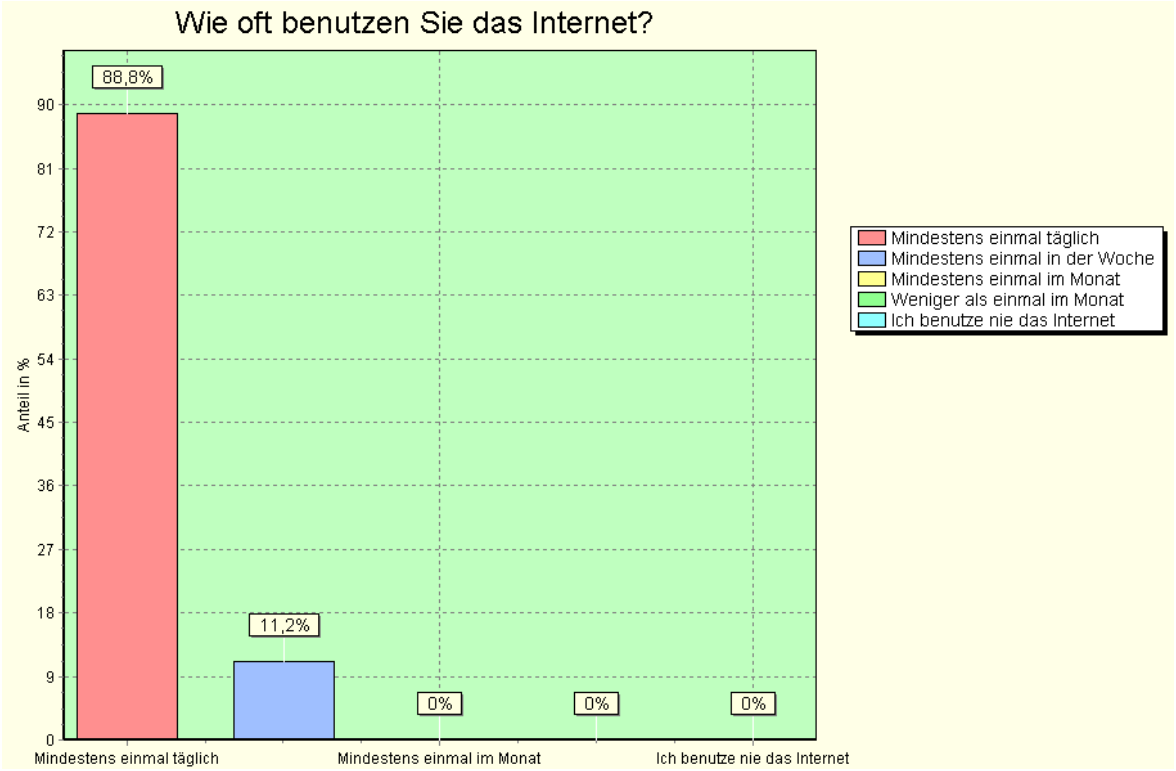
49. Leben Sie in einer Stadt oder auf dem Lande?

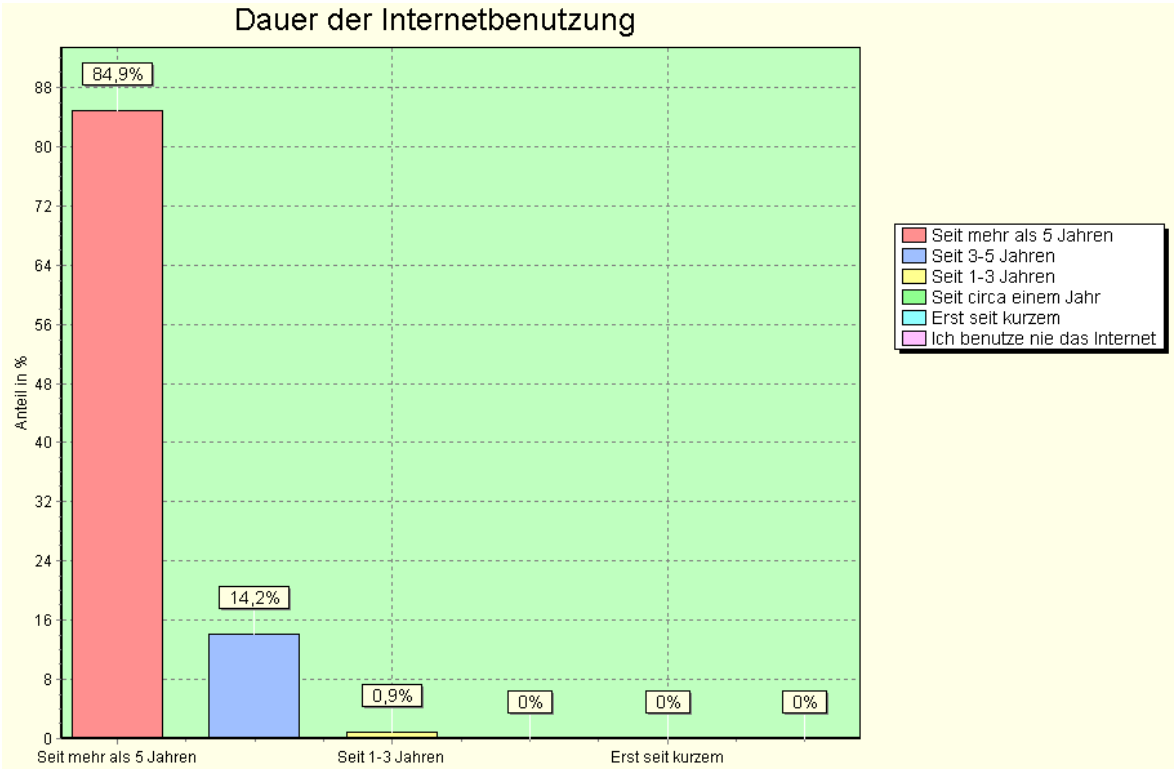
a) ☐Eine Großstadt b) ☐eine Kleinstadt c) ☐Auf dem Lande

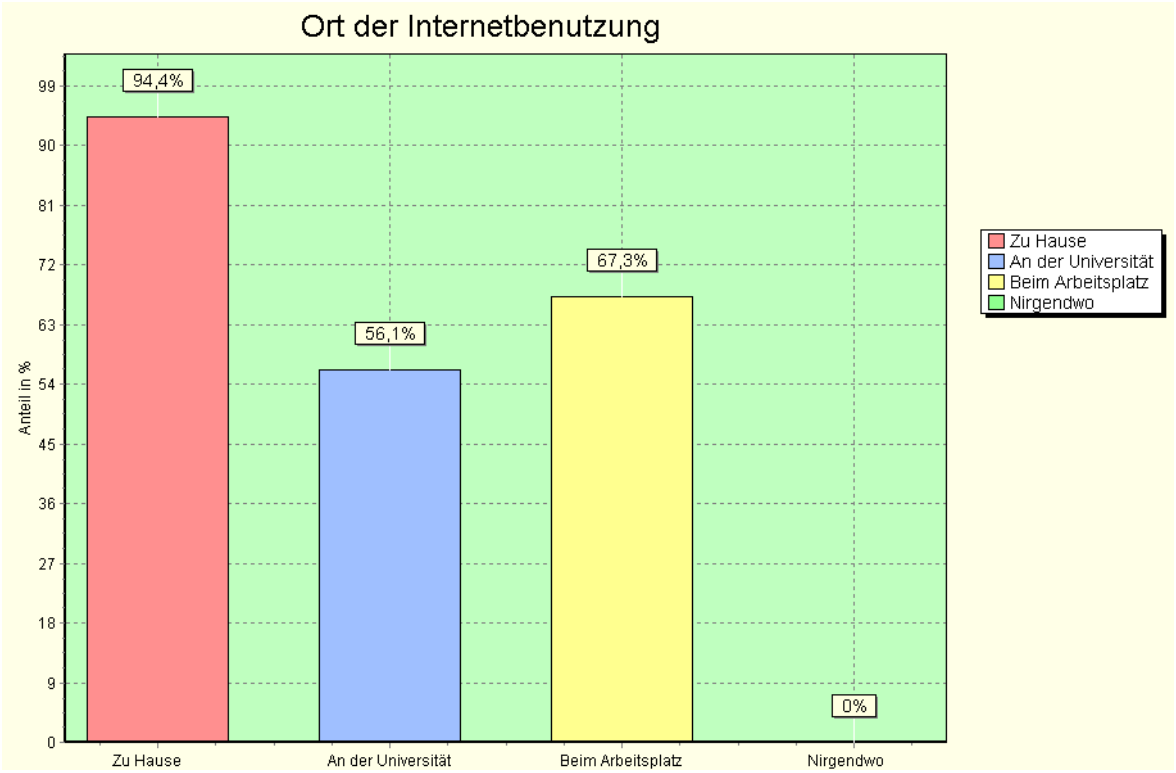
Ich bedanke mich herzlich für Ihre Mithilfe.

Auswertung:


Haben Sie Computer zu Hause?
96,3%
3,7%
Anteil in %
100
90
80
70
60
50
40
30
20
10
0
ja
nein
ja
nein


Wie oft benutzen Sie das Internet?
88,8%
11,2%
0%
0%
0%
Anteil in %
90
81
72
63
54
45
36
27
18
9
0
Mindestens einmal täglich
Mindestens einmal im Monat
Ich benutze nie das Internet
Mindestens einmal täglich
Mindestens einmal in der Woche
Mindestens einmal im Monat
Weniger als einmal im Monat
Ich benutze nie das Internet

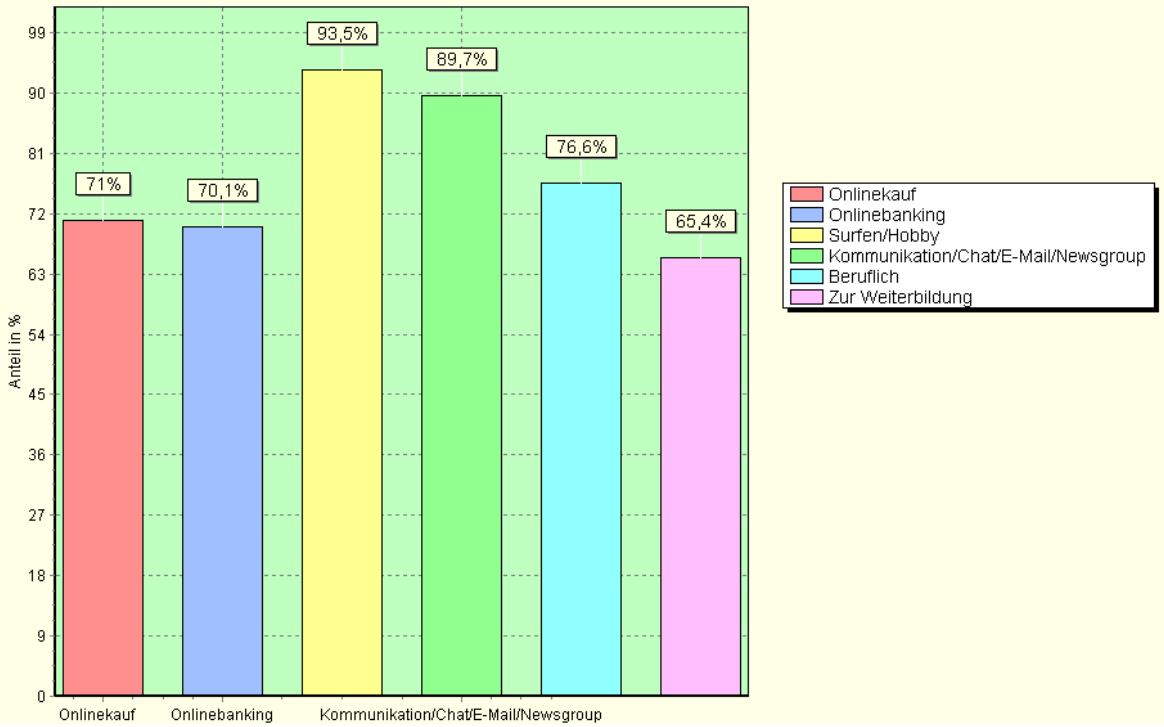

Dauer der Internetbenutzung
Anteil in %
84,9%
14,2%
0,9%
0%
0%
0%
Seit mehr als 5 Jahren
Seit 1-3 Jahren
Erst seit kurzem
Seit mehr als 5 Jahren
Seit 3-5 Jahren
Seit 1-3 Jahren
Seit circa einem Jahr
Erst seit kurzem
Ich benutze nie das Internet


Ort der Internetbenutzung
Anteil in %
94,4%
56,1%
67,3%
0%
Zu Hause
An der Universität
Beim Arbeitsplatz
Nirgendwo
Zu Hause
An der Universität
Beim Arbeitsplatz
Nirgendwo

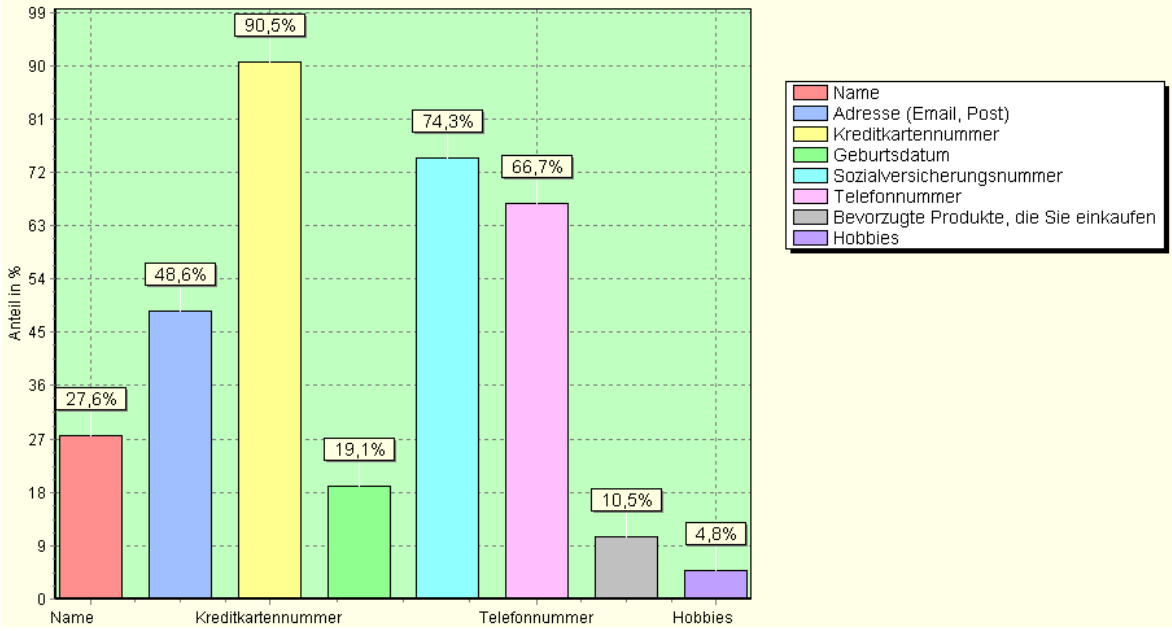
Beurteilen Sie die folgenden Aussagen über das Internet

Merkmal	trifft voll zu	trifft eher zu	trifft weniger zu	trifft nicht zu	trifft überhaupt nicht zu	Summe
Es ist schwierig das zu finden was ich will	0,9%	12,2%	25,2%	43,0%	18,7%	100,0%
Jemand kann verfolgen was ich online mache	26,2%	41,1%	20,6%	5,6%	6,5%	100,0%
Ich bekomme zuviel SPAM (junk mail)	30,8%	30,8%	28,0%	8,4%	1,9%	100,0%
Meine persönliche Information kann online gestohlen werden	22,4%	37,4%	29,0%	8,4%	2,8%	100,0%
Jemand kann meine persönliche Information, die ich preisgebe, missbrauchen	33,6%	35,5%	19,6%	8,4%	2,8%	100,0%
Die preisgegebene Information kann später zu unerwünschten Folgen führen	31,8%	38,3%	18,7%	9,4%	1,9%	100,0%
Ich bin skeptisch was das Internet angeht	0,9%	15,9%	39,3%	29,9%	14,0%	100,0%
Ich finde, das Internet ist eine tolle Sache	74,3%	20,9%	1,0%	1,0%	2,9%	100,0%

Zweck der Internetnutzung



Falls Sie im Internet persönliche Daten preisgeben müssen, um z.B. ein Konto zu errichten oder online einzukaufen, bei welchen Daten haben Sie Bedenken,diese preiszugeben?



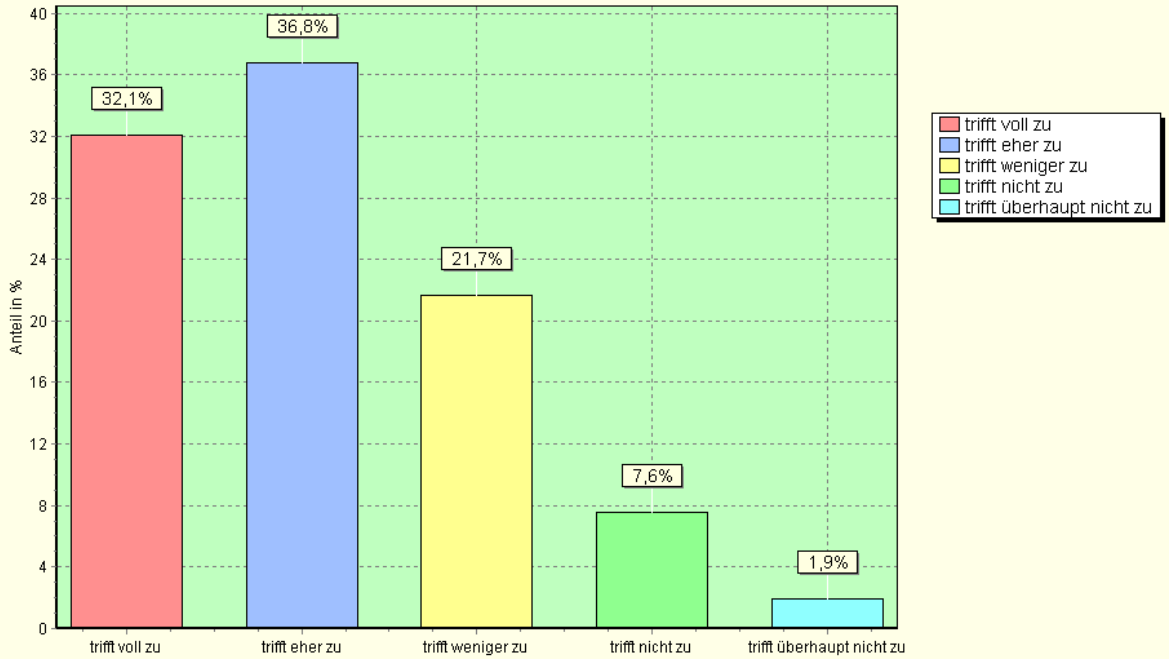
Wie würden Sie die Preisgabe folgender personenbezogenen Daten an eine Webseite beurteilen?

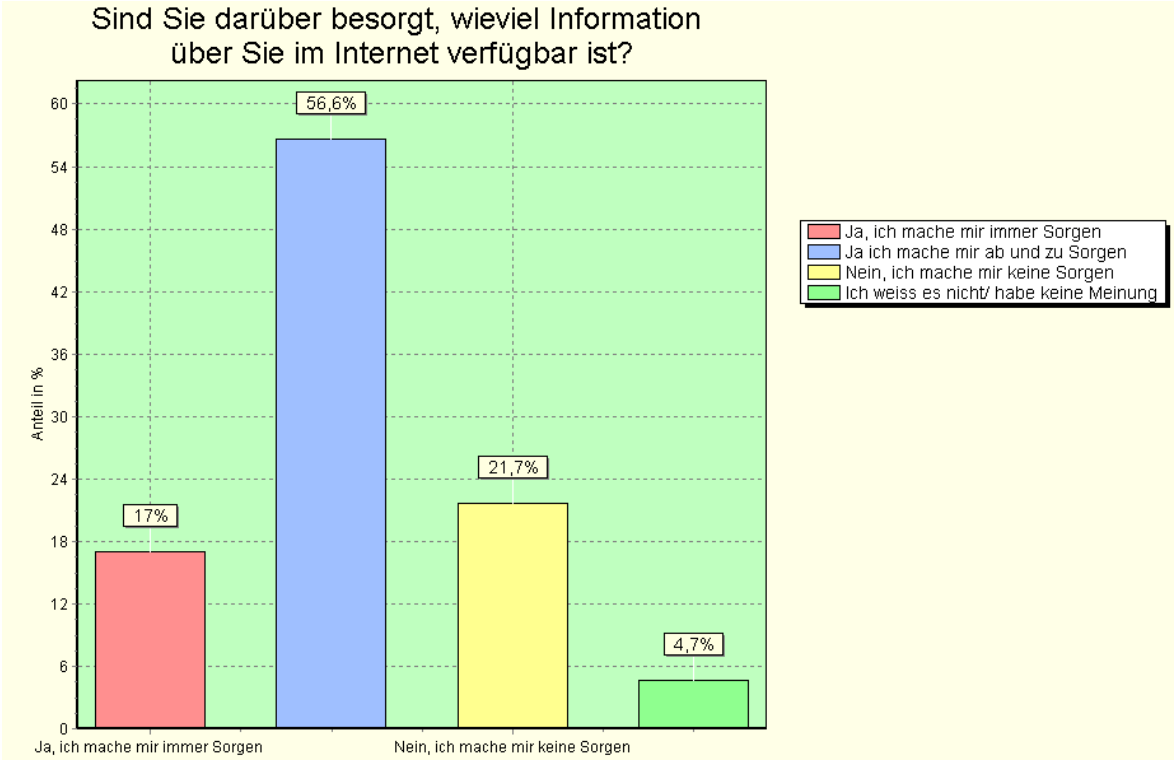
Merkmal	sehr gefährlich	2	3	4	5	6	gar nicht gefährlich	Summe
Name	11,8%	7,8%	11,8%	21,6%	17,7%	21,6%	7,8%	100,0%
Adresse (Email, Post)	17,7%	14,7%	19,6%	25,5%	10,8%	7,8%	3,9%	100,0%
Kreditkartennummer	68,9%	16,5%	8,7%	1,9%	1,0%	1,0%	1,9%	100,0%
Geburtsdatum	5,9%	6,9%	18,8%	17,8%	21,8%	15,8%	12,9%	100,0%
Sozialversicherungsnummer	47,1%	23,5%	13,7%	5,9%	2,0%	3,9%	3,9%	100,0%
Telefonnummer	24,5%	18,6%	25,5%	14,7%	8,8%	4,9%	2,9%	100,0%
Bevorzugte Produkte, die sie einkaufen	3,9%	4,8%	4,8%	14,6%	16,5%	28,2%	27,2%	100,0%
Hobbies	0,0%	1,9%	3,9%	12,6%	18,5%	24,3%	38,8%	100,0%

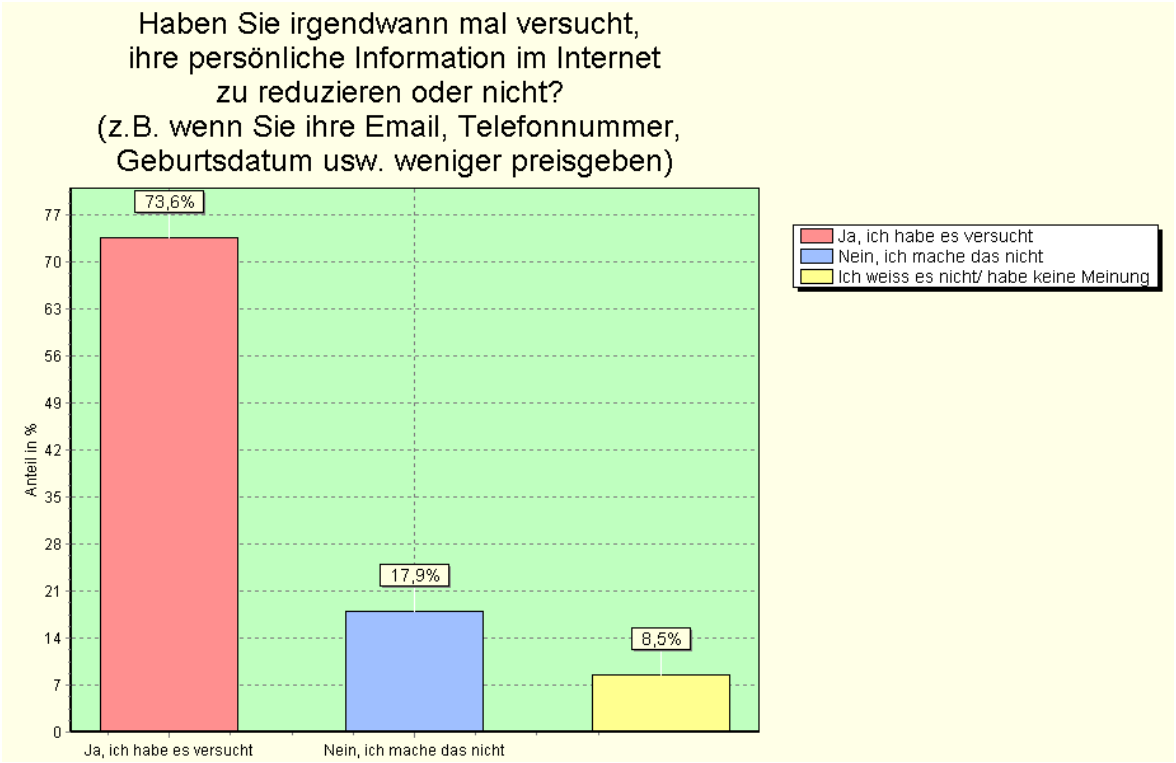
Haben Sie es jemals abgelehnt, persönliche Information an Unternehmen oder eines Geschäftes preiszugeben (z.B. kein Online-Banking errichtet), weil Sie gedacht haben, es sei zu persönlich, Angst hatten, jemand könnte in Ihre Daten einsehen oder diese missbrauchen? (mehrfache Benennung)

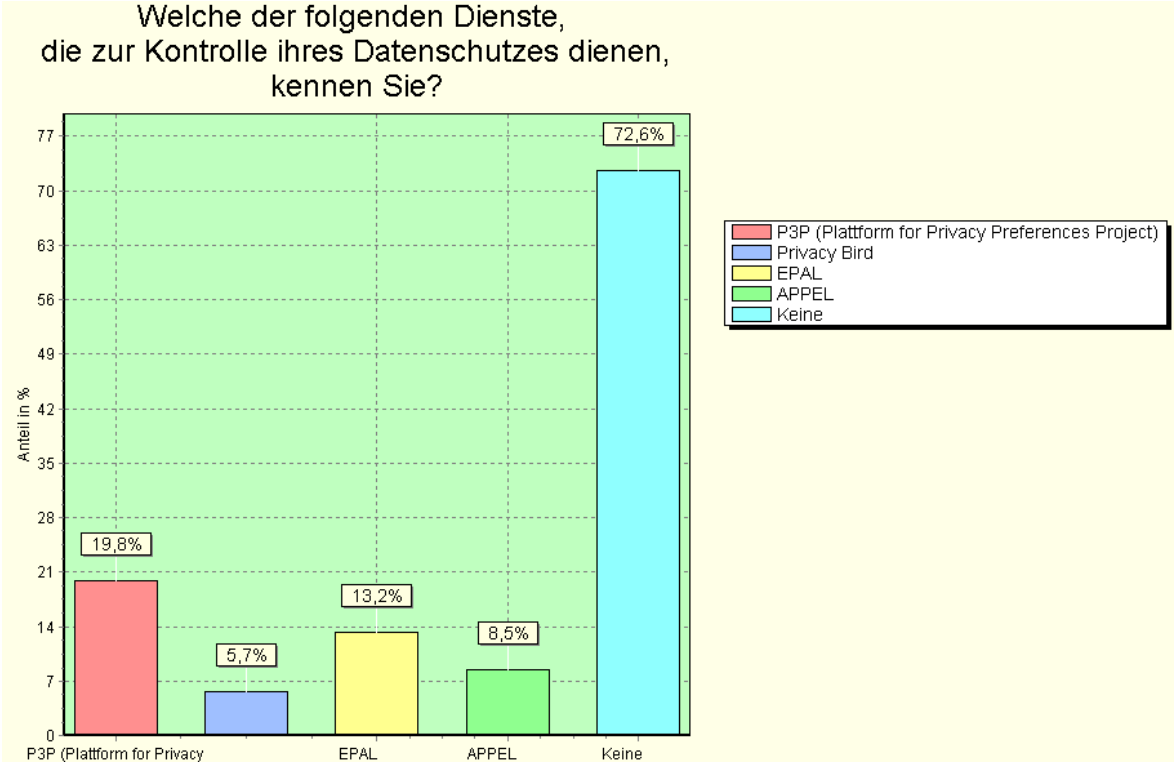
Nennung	Anteil
Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil ich Angst hatte, jemand könnte in meine Daten einsehen	45,8%
Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil sie mir zu persönlich waren	46,7%
Ja, ich habe schon persönliche Angaben nicht weitergegeben, weil mir die Seite nicht sicher erschien	69,2%
Nein, ich gebe meistens meine Daten preis	9,4%
Nein, ich habe im Internet nie ein Geschäft abgeschlossen	3,7%
Ich weiss es nicht/ habe keine Meinung	2,8%
Anteil	177,6%

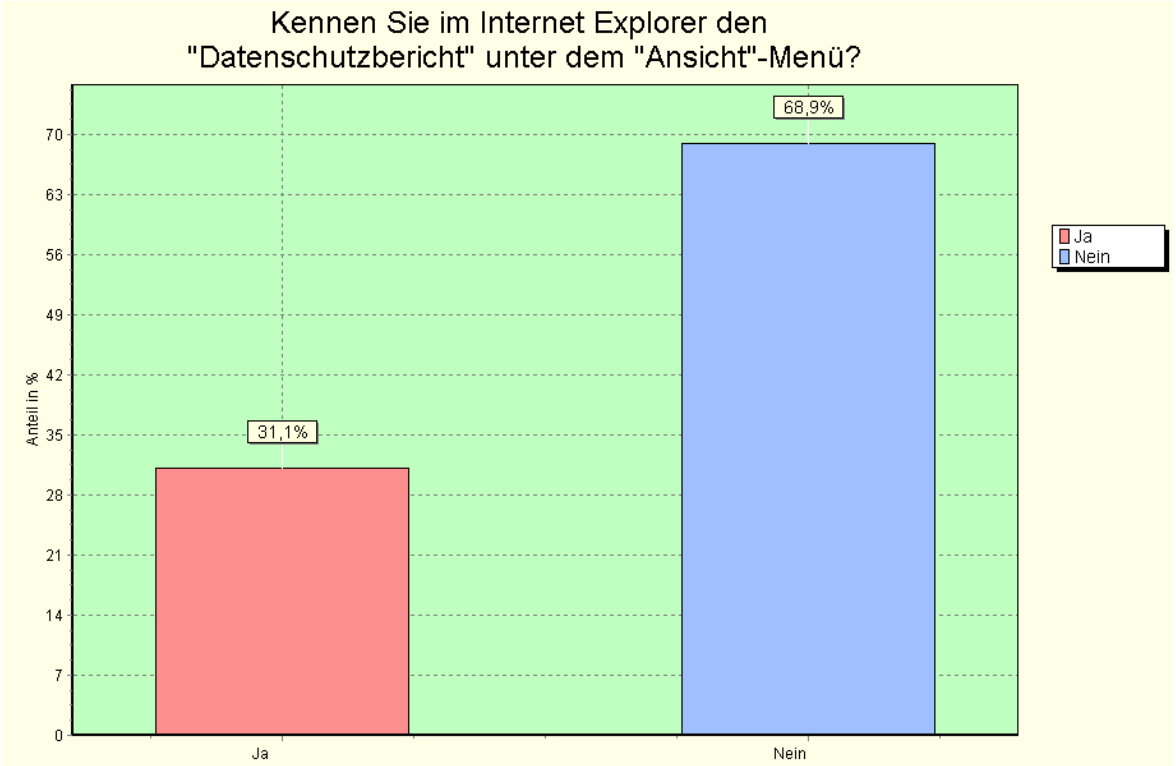
Wenn ich meine persönlichen Daten im Internet preisgebe, bin ich mir nicht sicher, wer diese sammelt

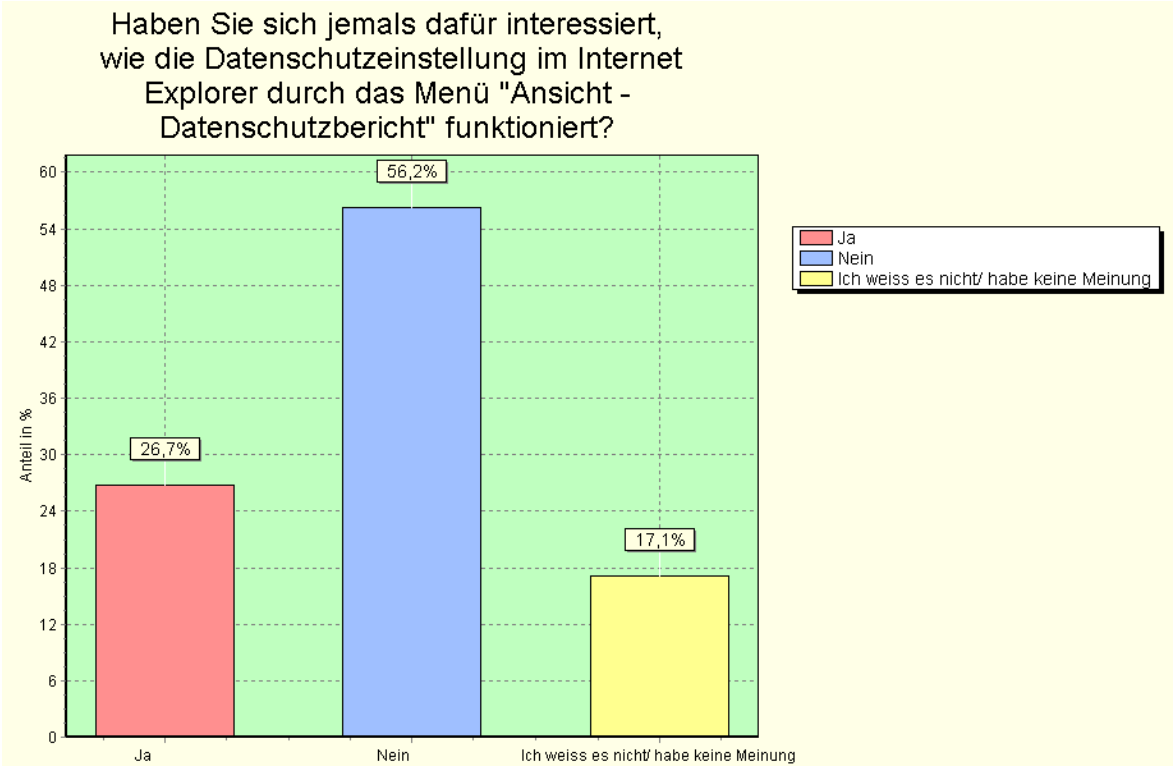


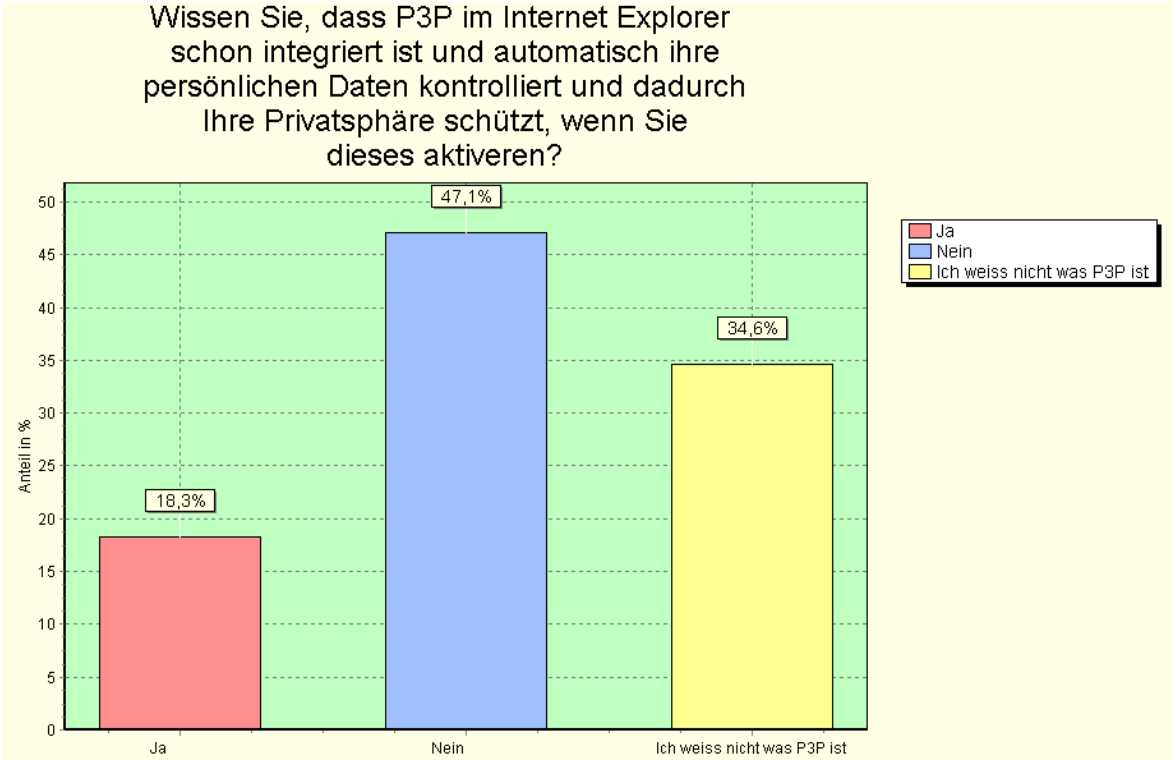

Sind Sie darüber besorgt, wieviel Information über Sie im Internet verfügbar ist?
Anteil in %
60
54
48
42
36
30
24
18
12
6
0
56,6%
21,7%
17%
4,7%
Ja, ich mache mir immer Sorgen
Nein, ich mache mir keine Sorgen
Ja, ich mache mir immer Sorgen
Ja ich mache mir ab und zu Sorgen
Nein, ich mache mir keine Sorgen
Ich weiss es nicht/ habe keine Meinung

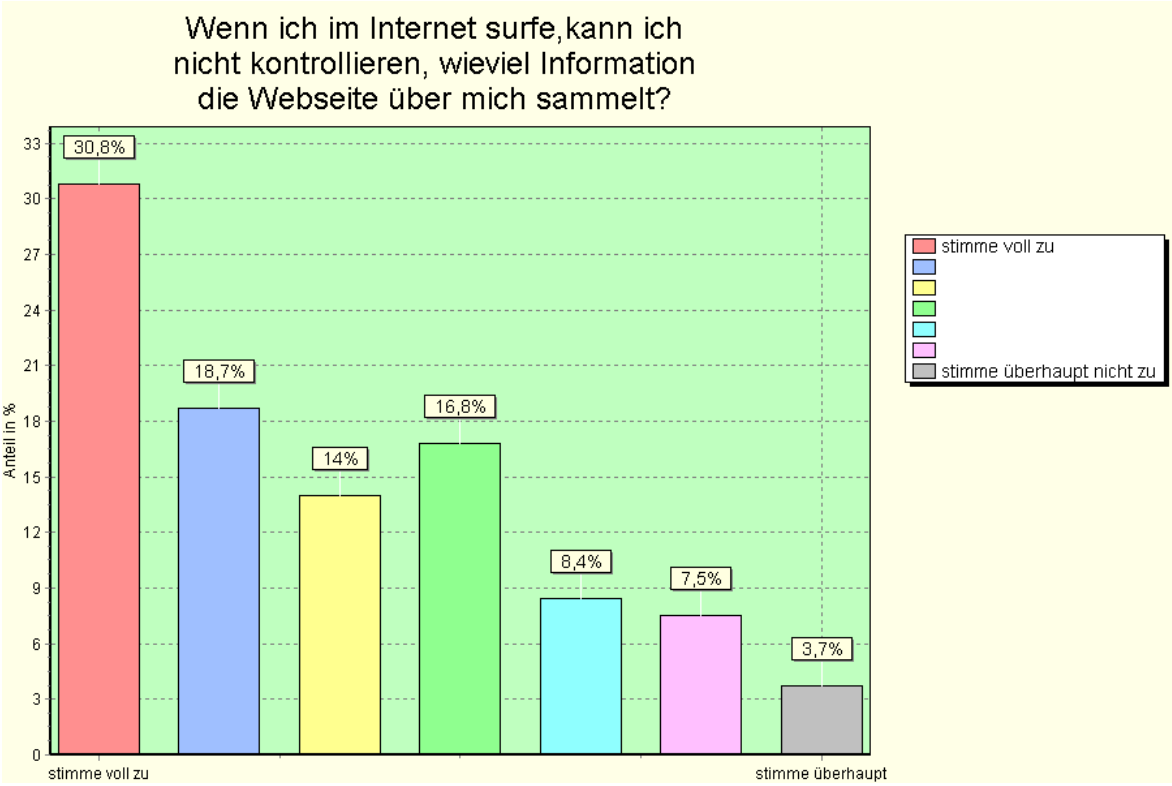

Haben Sie irgendwann mal versucht, ihre persönliche Information im Internet zu reduzieren oder nicht? (z.B. wenn Sie ihre Email, Telefonnummer, Geburtsdatum usw. weniger preisgeben)
Anteil in %
77
70
63
56
49
42
35
28
21
14
7
0
73,6%
17,9%
8,5%
Ja, ich habe es versucht
Nein, ich mache das nicht
Ja, ich habe es versucht
Nein, ich mache das nicht
Ich weiss es nicht/ habe keine Meinung

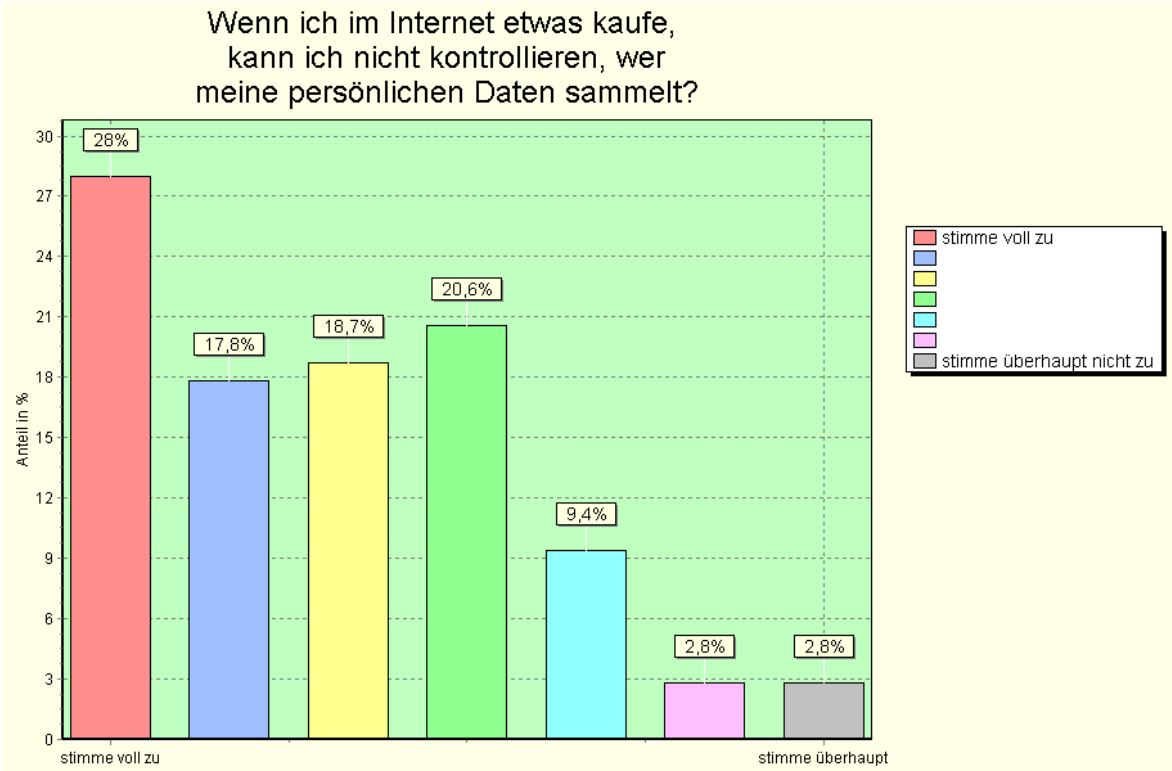

Welche der folgenden Dienste, die zur Kontrolle ihres Datenschutzes dienen, kennen Sie?
Anteil in %
77
70
63
56
49
42
35
28
21
14
7
0
19,8%
5,7%
13,2%
8,5%
72,6%
P3P (Plattform for Privacy
EPAL
APPEL
Keine
P3P (Plattform for Privacy Preferences Project)
Privacy Bird
EPAL
APPEL
Keine

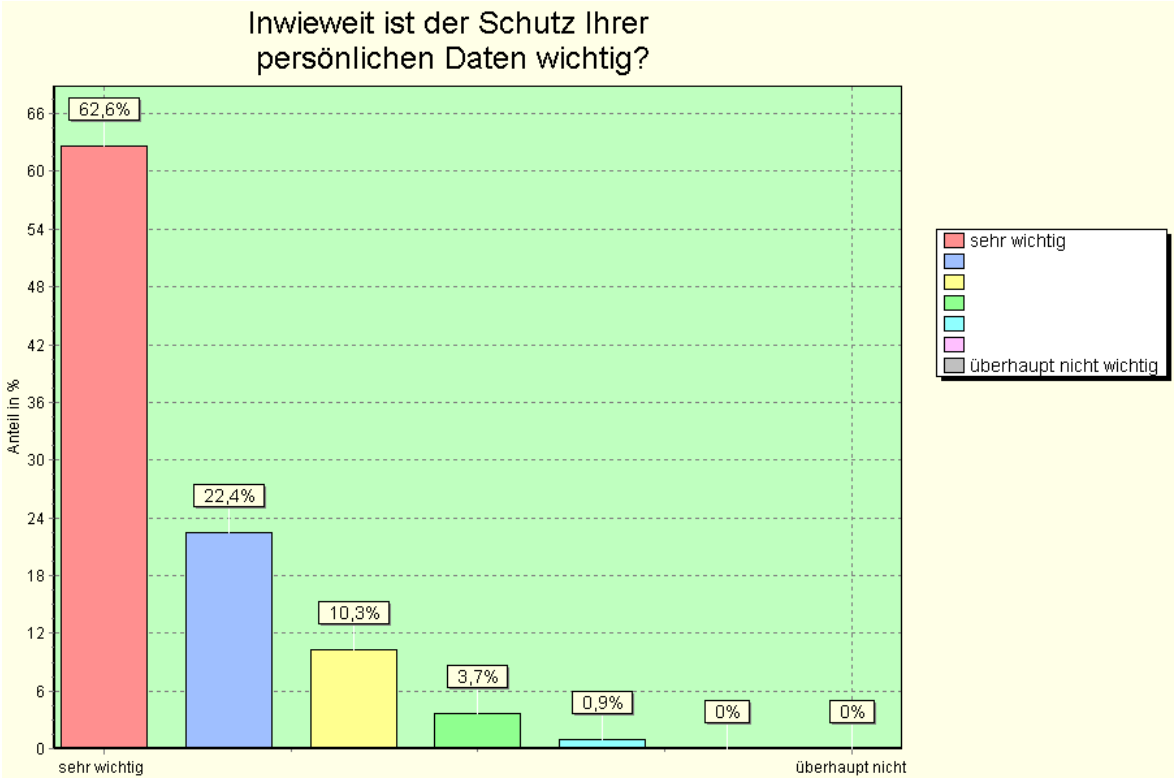

Kennen Sie im Internet Explorer den "Datenschutzbericht" unter dem "Ansicht"-Menü?
Anteil in %
70
63
56
49
42
35
28
21
14
7
0
31,1%
68,9%
Ja
Nein
Ja
Nein

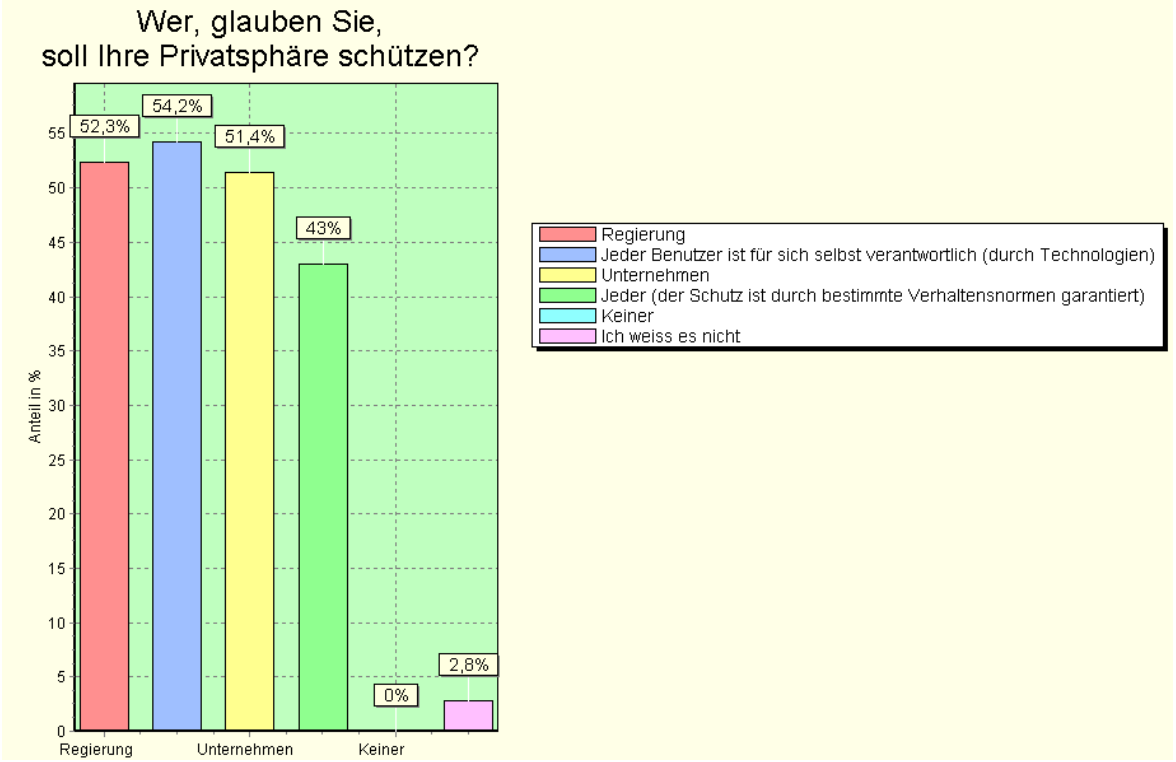

Haben Sie sich jemals dafür interessiert, wie die Datenschutzeinstellung im Internet Explorer durch das Menü "Ansicht - Datenschutzbericht" funktioniert?
Anteil in %
60
54
48
42
36
30
24
18
12
6
0
26,7%
56,2%
17,1%
Ja
Nein
Ich weiss es nicht/ habe keine Meinung
Ja
Nein
Ich weiss es nicht/ habe keine Meinung

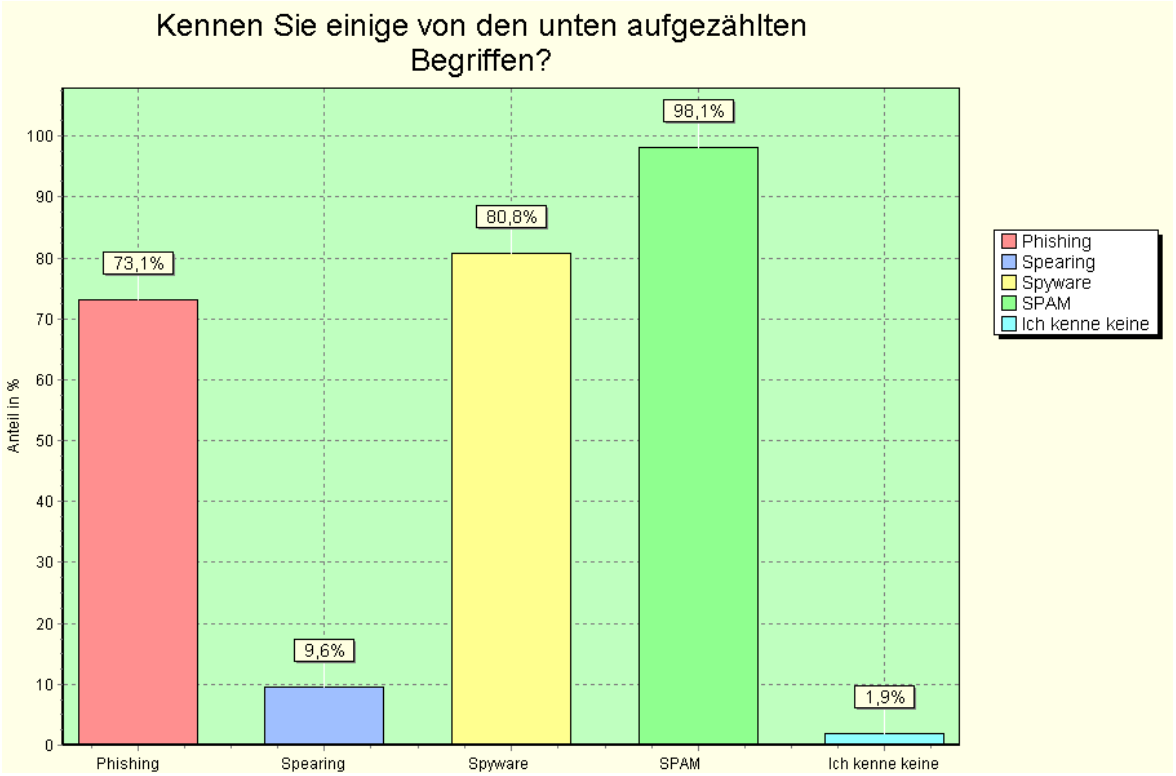

Wissen Sie, dass P3P im Internet Explorer schon integriert ist und automatisch ihre persönlichen Daten kontrolliert und dadurch Ihre Privatsphäre schützt, wenn Sie dieses aktiveren?
Anteil in %
50
45
40
35
30
25
20
15
10
5
0
18,3%
47,1%
34,6%
Ja
Nein
Ich weiss nicht was P3P ist
Ja
Nein
Ich weiss nicht was P3P ist

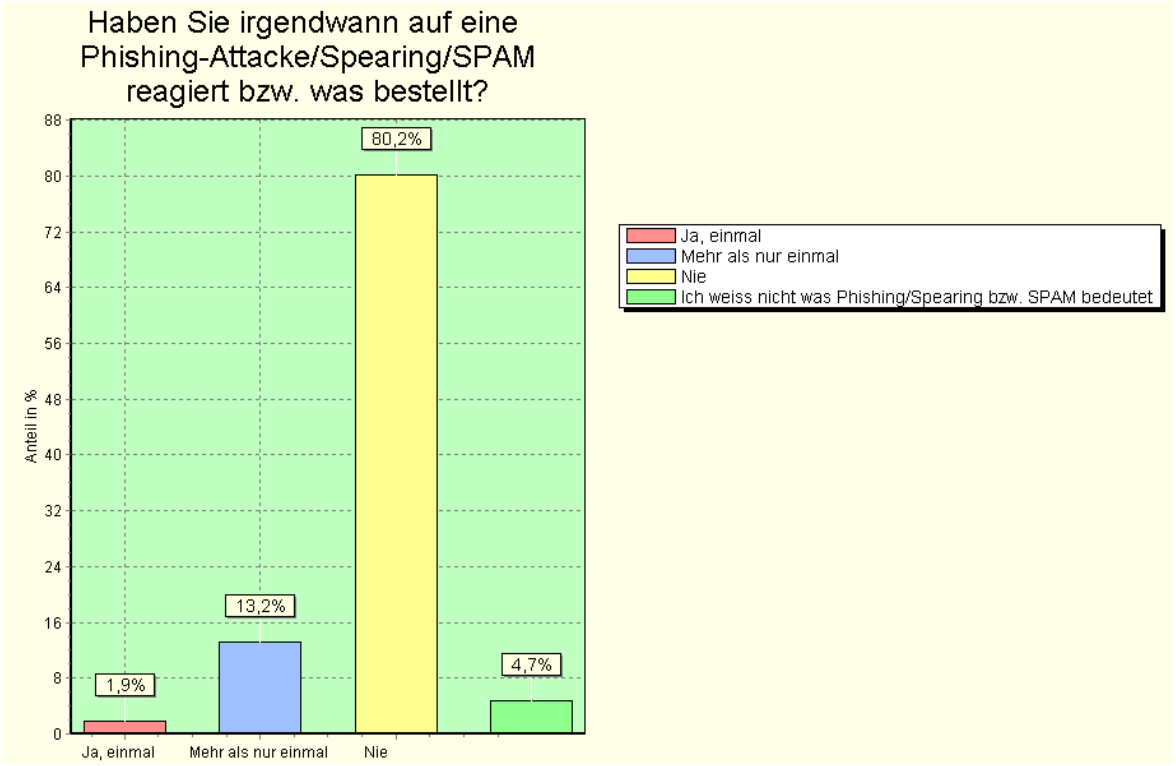

Wenn ich im Internet surfe,kann ich nicht kontrollieren, wieviel Information die Webseite über mich sammelt?
Anteil in %
30,8%
18,7%
14%
16,8%
8,4%
7,5%
3,7%
stimme voll zu
stimme überhaupt
stimme voll zu
stimme überhaupt nicht zu

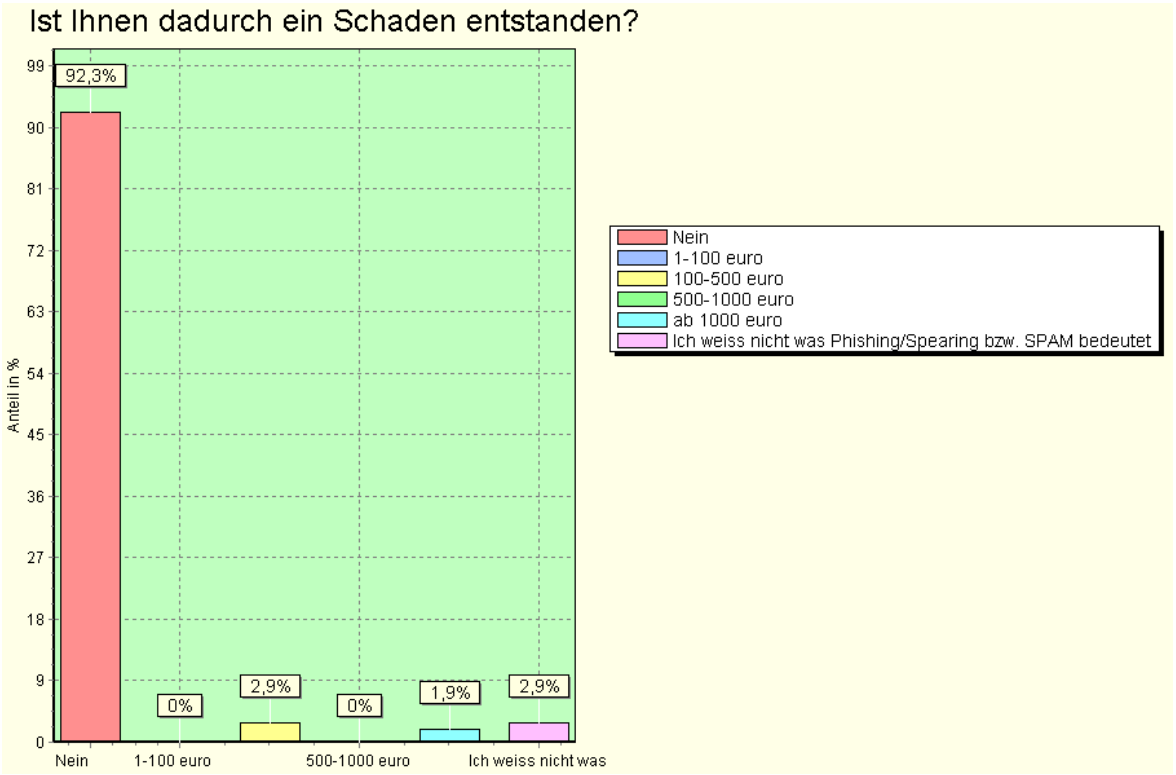

Wenn ich im Internet etwas kaufe, kann ich nicht kontrollieren, wer meine persönlichen Daten sammelt?
Anteil in %
28%
17,8%
18,7%
20,6%
9,4%
2,8%
2,8%
stimme voll zu
stimme überhaupt
stimme voll zu
stimme überhaupt nicht zu

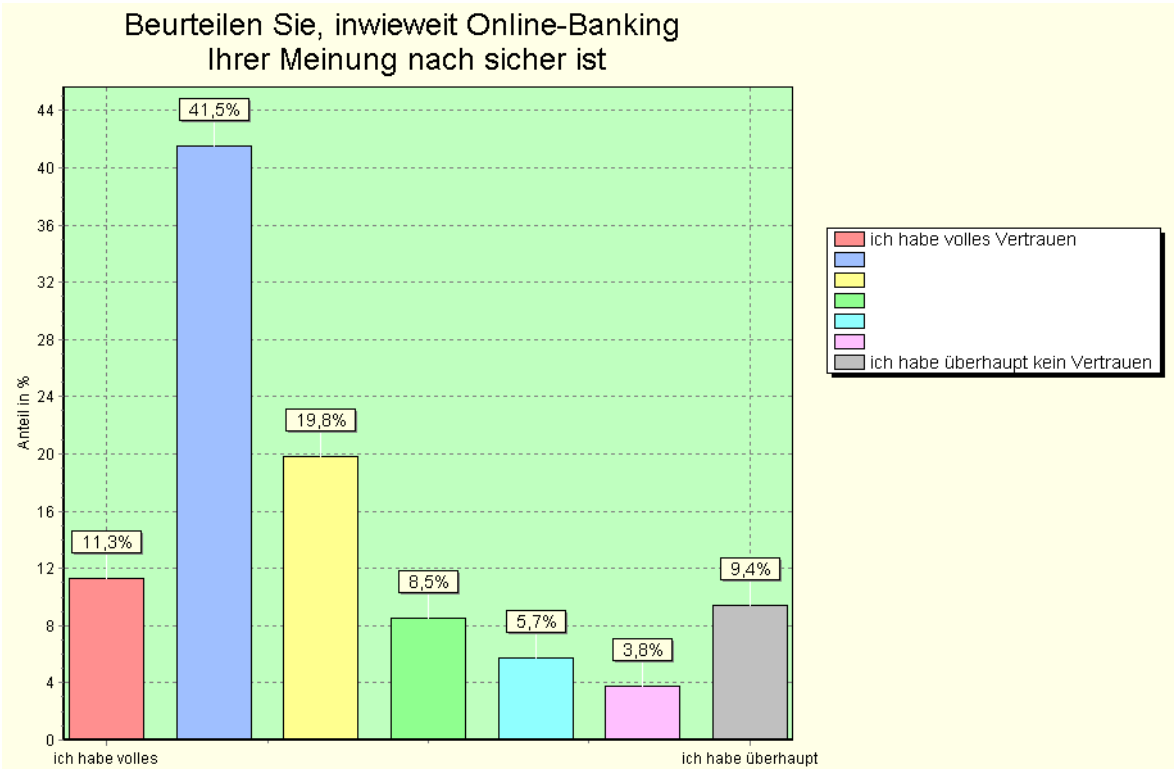

Inwieweit ist der Schutz Ihrer persönlichen Daten wichtig?
Anteil in %
62,6%
22,4%
10,3%
3,7%
0,9%
0%
0%
sehr wichtig
überhaupt nicht
sehr wichtig
überhaupt nicht wichtig

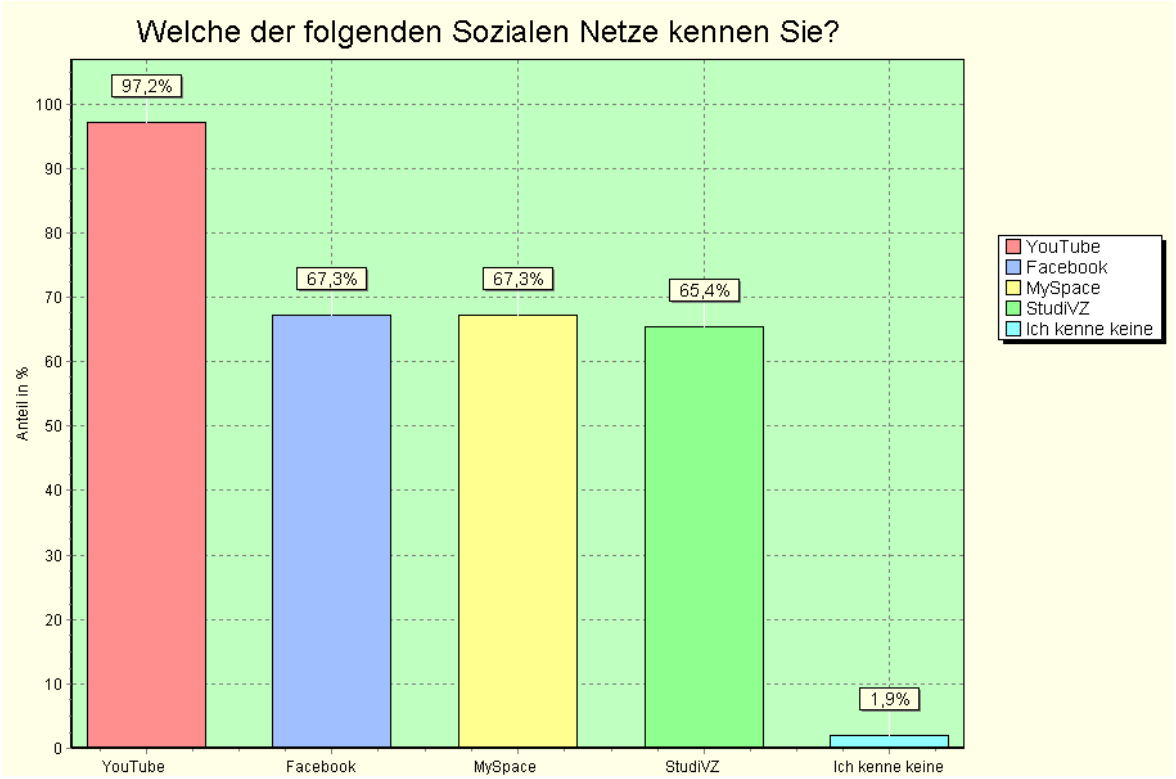

Wer, glauben Sie, soll Ihre Privatsphäre schützen?
Anteil in %
52,3%
54,2%
51,4%
43%
0%
2,8%
Regierung
Unternehmen
Keiner
Regierung
Jeder Benutzer ist für sich selbst verantwortlich (durch Technologien)
Unternehmen
Jeder (der Schutz ist durch bestimmte Verhaltensnormen garantiert)
Keiner
Ich weiss es nicht

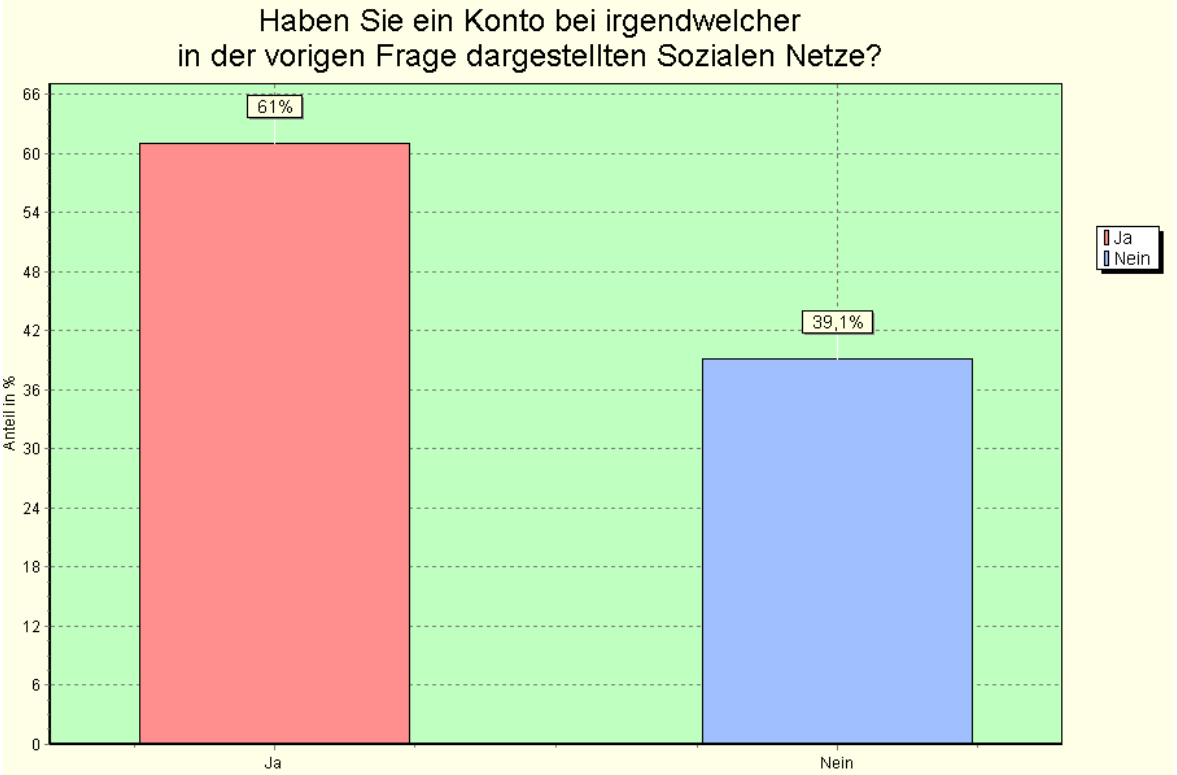

Kennen Sie einige von den unten aufgezählten Begriffen?
Anteil in %
100
90
80
70
60
50
40
30
20
10
0
73,1%
9,6%
80,8%
98,1%
1,9%
Phishing
Spearing
Spyware
SPAM
Ich kenne keine
Phishing
Spearing
Spyware
SPAM
Ich kenne keine

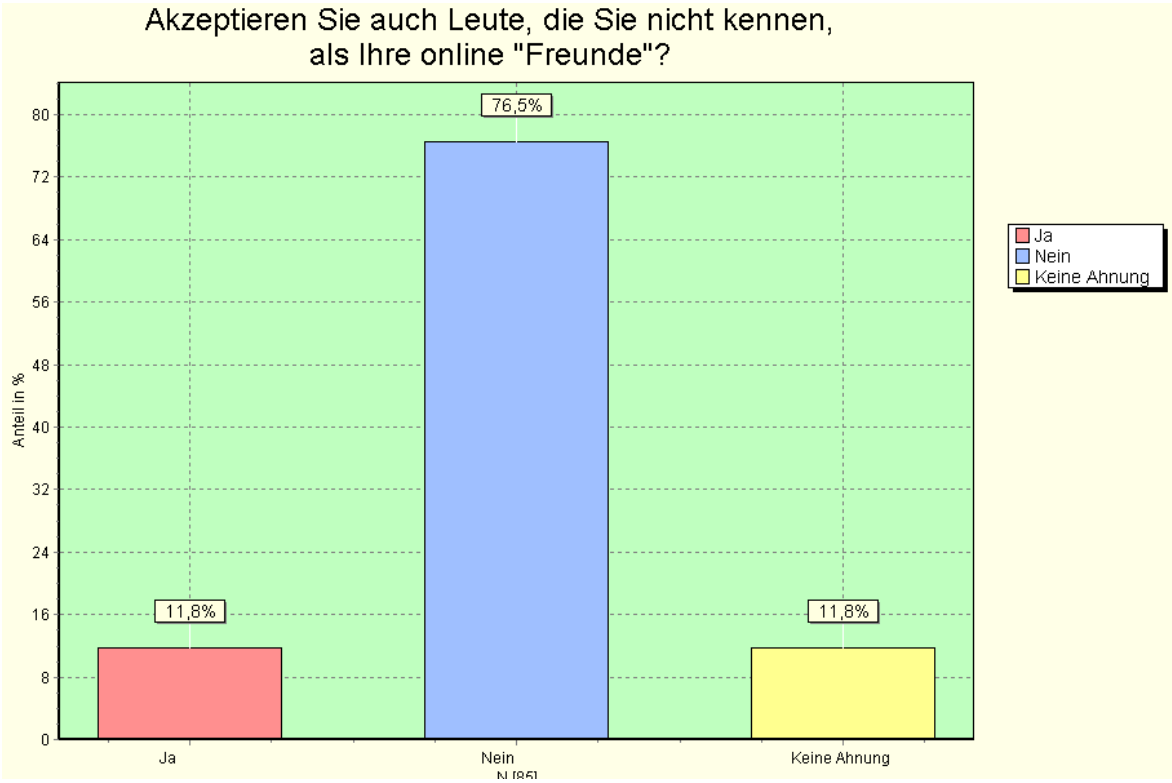

Haben Sie irgendwann auf eine Phishing-Attacke/Spearing/SPAM reagiert bzw. was bestellt?
Anteil in %
88
80
72
64
56
48
40
32
24
16
8
0
1,9%
13,2%
80,2%
4,7%
Ja, einmal
Mehr als nur einmal
Nie
Ich weiss nicht was Phishing/Spearing bzw. SPAM bedeutet

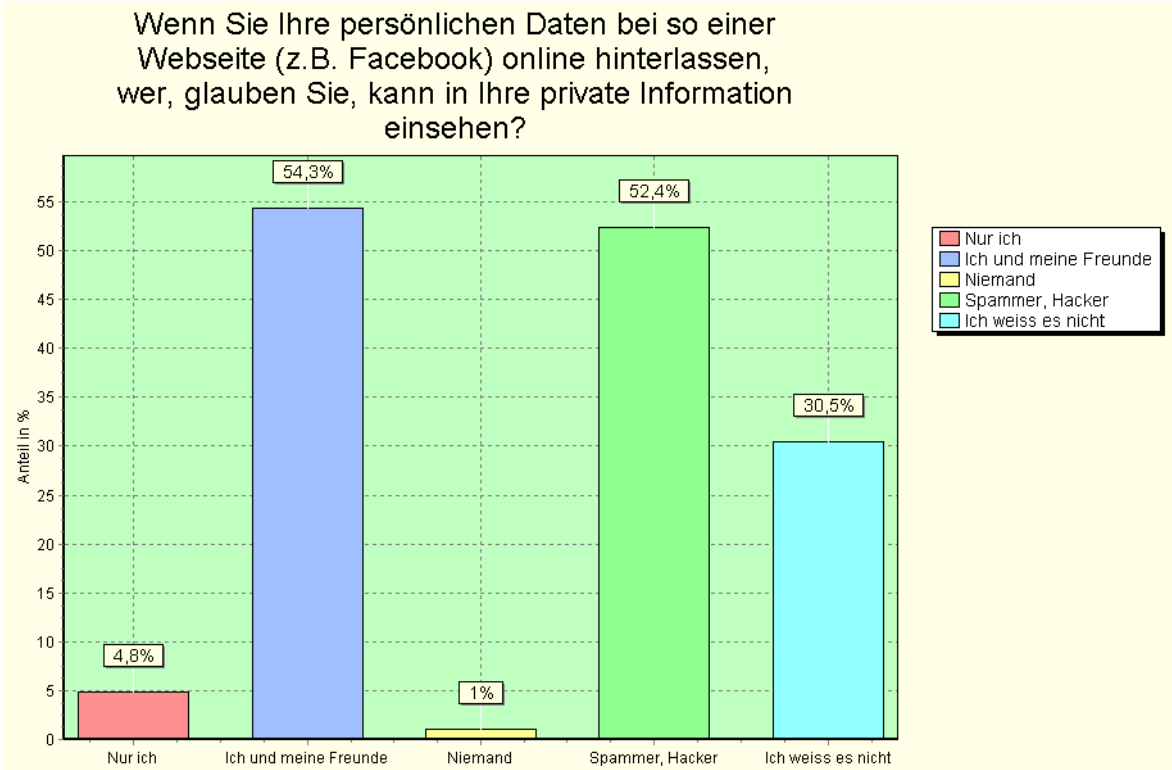

Ist Ihnen dadurch ein Schaden entstanden?
Anteil in %
99
90
81
72
63
54
45
36
27
18
9
0
92,3%
0%
2,9%
0%
1,9%
2,9%
Nein
1-100 euro
500-1000 euro
Ich weiss nicht was
Nein
1-100 euro
100-500 euro
500-1000 euro
ab 1000 euro
Ich weiss nicht was Phishing/Spearing bzw. SPAM bedeutet

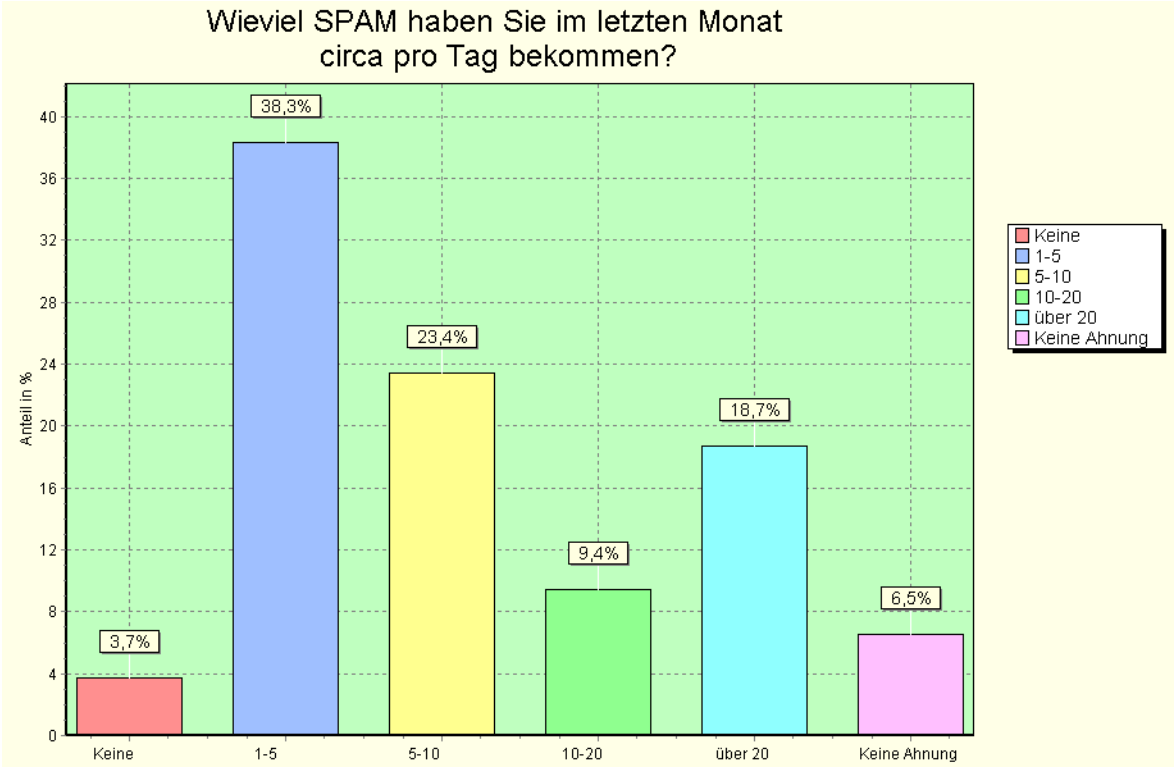

Beurteilen Sie, inwieweit Online-Banking
Ihrer Meinung nach sicher ist
Anteil in %
44
40
36
32
28
24
20
16
12
8
4
0
11,3%
41,5%
19,8%
8,5%
5,7%
3,8%
9,4%
ich habe volles
ich habe überhaupt
ich habe volles Vertrauen
ich habe überhaupt kein Vertrauen

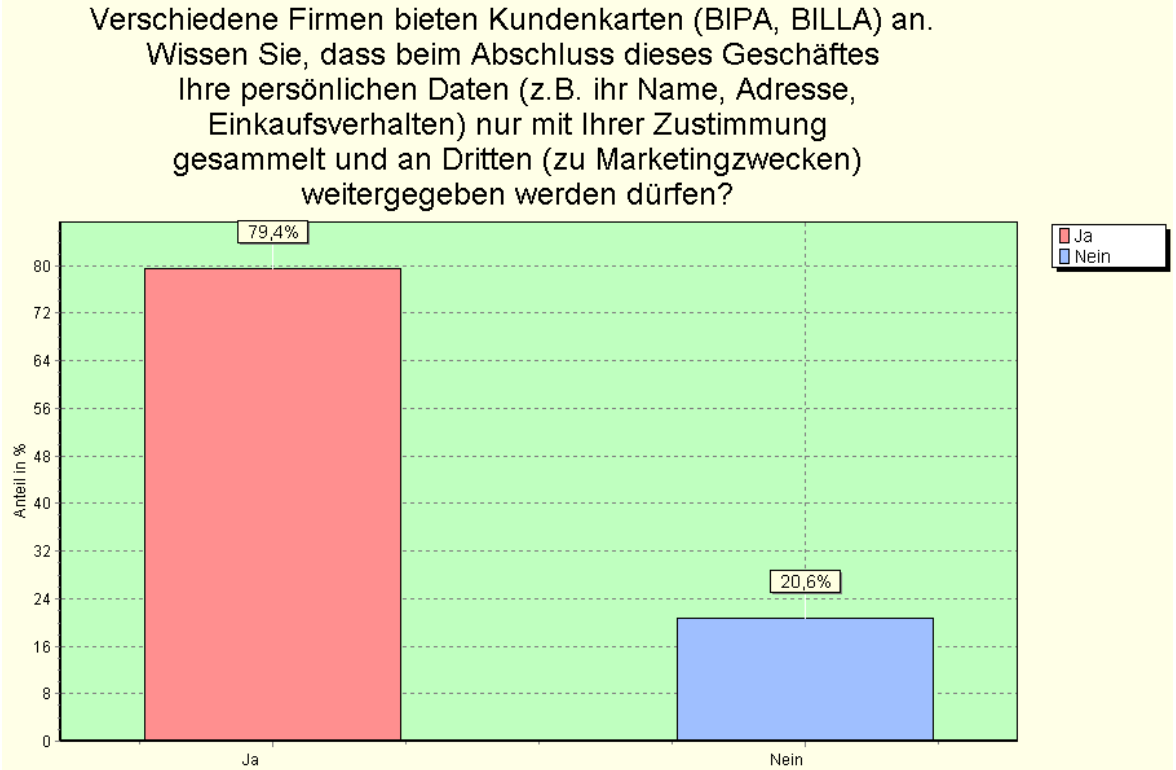

Welche der folgenden Sozialen Netze kennen Sie?
Anteil in %
97,2%
67,3%
67,3%
65,4%
1,9%
YouTube
Facebook
MySpace
StudiVZ
Ich kenne keine

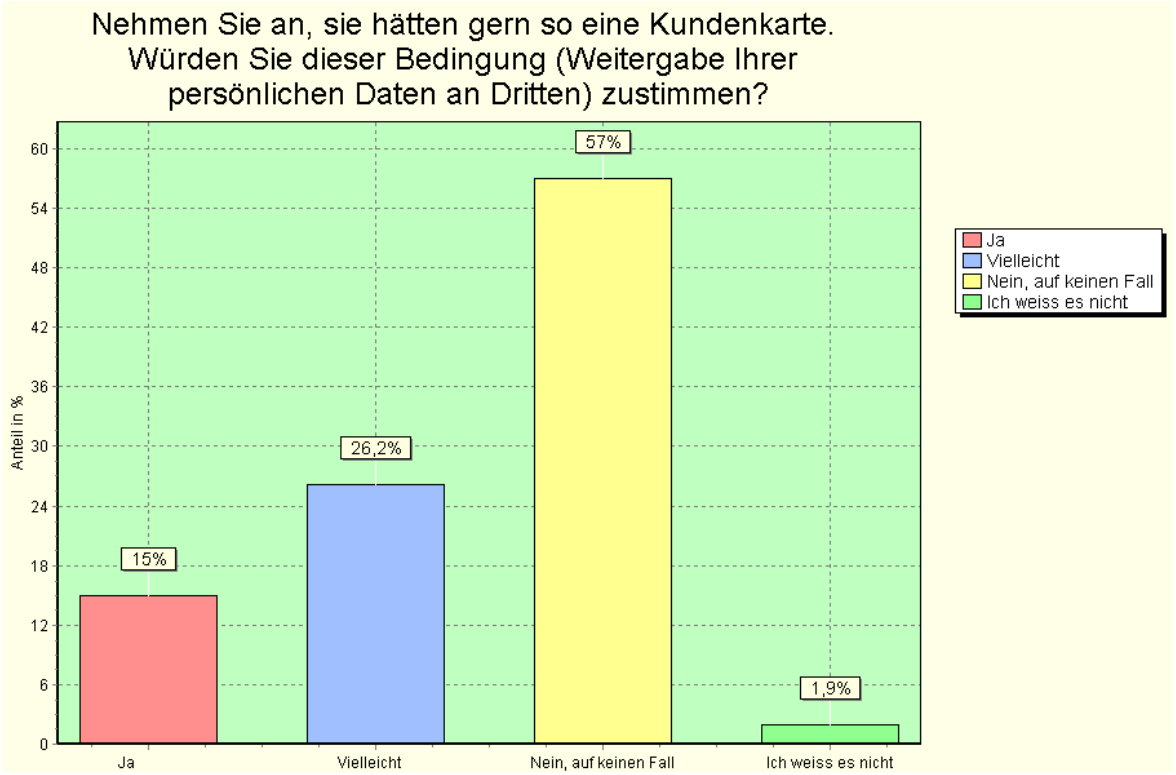

Haben Sie ein Konto bei irgendwelcher
in der vorigen Frage dargestellten Sozialen Netze?
Anteil in %
61%
39,1%
Ja
Nein

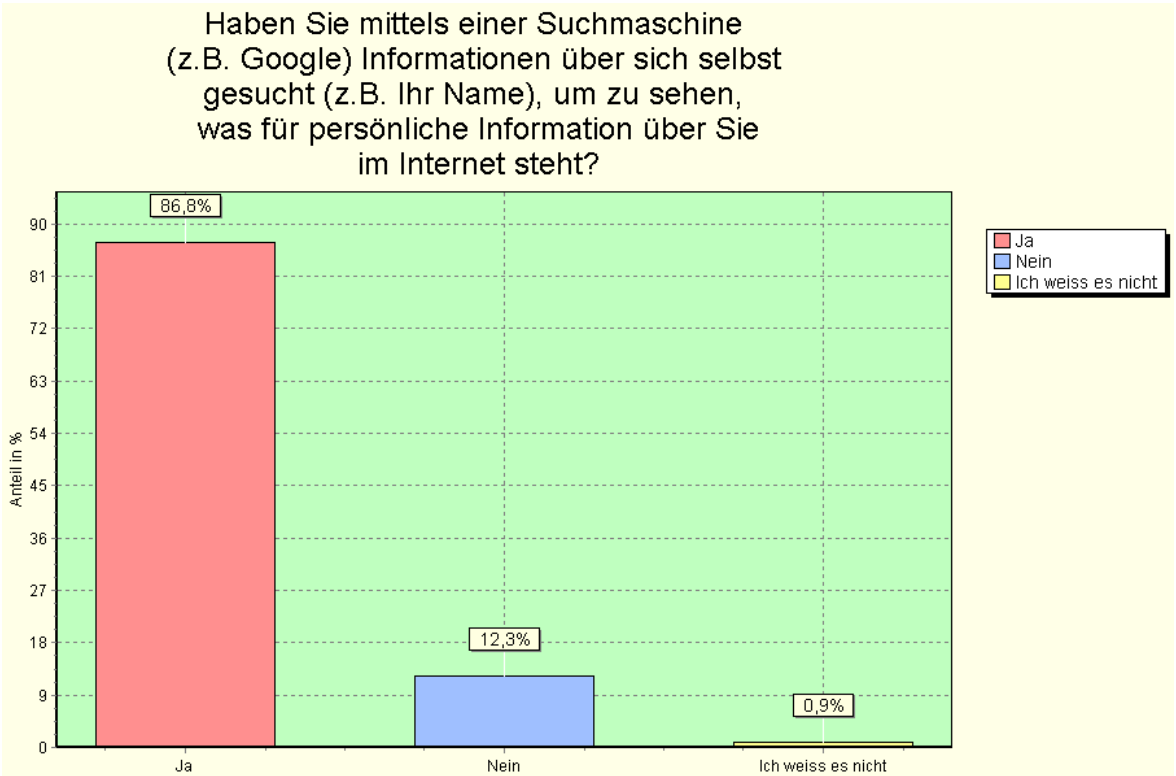

Akzeptieren Sie auch Leute, die Sie nicht kennen, als Ihre online "Freunde"?
Anteil in %
80
72
64
56
48
40
32
24
16
8
0
76,5%
11,8%
11,8%
Ja
Nein
Keine Ahnung
N [85]
Ja
Nein
Keine Ahnung

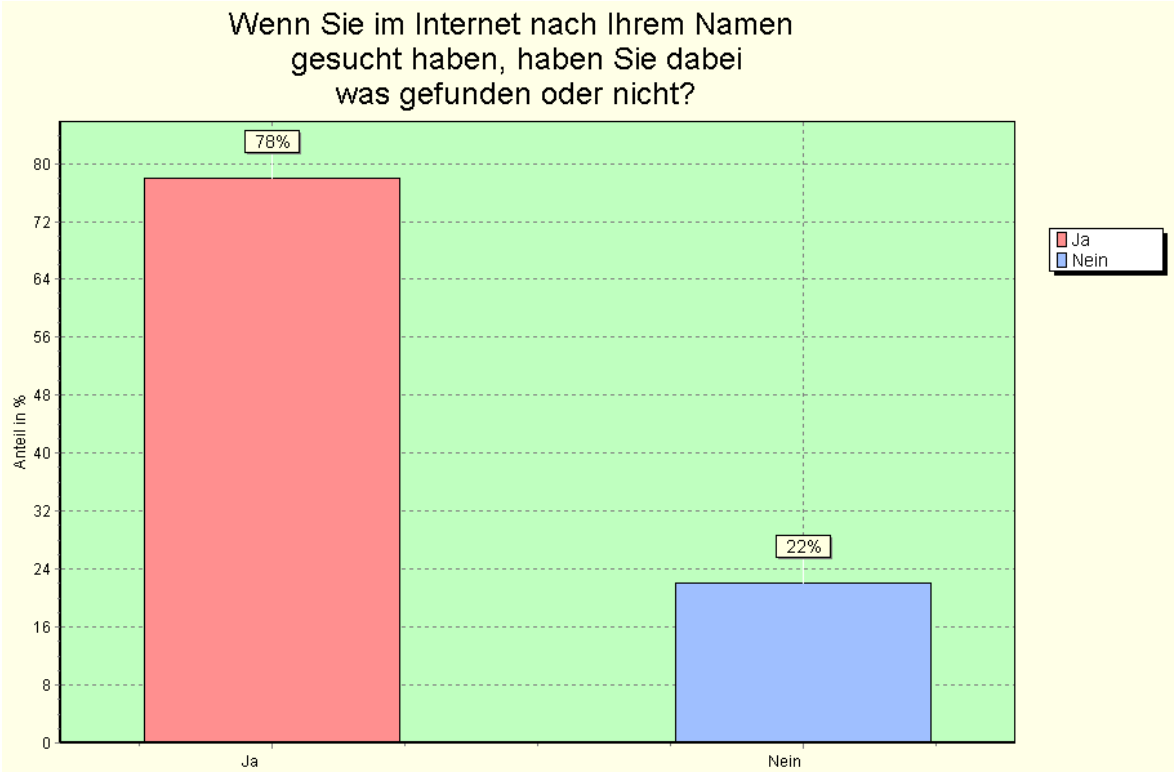

Wenn Sie Ihre persönlichen Daten bei so einer Webseite (z.B. Facebook) online hinterlassen, wer, glauben Sie, kann in Ihre private Information einsehen?
Anteil in %
55
50
45
40
35
30
25
20
15
10
5
0
54,3%
52,4%
30,5%
4,8%
1%
Nur ich
Ich und meine Freunde
Niemand
Spammer, Hacker
Ich weiss es nicht
Nur ich
Ich und meine Freunde
Niemand
Spammer, Hacker
Ich weiss es nicht

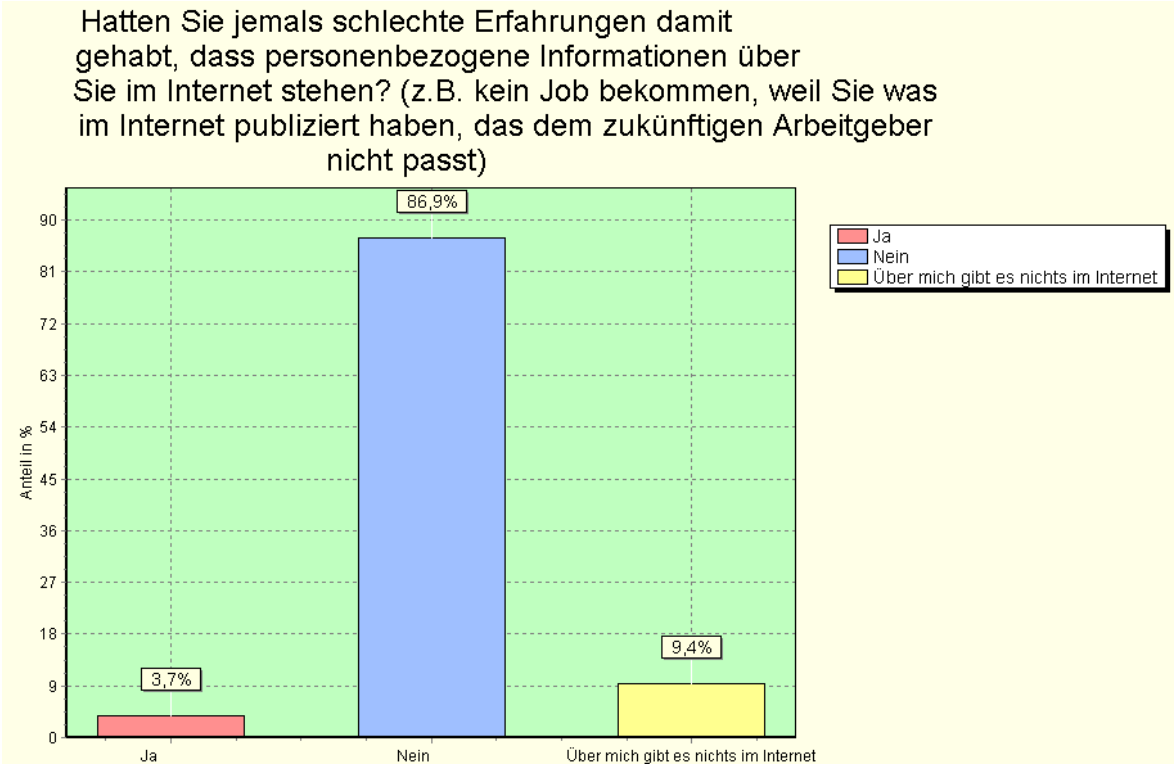

Wieviel SPAM haben Sie im letzten Monat circa pro Tag bekommen?
Anteil in %
0
4
8
12
16
20
24
28
32
36
40
38,3%
23,4%
18,7%
9,4%
6,5%
3,7%
Keine
1-5
5-10
10-20
über 20
Keine Ahnung
Keine
1-5
5-10
10-20
über 20
Keine Ahnung

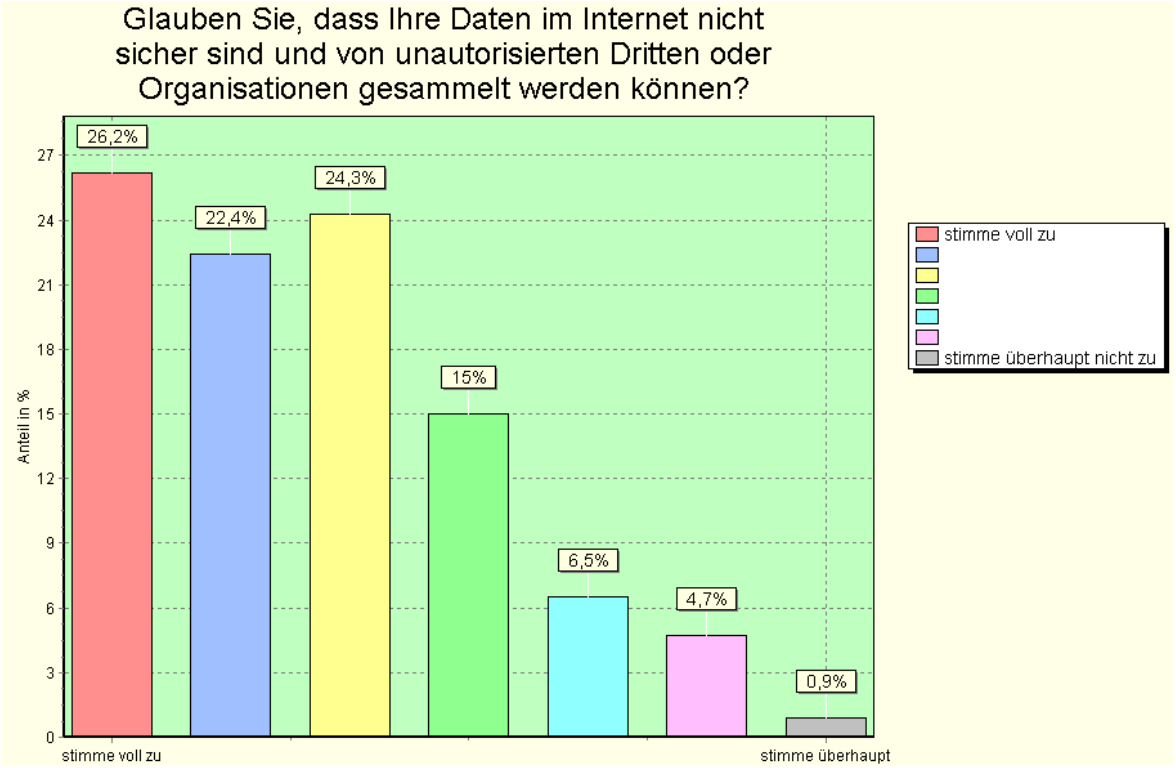

Verschiedene Firmen bieten Kundenkarten (BIPA, BILLA) an. Wissen Sie, dass beim Abschluss dieses Geschäftes Ihre persönlichen Daten (z.B. ihr Name, Adresse, Einkaufsverhalten) nur mit Ihrer Zustimmung gesammelt und an Dritten (zu Marketingzwecken) weitergegeben werden dürfen?
Anteil in %
0
8
16
24
32
40
48
56
64
72
80
79,4%
20,6%
Ja
Nein
Ja
Nein

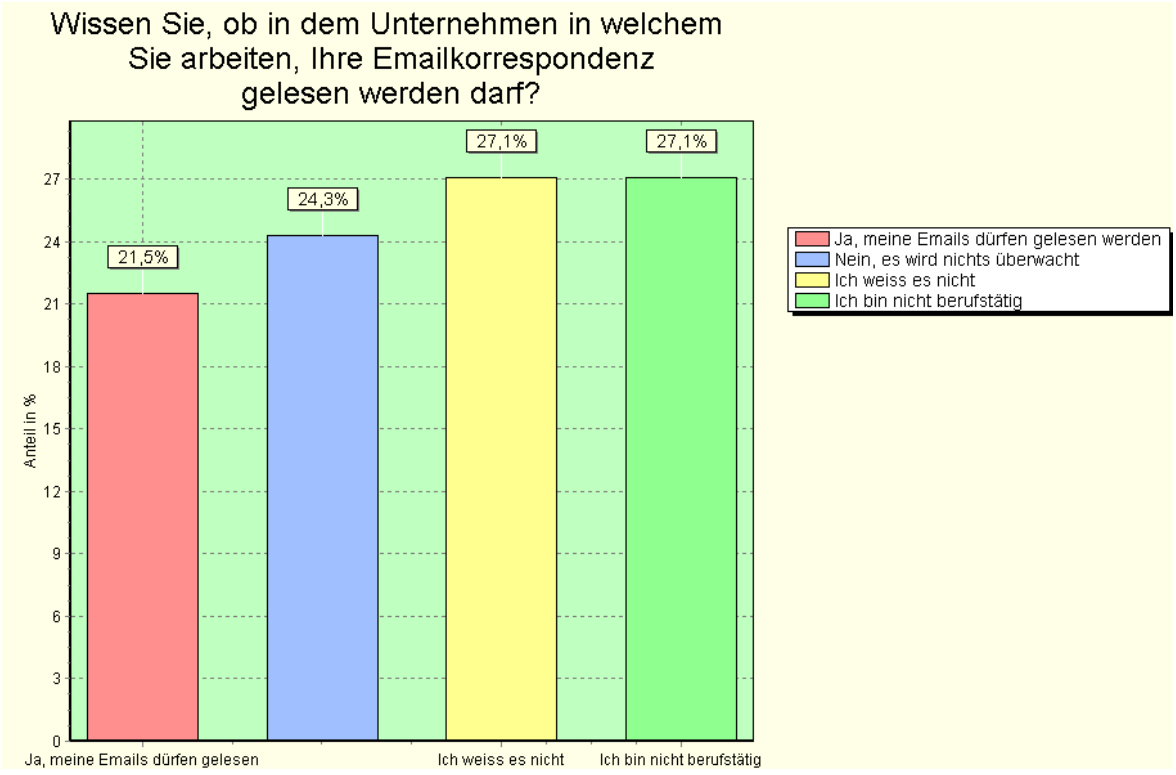

Nehmen Sie an, sie hätten gern so eine Kundenkarte. Würden Sie dieser Bedingung (Weitergabe Ihrer persönlichen Daten an Dritten) zustimmen?
Anteil in %
60
54
48
42
36
30
24
18
12
6
0
15%
26,2%
57%
1,9%
Ja
Vielleicht
Nein, auf keinen Fall
Ich weiss es nicht

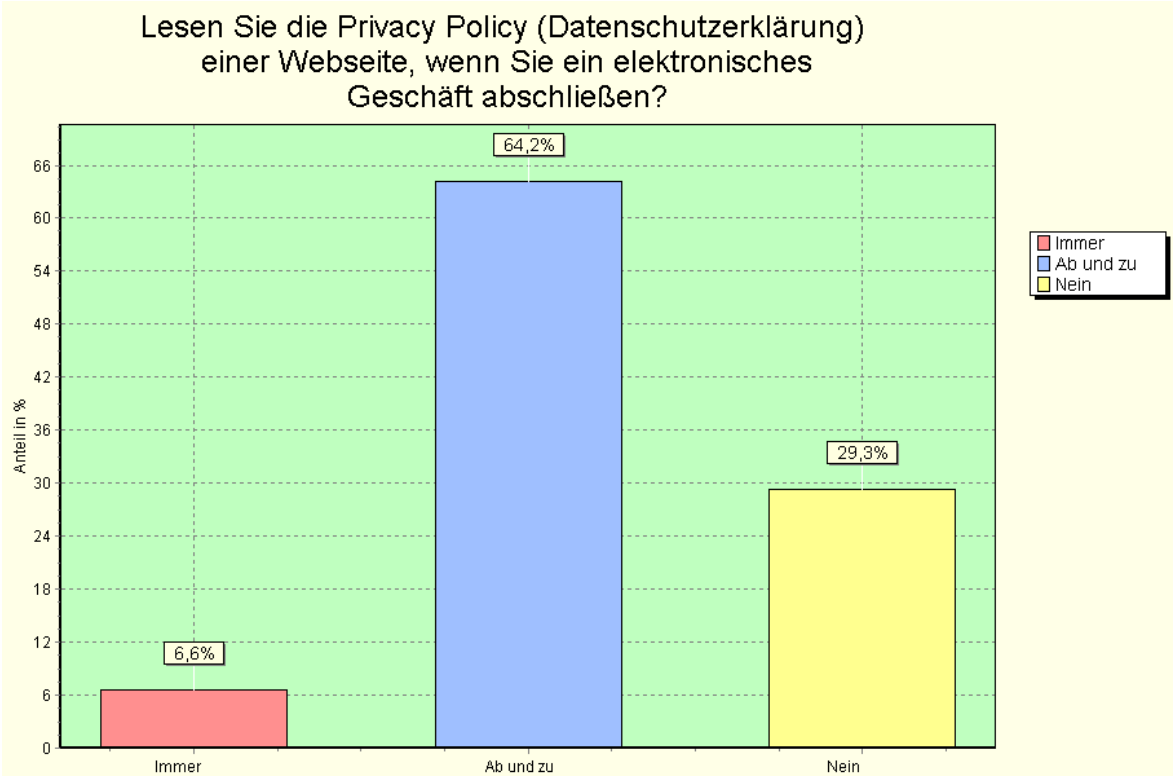

Haben Sie mittels einer Suchmaschine (z.B. Google) Informationen über sich selbst gesucht (z.B. Ihr Name), um zu sehen, was für persönliche Information über Sie im Internet steht?
Anteil in %
90
81
72
63
54
45
36
27
18
9
0
86,8%
12,3%
0,9%
Ja
Nein
Ich weiss es nicht

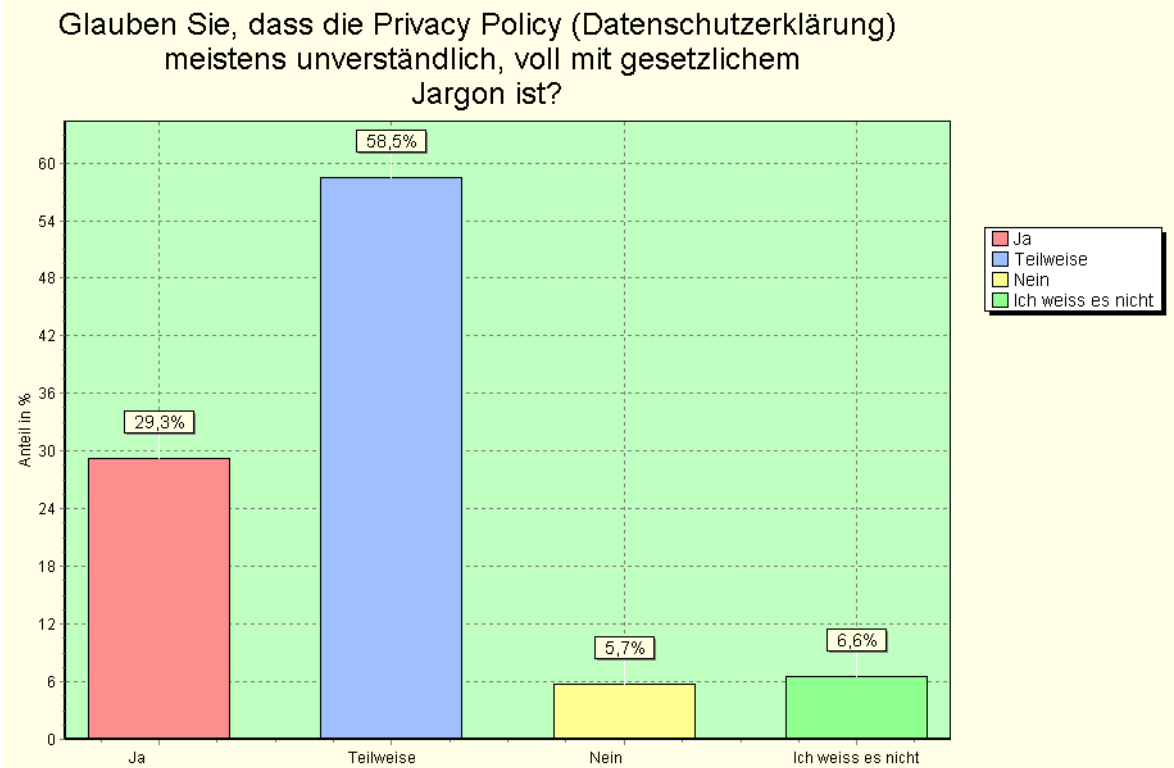

Wenn Sie im Internet nach Ihrem Namen gesucht haben, haben Sie dabei was gefunden oder nicht?
78%
22%
Anteil in %
0
8
16
24
32
40
48
56
64
72
80
Ja
Nein
Ja
Nein

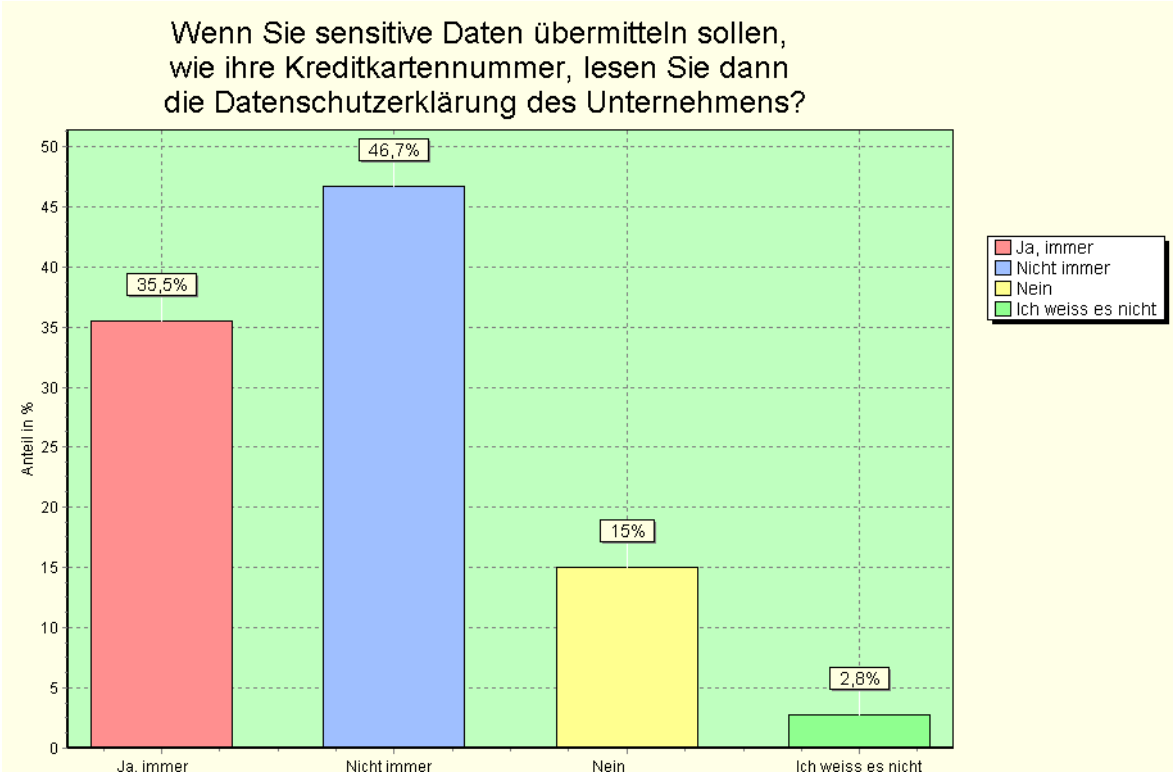

Hatten Sie jemals schlechte Erfahrungen damit gehabt, dass personenbezogene Informationen über Sie im Internet stehen? (z.B. kein Job bekommen, weil Sie was im Internet publiziert haben, das dem zukünftigen Arbeitgeber nicht passt)
86,9%
3,7%
9,4%
Anteil in %
0
9
18
27
36
45
54
63
72
81
90
Ja
Nein
Über mich gibt es nichts im Internet
Ja
Nein
Über mich gibt es nichts im Internet

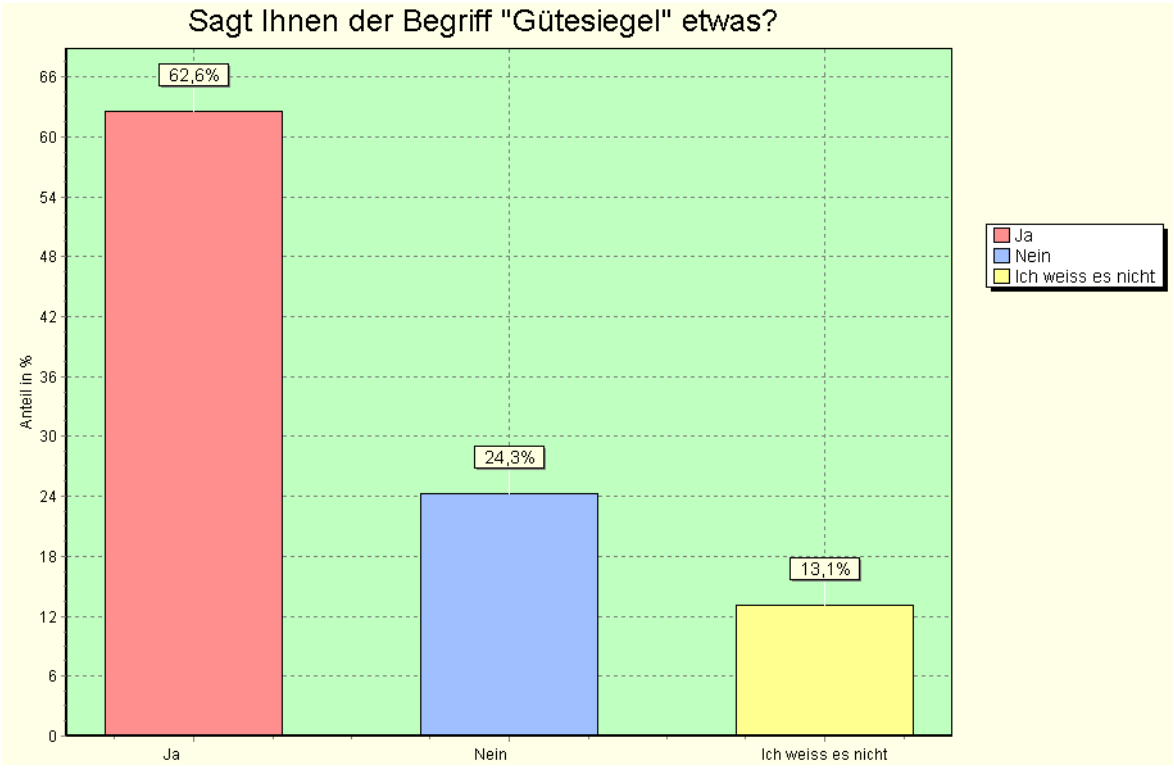

Glauben Sie, dass Ihre Daten im Internet nicht sicher sind und von unautorisierten Dritten oder Organisationen gesammelt werden können?
26,2%
22,4%
24,3%
15%
6,5%
4,7%
0,9%
Anteil in %
0
3
6
9
12
15
18
21
24
27
stimme voll zu
stimme überhaupt
stimme voll zu
stimme überhaupt nicht zu

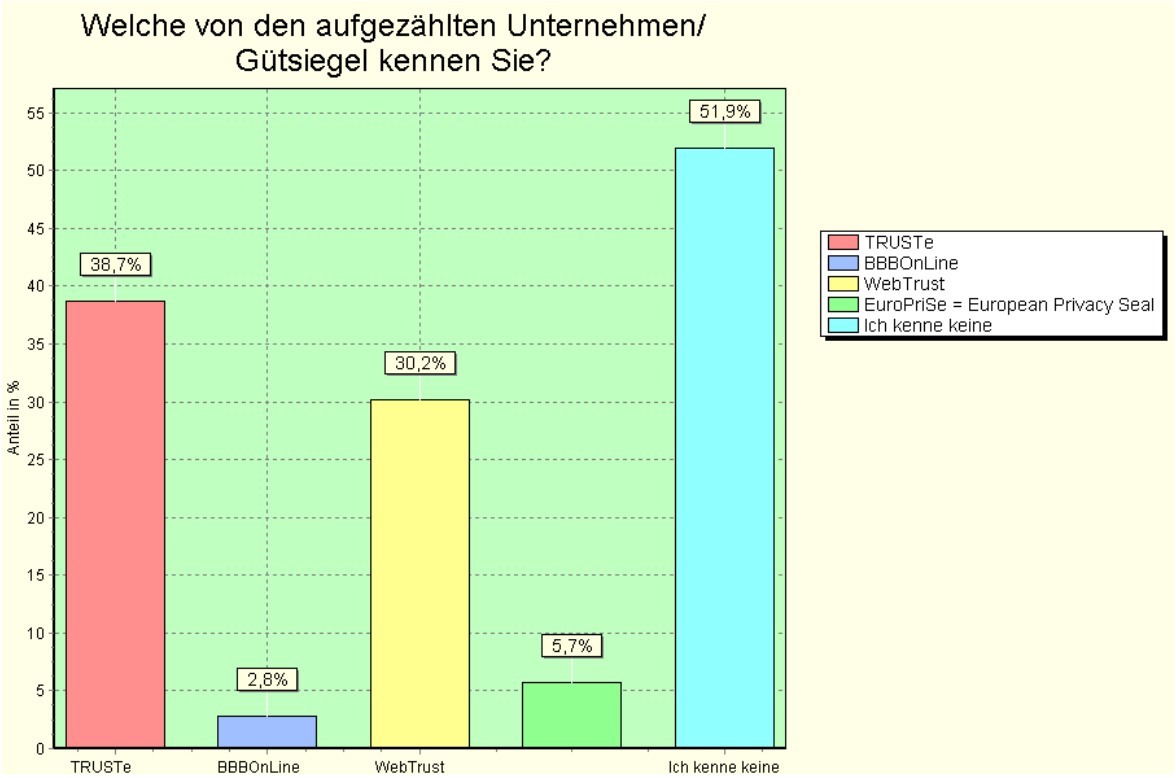

Wissen Sie, ob in dem Unternehmen in welchem Sie arbeiten, Ihre Emailkorrespondenz gelesen werden darf?
21,5%
24,3%
27,1%
27,1%
Anteil in %
0
3
6
9
12
15
18
21
24
27
Ja, meine Emails dürfen gelesen
Ich weiss es nicht
Ich bin nicht berufstätig
Ja, meine Emails dürfen gelesen werden
Nein, es wird nichts überwacht
Ich weiss es nicht
Ich bin nicht berufstätig

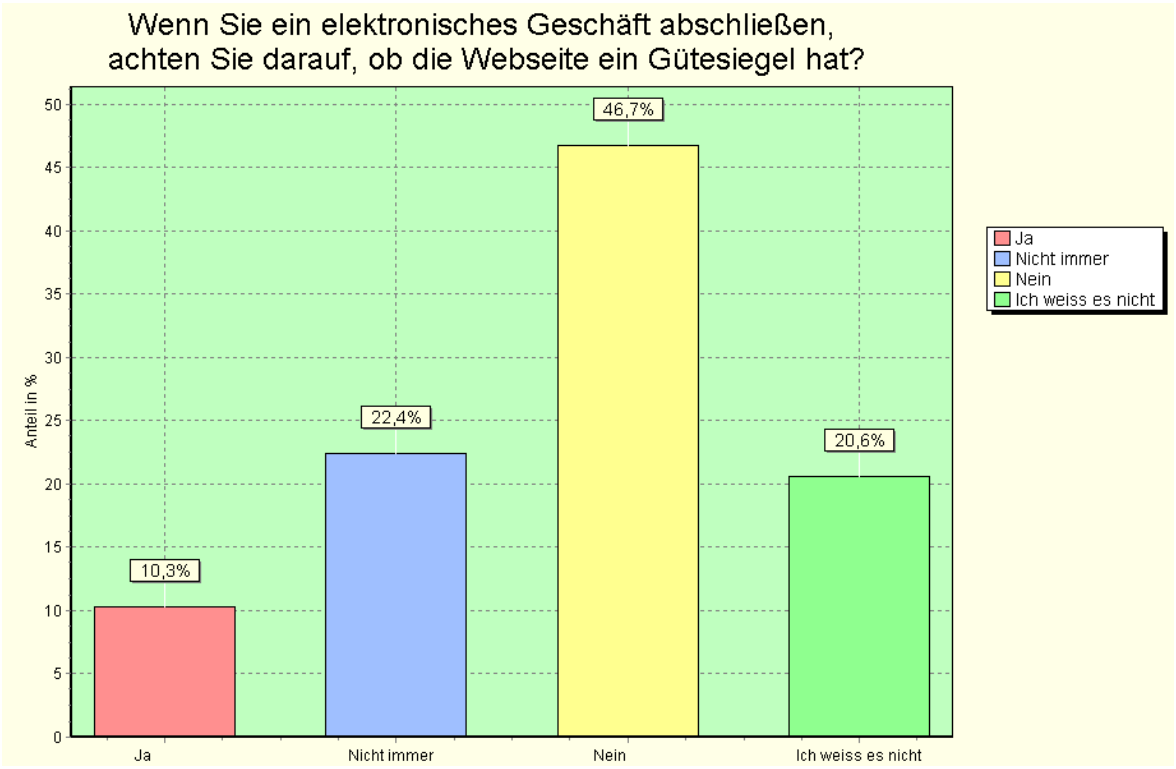

Lesen Sie die Privacy Policy (Datenschutzerklärung) einer Webseite, wenn Sie ein elektronisches Geschäft abschließen?
Anteil in %
0
6
12
18
24
30
36
42
48
54
60
66
64,2%
29,3%
6,6%
Immer
Ab und zu
Nein
Immer
Ab und zu
Nein

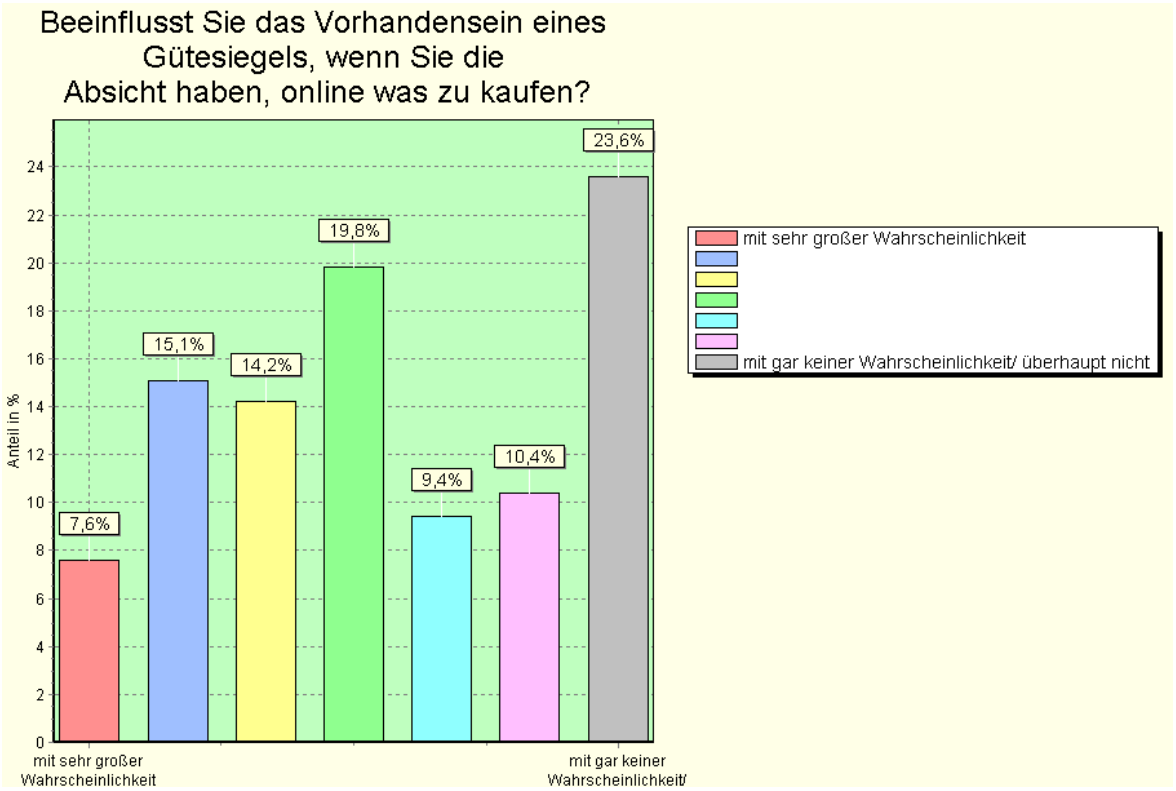

Glauben Sie, dass die Privacy Policy (Datenschutzerklärung) meistens unverständlich, voll mit gesetzlichem Jargon ist?
Anteil in %
0
6
12
18
24
30
36
42
48
54
60
58,5%
29,3%
5,7%
6,6%
Ja
Teilweise
Nein
Ich weiss es nicht
Ja
Teilweise
Nein
Ich weiss es nicht

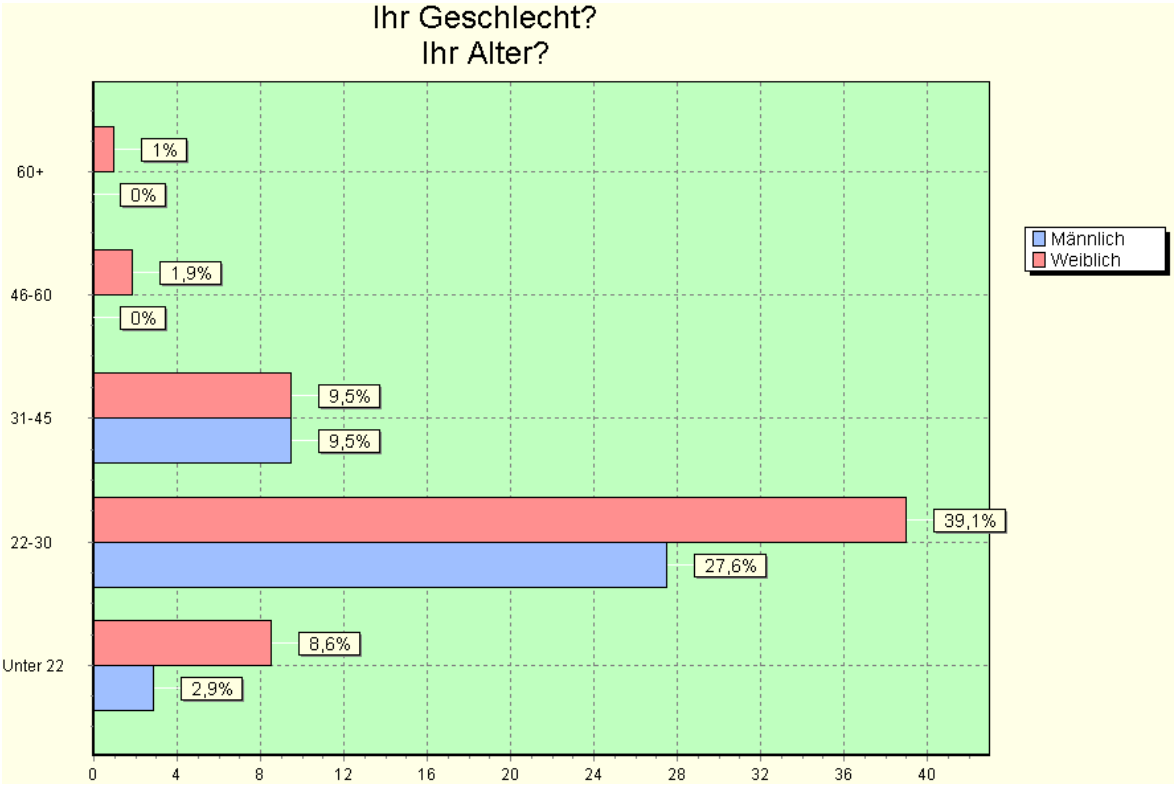

Wenn Sie sensitive Daten übermitteln sollen, wie ihre Kreditkartennummer, lesen Sie dann die Datenschutzerklärung des Unternehmens?
Anteil in %
50
45
40
35
30
25
20
15
10
5
0
46,7%
35,5%
15%
2,8%
Ja. immer
Nicht immer
Nein
Ich weiss es nicht
Ja, immer
Nicht immer
Nein
Ich weiss es nicht

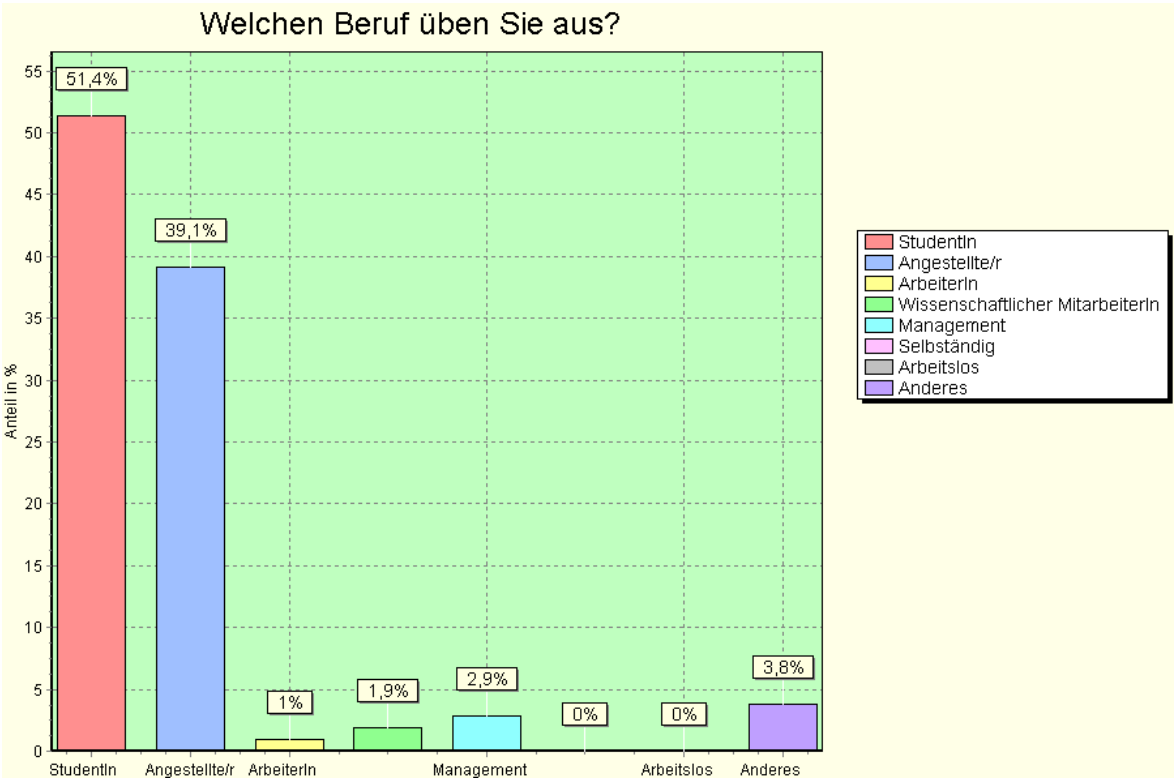

Sagt Ihnen der Begriff "Gütesiegel" etwas?
Anteil in %
66
60
54
48
42
36
30
24
18
12
6
0
62,6%
24,3%
13,1%
Ja
Nein
Ich weiss es nicht
Ja
Nein
Ich weiss es nicht


Welche von den aufgezählten Unternehmen/ Gütsiegel kennen Sie?
Anteil in %
0
5
10
15
20
25
30
35
40
45
50
55
38,7%
2,8%
30,2%
5,7%
51,9%
TRUSTe
BBBOnLine
WebTrust
Ich kenne keine
TRUSTe
BBBOnLine
WebTrust
EuroPriSe = European Privacy Seal
Ich kenne keine


Wenn Sie ein elektronisches Geschäft abschließen, achten Sie darauf, ob die Webseite ein Gütesiegel hat?
Anteil in %
0
5
10
15
20
25
30
35
40
45
50
10,3%
22,4%
46,7%
20,6%
Ja
Nicht immer
Nein
Ich weiss es nicht
Ja
Nicht immer
Nein
Ich weiss es nicht


Beeinflusst Sie das Vorhandensein eines Gütesiegels, wenn Sie die Absicht haben, online was zu kaufen?
Anteil in %
0
2
4
6
8
10
12
14
16
18
20
22
24
7,6%
15,1%
14,2%
19,8%
9,4%
10,4%
23,6%
mit sehr großer Wahrscheinlichkeit
mit gar keiner Wahrscheinlichkeit/
mit sehr großer Wahrscheinlichkeit
mit gar keiner Wahrscheinlichkeit/ überhaupt nicht


Ihr Geschlecht?
Ihr Alter?
60+
46-60
31-45
22-30
Unter 22
1%
0%
1,9%
0%
9,5%
9,5%
39,1%
27,6%
8,6%
2,9%
0
4
8
12
16
20
24
28
32
36
40
Männlich
Weiblich



Wo wohnen Sie?
Leben Sie in einer Stadt oder auf dem Lande?

	Europa	Nordamerika	Südamerika	Asien	Afrika	Australien, Neuseeland	Anteil
Eine Großstadt	69,8%	0,0%	0,0%	0,0%	0,0%	0,0%	69,8%
Eine Kleinstadt	14,2%	0,0%	0,0%	0,0%	0,0%	0,0%	14,2%
Auf dem Lande	16,0%	0,0%	0,0%	0,0%	0,0%	0,0%	16,0%
Anteil	100,0%	0,0%	0,0%	0,0%	0,0%	0,0%	100,0%

10 Literaturverzeichnis

[AG04] Acquisti, Alessandro; Grossklags, Jens (2004): *Privacy Attitudes and Privacy Behavior. Losses, Gains and Hyperbolic Discountig.* http://www.heinz.cmu.edu/~acquisti/papers/acquisti_grossklags_eis_refs.pdf, Abruf am 2008-03-10.

[AGr05] Acquisti, Alessandro; Gross, Ralph (2005): *Information Revelation and Privacy in Online Social Networks (The Facebook case).* http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf, Abruf am 2008-09-1.

[ABNT07] Annie I. Anton; Elisa Bertino; Ninghui Li and Ting Yu (2007): *A roadmap for comprehensive online privacy policy management.* In: ACM 50, 7 (Jul. 2007), p. 109 – 116.

[AckCraRea99] Ackerman, M.S., Cranor, L.F., & Reagle, J. (1999): *Privacy in e-commerce: examing user scenarios and privacy preferences.* In: Proceedings of the 1st ACM conference on electronic commerce (pp. 1-8) New York: ACM.

[AdTu05] Adomavicius, D.; Tuzhilin, A (2005): Personalization Technologies: A Process-Oriented Perspective. In: CACM 48, 10.

[ARGE08a] ARGE DATEN: Österreichische Gesellschaft für Datenschutz (2008): *Veröffentlichte Daten begünstigen Datenschutz – Missbrauch.* http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=78208nhz, Abruf am 2007-10-17.

[ARGE08b] ARGE DATEN (2008): *Vorratsdatenspeicherung – eine sicherheitspolitische Sackgasse.* http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=28764tot, Abruf am 2008-06-04.

[ARGE08c] ARGE DATEN (2008): *Safer Internet Day 2008. Selbstbeweihräucherung2.0.*
http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=89650her, Abruf am 2008-02-11.

[ARGE08d] ARGE DATEN (2008): *EG-Richtlinie 2006/24/EG – Vorratsdatenspeicherung von EU beschlossen.*
http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=11563vpp, Abruf am 2008-02-11.

[APS] Ashley, Paul; Powers, Calvin; Shunter, Matthias (o.J.): *From Privacy Promises to Privacy Management. A new Approach for Enforcing Privacy Throughout an Enterprise.*
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.3186, Abruf am 2008-04-09.

[BaerRud02] Baeriswyl, Bruno; Rudin, Beat (2002): *Perspektive Datenschutz. Praxis und Entwicklungen in Recht und Technik.* Verlag Österreich GmbH, Wien.

[Bäu00] Bäumler, H. (Hrsg.): *E-Privacy*, Vieweg Verlag, 2000.

[Ben99] Bennassi, P. (1999): TRUSTe: an online privacy seal program. In: ACM 42, 2, pp.56-59.

[Bloom02] Bloomfield, Dean (2002): *P3P- Making Your Site Compliant.* 31.Januar 2002.
http://evolt.org/node/20756/, Abruf am 2008-07-07.

[Borking98] Borking, J.: *2008 – Ende der Privatheit?* In. Bäumler, H. Hrsg., 1998, *Der neue Datenschutz*, 283-293.

[Braun00b] Braun, Tilman. NETHICS. Portal zur Informationsethik (2000): *Privacy gefährdete Tendenzen.*
http://www.nethics.net/nethics/de/themen/privacy/tendenzen.html, Abruf am 2008-01-07.

[Braun00c] NETHICS. Portal zur Informationsethik (2000): *Wirtschaftliche Selbstregulierung.*
http://www.nethics.net/nethics/de/themen/privacy/selbstregulierung_wirtschaft.htm, Abruf am 2008-01-07.

[Braun00d] Braun, Tilman (2000): *Begriffserläuterung, Definition und wirtschaftliche Rezeption.* NETHICS Portal zur Informationsethik. http://www.nethics.net/nethics/de/themen/privacy/begriffserlaeuterung.html, Abruf am 2008-01-07.

[Buck03] Bucksteeg, Andreas (2003): Methoden und Technicken zur Sicherstellung des vertrauenswürdigen Managements von Benutzerprofildaten in vernetzten Anwendungen. Diplomarbeit. Technische Universität München. Fakultät für Informatik. Lehrstuhl XIX. Software Engineering betrieblicher Informationssysteme.

[CAG05] Cranor, Lorrie Faith; Arjula, Manjula; Guduru, Praveen (2005): *User Interfaces for Privacy Agents.* Draft by AT&T. 14.Juli 2005. http://lorrie.cranor.org/pubs/privacy-bird-20050714.pdf, Abruf am 2008-07-03.

[CaPeJo00] Cas, Jochan; Peissl, Walter und Jochims, Telse (2000): Beeinträchtigung der Privatsphäre in Österreich. Datensammlungen über Österreicher und Österreicherinnen. Bestandsaufnahme. Wien, 1.Teil.

[CaPe02] Cas, Jochan; Peissl, Walter (2002): *Datenvermeidung in der Praxis. Individuelle und gesellschaftliche Verantwortung. Endbericht.* ITA-Institut für Technikfolgen-Abschätzung der österreichischen Akademie der Wissenschaften. Wien, September 2002.
http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a29.pdf, Abruf am 2008-05-07.

[Cio07] Corey A., Ciocchett (2007): *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors.* In: American Business Law Journal. Austin: Spring 2007. Vol. 44, Iss. 1; pp. 55-72.

[CM07] Castaneda, Alberto J.; Montoro, Francisco J. (2007): *The effect of Internet general privacy concern on customer behavior.* In: Electronic Commerce Research, 7/2, Juni 2007, S.117-141.

[Comp08] *Datenschutz: Google will YouTube-Daten anonymisieren.* http://www.computerbild.de/artikel/cb-Aktuell-Internet-Google-will-YouTube-Daten-anonymisieren_3093716.html/, Abruf am 2008-07-16.

[Cla99] Clarke, R. (1999): *Internet Privacy Concern Confirm the Case for Intervention.* In: Communications of the ACM, Vol. 42, No. 2, Feb. 1999, S. 60-67.

[Cra99] Cranor, L. F.: Agents of Choice (1999): *Tools that Facilitate Notice and Choice about Web Site Data Practices.* In: Proc. 21 st Intl. Conf. On Privacy and Personal Data Protection, Hong Kong, China, Sept. 1999.

[Dohr96] Dohr, Walter (1996): Das Österreichische Datenschutzgesetz. In: Fleissner, Peter; Choc, Marce (1996): Datensicherheit und Datenschutz. Technische und rechtliche Perspektive. Innsbruck-Wien.

[DSG00] Datenschutzgesez 2000. Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 –DSG 2000).
http://www.dsk.gv.at, Abruf am 2007-09-25.

[Eco07] Economic and Social Research Council (2007): *Internet Users give up their Privacy in Exchange for trust.* 22. November 2007.
http://www.egovmonitor.com/node/, Abruf am 2008-04-17.

[Eggen05] Eggendorfer, Tobias (2005): *No Spam! Besser vorbeugen als heilen.* Software&Support Verlag GmbH, Frankfurt.

[Egg93] Egger, Edeltraud (1993): *Considering Privacy-Aspects in Designing CSCW-Applications.* In: NetWORKing: Connecting Workers In and Between Organizations, Proceedings of the IFIP WG9.1 Working Conference on NetWORKing, Vienna, Austria, June 16-18 (edited by Clement, A.; Kolm, P.; Wagner, I.); North-Holland; pp. 133–141.

[Egg90] Egger, Edeltraud (1990): Datenschutz versus Informationsfreiheit- Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien. In: Schriftenreihe der Österreichischen Computer Gesellschaft, Band 52, Wien und München: OCG, Oldenbourg.

[EPIC08] Electronic Privacy Information Center (2008):
http://epic.org/, Abruf am 2008-02-07.

[EPIC08a] Electronic Privacy Information Center (2008): *First European Union Privacy Seal Awarded to Search Company.*
http//epic.org/, Abruf am 2008-07-16.

[Fin06] Finder, Alan: For Some, Online Persona Undermines a Resume. In: The New York Times. 11. Juni 2006.
http://www.nytimes.com/2006/06/11/us/11recruit.html, Abruf am 2008-09-22.

[FCho96] Fleissner, Peter; Choc, Marce (1996): Datensicherheit und Datenschutz.Technische und rechtliche Perspektive. Innsbruck-Wien.

[Fischer01] Fischer-Hübner, Simone (2001): IT-Security and Privacy Design and Use of Privacy-Enhancing Security Mechanism. Springer Verlag Berlin Heidelberg New York.

[FHW01] Fuhrberg, Kai; Häger, Dirk; Wolf, Stefan (2001): *Internet – Sicherheit.* Auflage 3, Hanser Fachbuch Verlag.

[For01] Forrester Research: *Surviving the Privacy Revolution.* Report, Feb. 2001.

[Garstka] Garstka, Hansürgen (o.J.): *Informationelle Selbstbestimmung und Datenschutz.*
http://www.bpb.de/files/YRPN3Y.pdf, Abruf am 2008-02-21.

[GaSp02] Garfinkel, Simson and Spafford, Gene (2002): *Web Security, Privacy and Commerce.* O'Reilly, Second Edition.

[Gartner04] Gartner Group. Gartner study finds significant increase in e-mail phishing attacks (Apr. 2004). www.gartner.com/5_about/press_releases/asset_71087_11.jsp, Abruf am 2008-09-23.

[GCH07] Goodman, Joshua; Cormack, Gordon V. and Heckerman, David: *Spam and the Ongoing Battle for the Inbox.* In: Communications of the ACM, Feb2007, Vol. 50 Issue 2, p25-31, 8p.

[Geis97] Geis, Ivo (1997): *Internet und Datenschutzrecht.* In: Neue Juristische Wochenschrift, 50. Jg. (1997), Heft 5, S. 288-293.

[GolLe01] Goldfeder, A. and Leibfried, L.: *Privacy in Internet Explorer 6.* MSDN Liabrary, Oktober 2001.

[GLN00] Grimm, Rüdiger; Löhndorf, Nils; Rossnagel, Alexander (2000): *E-Commerce meets E-Privacy.* In Bäumler, H. (Hrsg.): E-Privacy, Wiesbaden, 2000. http://www.u7ni-kassel.de/fb7/oeff_recht/publikationen/pubOrdner/Dasit_Kiel.pdf, Abruf am 2008-03-28.

[Gri04] Gritzalis, Stefanos (2004): *Enhancing Web Privacy and anonymity in the digital ara.* In: Information Management & Computer Security; 12, 2/3; p.255.

[Grill06] Grill, Franz Hermann (2006): *Software Tools for Website Personalization in E-Commerce Application. A Review of Commercial Products.* Diplomarbeit, Institut für Wirtschaftsinformatik, Wirtschaftsunivesität Wien.

[Hab89] Habermas, J. (1989): *The structural transformation of the public sphere: an inquiry into a category of bourgeois society.* Cambridge: MIT (translated by T. Burger).

[HaHuLeePng03] Hann, Il-Horn; Hui, Kai-Lung; Lee, Tom S, and Png, I.P.L (2003): *The Value of Information Privacy: An Empirical Investigation.* AEI- Brookings Joint Center for Regulatory Studies. Oktober 2003.
http://aei-brookings.org/admin/authorpdfs/redirect-safely.php?fname=../pdffiles/php2b.pdf, Abruf am 2008-03-28.

[Him04] Himberger, Simon (2004): *Fernmeldegeheimnis und Überwachung. Schutzbereiche und Eingriffe. Durchführung und Kosten.* Wien Graz 2004.

[HaLaLePNG06] Hann, Il-Horn; Hui, Kai-Lung; Lee, Yee-Lin Lai; S.Y.T. and PNG, I.P.L. (2006): *Who gets spammed?* In: Communications of the ACM, Oktober 2006, Vol.49 Issue 10, p.83-87.

[Hof02] Hofer, Marcus (2002): Datenschutz@Internet. *Die Privatsphäre im Informationszeitalter.* Wien, Graz.

[InternetRecht06a] Internet & Recht (2008): *Datenschutz im Internet.*
http://www.internet4jurists.at/intern27a.htm, Abruf am 2008-06-06.

[InternetRecht06b] Internet&Recht (2008): *Die österreichische Rechtslage zur E-Mail Werbung.*
http://www.internet4jurists.at/e-mail/oe1a.htm, Abruf am 2008-02-05.

[ITA08] ITA. Institut für Technologen-Abschätzung. Wien. *EuroPriSe-European Privacy Seal.* Juni 2007- November 2008.
http://www.oeaw.ac.at/ita/ebene4/d2-2a49.htm, Abruf am 2008-07-05.

[IWG08] International Working Group on Data Protection in Telecommunications (2008): *Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum".* 43. Sitzung, 3-4. März 2008 (Italien).
http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf?1208956853, Abruf am 2008-10-04.

[JaJoNat07] Jagatic, Tom N.; Johnson, Nathaniel A.; Menczer, Filippo (2007): *Social Phishing.* In: ACM, Vol. 50, No. 10, pp. 96-100. Oktober 2007.

[Ja04] Jahnel, Dietmar (2004): Datenschutzrecht in der Praxis. Grundbegriffe, Zulässigkeit, Meldepflicht, Datensicherung, Rechtsschutz und Spamming. Dbv- Verlag Graz, Wien.

[Jak05] Jakobsson, M; Myers, S. (2004): Modeling and preventing phishing attacks. In: Phishing Panel at Financial Cryptography. Feb. 2005.

[JAP01] JAP – Anonymity and Privacy: *Datenschutzeinstellungen im Internet Explorer 6.0.*
http://anon.inf.tu-dresden.de/, Abruf am 2008-07-02.

[Ka04] Kahlert, Henning (2004): *Als Big Brother noch keine Fernsehsendung war. Entwicklung des Datenschutzes.*
http://www.forum-recht-online.de/2004/304/304kahlert.pdf, Abruf am 2007-11-02.

[Kob07] Kobsa, Alfred (2007): *Privacy – enhanced personalization.* In: Commun. ACM 50, 8 (Aug. 2007), p. 24 –33.

[Kob07b] Kobsa, Alfred (2007): *A Privacy-enhanced personalization.* In: The Adaptive Web: *Methods and Strategies of Web Personalization.* P. Brusilovsky, A. Kobsa, and W. Nejdl, eds. Springer Verlag, 2007, 628-670; doi 10.1007/978-3-540-72079-9_21.

[KOM04] Kommission der Europäischen Gemeinschaft. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. *Über unerbetete Werbenachrichten (Spam).* 22 Januar 2004.

[Kuhl04] Kuhlen, Rainer (2004): Informationsethik. Ethik in elektronischen Räumen (Kapitel 6: Privacy in elektronischen Räumen- informationelle Selbstbestimmung, informationelle Autonomie. UTB, 2004.

[Lang02] Langheinrich, Marc (2002): P3P- ein neuer Standard für Datenschutz im Internet. ETH Zürich. Institut für Informationssysteme.
http://vs.inf.ethz.ch/res/papers/p3p-digma.ps, Abruf am 2008-07-25.

[Lang04] Langheinrich, Marc (2004): Die Privatsphäre in Ubiquitous Computing – Datenschutzaspekte der RFID –Technologie. Institut für Pervasive Computing, ETH Zürich.

[Lange05] Lange, Jörg Andreas (2005): Sicherheit und Datenschutz als notwendige Eigenschaften von computergestützten Informationssystemen. Ein integrierender Gestaltungsansatz für vertrauenswürdige computergestützte Informationssysteme. Deutscher Universitäts-Verlag/GWV Fachverlage GmbH, Wiesbaden 2005.

[Lau03] Lauren, C. (2003): *Privacy and Human Rights 2003. Privacy International,* London, UK.
http://www.privacyinternational.org/survey/phr2003, Abruf am 2008-03-17.

[Les01] Lester, T. (2001): The Reinvention of Privacy. The Atlantic Monthly, Mar. 2001.
http://www.theatlantic.com/issues/2001/03/lester-p1.htm, Abruf am 2008-01-10.

[Lind08] Lindau, Edmund E. (2008): *Unerwünschte E-Mails können sehr teuer werden.* In: Computerwelt.
http://www.computerwelt.at/detailArticle.asp?a=113869&n=1, Abruf am 2008-02-13.

[Mähr99] Mähr, Stefan (1999): Aktuelle Verbraucherprobleme beim Schutz personenbezogener Daten. Diplomarbeit der Wirtschaftsuniversität Wien.

[MaLa01] Mattern, Friedemann; Langheinrich, Marc: Allgegenwärtigkeit des Computers –Datenschutz in einer Welt intelligenter Alltagsdinge.
http://www.vs.inf.ethz.ch/res/papers/allgegenwaertig.pdf, Abruf am 2007-10-15.

[Matt08] Mattern, Friedemann: *Suchmaschinen - eine kurze Einführung.* In: Wie arbeiten die Suchmaschinen von morgen. acatec – Deutsche Akademie der Technikwissenschaften, Frauenhofer IRB Verlag, 2008.
http://intern.acatech.de/public_download.php?PHPSESSID=4922e089ae94aa928c6c3903ec4f6c0e&fileid=631&type=news, Abruf am 2008-07-17.

[MB06] Mayer-Schönberger, Viktor; Brandl, Ernst O. (2006): Datenschutzgesetz. Grundsätze und europarechtliche Rahmenbedingungen.Gesetztext mit Materialien.Datenschutz-Verordnungen und Richtlinien im Anhnang. Linde Verlag Wien Ges.m.b.H., Wien.

[McBurPar03] McBurney, P., & Parsons, S. (2003): Posit spaces: a performative model of e-commerce. In: Proceedings of the second international joint conference on autonomous agents and multiagent systems (pp. 624-631). New York: ACM.

[Mey02] Meyer, Bhakti (2002): P3P und dessen Erweiterungsmöglichkeiten - Abgleich von Datenschutzpraktiken/ -präfernezen am Beispiel des Lufthansa AG Intranets. Diplomarbeit. Johann Wolfgang Goethe-Universität. Fachbereich Informatik. Frankfurt am Main.

[Moor97] Moor, J.H. (1997): Towards a theory of privacy in the information age. In: ACM SIGCAS Computer and Society, 27(3), 27-32.

[MR01] Müller, Günther, Reichenbach, Martin (2001): *Sicherheitskonzepte für das Internet.* Springer Verlag Berlin Heidelberg 2001.

[Moor97] Moor, J.H. (1997): *Towards a theory of privacy in the information age.* In ACM SIGCAS Computers and Society, 27(3), 27-32.

[Murr07] Murray, Ben (2007): *Electronic Privacy is Age dependent.* In: Strategic Communication Management; Aug/Sep 2007; 11, 5; p.9.

[Neh07] Nehf, James P. (2007): *Shopping for Privacy on the Internet.* In: The Journal of Consumer Affairs, 41, 2, Winter 2007, p.351-375.

[Nethics00a] NETHICS. Portal zur Informationsethik (2000): *Privacy – infomationelle Privatsphäre.*
http://www.nethics.net/nethics/de/themen/privacy.html, Abruf am 2007-11-05.

[OECD80] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980.*

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_37441,00.html, Abruf am 2008-07-05.

[ORF08] Online-Medien: *Google liest mit.* 11 Juni 2008. http://futurezone.orf.at/it/stories/284580/, Abruf am 2008-07-17.

[Pat01] Patalong, Frank: *Großer, dummer Bruder.* In: SpiegelOnline 2001. https://www.spiegel.de/netzwelt/tech/0,1518,169697,00.html, Abruf am 2008-02-27.

[Pat08] Patalong, Frank: *Invasion der Freiheitsfresser.* In: SpiegelOnline. http://www.spiegel.de/netzwelt/web/0,1518,529413-2,00.html, Abruf am 2008-02-19.

[Petri] Petri,Thomas Bernhard (0.J.): Kommerzielle Datenverarbeitung und Datenschutz im Internet. Lässt sich der internationale Datenhandel im Netz noch kontrollieren? http://www.bpb.de/files/VC62V.pdf, Abruf am 2008-02-04.

[Peissl02] Peissl, Walter (2002): Privacy. Ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte. ITA-Institut für Technikfolgen-Abschätzung der österreichischen Akademie der Wissenschaften. http://www.austriaca.at/3232-8a, Abruf am 2008-04-09.

[Pilz01] Pilzweger, Markus (2001): *Toysmart soll 250.000 Kundendaten löschen.* In: PC.Welt. http://www.pcwelt.de/start/computer/archiv/10455/toysmart_soll_250000_kundendaten_loeschen/, Abfrage am 2008-04-11.

[Plaß05] Plaß, Christine (2005): *Das große Vergessen. Datenschwund im digitalen Zeitalter.* In Lehman, Kai/ Schetsche, Michael (Hrsg.): *Die Google Gesellschaft. Vom digitalen Wandel des Wissens.* Bielefeld: transcript, 2005, S.41-46.

[PlöDuHel02] Plöckinger; Duursma; Helm Hrsg. (2002): *Aktuelle Entwicklungen im Internet-Recht. Beiträge zur zivil-, straf- und verwaltungäsrechtlichen Diskussion.* Wien 2002.

[Privacy08] Privacy International (2008): http://www.privacyinternational.org/, Abruf am 2008-02-07.

[POWZu06] Parschalk, Martin; Otto, Gerald; Weber, Jan; Zuser, Alexander (2006): *Telekommunikationsrecht.* Linde Verlag Wien.

[PZ06] Pan, Jue and Zinkhan, George M. (2006): *Exploring the impact of online privacy disclosures on consumer trust.* In: Journal of Retailing, Sep2006, Vol.82, Issue 4, ps. 331-338.

[Reichmann] Reichmann, Gerhard (o.J.): *Schutz von Daten und Schutz von Wissen in der Informationsgesellschaft.* http://www.kfunigraz.ac.at/iwiwww/publ/reichmann_4.pdf, Abruf am 2008-03-12.

[Rosen92] Rosenberg, R. (1992): *The Social Impact of Computers.* In: Academic Press.

[RosenD07] Rosenblum, David (2007): What anyone can know? The privacy risks of social networking sites. In: IEEE Computer Society, S. 40-49. Mai/Juni 2007.

[Ross07] Rossnagel, Alexander (2007): Personalisierung in der E-Welt. Aus dem Blickwinkel der informationellen Selbstbestimmung gesehen. In: Wirtschaftsinformatik, Volume 49, Nummer 1, Februar 2007, S. 8-15. http://www.springerlink.com/content/k102451145438962/fulltext.pdf, Abruf am 2008-03-20.

[RP08] *Google muss YouTube-Nutzerdaten weitergeben.* http://www.rp-online.de/public/article/digitale/internet/586386/Google-muss-Nutzerdaten-weitergeben.html, Abruf am 2008-09-1.

[Sack07] Sackmann, Stefan (2007): *Privacy im World Wide Web.* In Wirtschaftsinformatik, Volume 49, Nummer 1, Februar 2007, S.49-54.

http://www.springerlink.com/content/r587046n7947147k/fulltext.pdf, Abruf am 2008-03-20.

[Sax83] Saxonhouse, A. W. (1983): *Classical greek conceptions of public and private.* In: Public and private in social life (pp. 363-384). New York: St.Martins (chapter 15).

[Schoe95] Schoechle, T. D. (1995): *Privacy on the information superhighway will my house still be my castle?* In: Teleconmmunications Policy Vol.19, Nr. 6, August 1995, 435-452.

[SKSt06] Schwaig, Kathy Stewart; Kane, Gerald C. and Storey, Veda C. (2006): *Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures?* In: Information and management: The international journal of information systems application, Oktober 2006, Band 43, Heft 7, S.805-820.

[SmSh07] Smith, Rhys; Shao, Jianhua (2007): Privacy and e-commerce: a consumer-centric perspective. In: Electronic Commerce Research, 7/2, Juni 2007, S.89-116.

[SOPHOS08] SOPHOS. Only one in 28 emails legitimate, Sophos report reveals rising tide of spam in April-June 2008. 15 Juli 2008. http://www.sophos.com/pressoffice/news/articles/2008/07/dirtydozjul08.html, Abruf am 2008-07-23.

[Strück07] Strücker, Jens (2007): *Der gläserne Kunde im Supermarkt der Zukunft.* In: Wirtschaftsinformatik, Volume 49, Nummer 1, Februar 2007, S. 59-62.

[Swe02] Sweeney, L. (2002): *k-Anonymity: a model for protecting privacy.* In: International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5): pp. 557-570.

[Swe04] Sweeney, L. (2004): *Uniqueness of simple demographics in the U.S. population.* Laboratory for International Data Privacy. Technical Report, Carnegie Mellon University (CMU).

[Tan06] Tangens, Rena & padeluun (2006): *Schwarzbuch Datenschutz. Ausgezeichnete Datenkraken der BigBrotherAwards.* Verlag Lutz Schulenburg.

[TaVa05] Tassabehji, Rana and Vakola, Maria (2005): *Business Email: The Killer Impact.* In: Communications of the ACM, Nov2005, Vol. 48 Issue 11, p.64-70, 6p.

[TiPa01] Tichy, Gunther; Peissl, Walter (2001): *Beeinträchtigung der Privatsphäre in der Informationsgesellschaft.*
http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf, Abruf am 2008-04-01.

[TRUSTe07a] TRUSTe Organization (2007) *Your Online Privacy Policy. An informational paper about drafting your first privacy statement or improving your existing one.*
http://www.truste.org/pdf/WriteAGreatPrivacyPolicy.pdf, Abruf am 2007-09-20.

[ULDa] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *Abhör- und Überwachungsskandal in Italien.*
https://www.datenschutzzentrum.de/allgemein/061018_italien.htm, Abruf am 2007-10-24.

[ULDb]: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: *P3P mit Netscape 7.0 von AOL.*
https://www.datenschutzzentrum.de/selbstdatenschutz/p3p/p3p_ns7.htm, Abruf am 2008-07-05.

[Wäll00] Wällisch, Thomas (2000): *P3P - Ein Modell für mehr Privatheit und Individualität im Internet?*
http://www.waellisch.de/home/p3p.pdf, Abruf am 2008-07-1.

[WB1890] Warren, Samuel D.; Brandeis, Louis D. (1890): *The Right to Privacy*. In: Harvard Law Review; IV (5): pp. 193–220

[Weintraub97] Weintraub J. (1997): *The theory and politics of the public/private distinction.* In: Public and private in thought and practise (pp. 1-42). Chicago: University of Chicago Press (chapter 1)

[Weiss08] Weiss, Oliver (2008): *Die E-Mail kämpft ums Überleben.* In: Computerwelt.
http://www.computerwelt.at/detailArticle.asp?a=113946&n, Abruf am 2008-02-12.

[West70] Westin, Alan F. (1970): *Privacy and Freedom*; Atheneum.

[W3Ca] W3C: World Wide Web Consortium: *Platform for Privacy Preferences (P3P) Project.*
http://www.w3.org/P3P, Abruf am 2007-09-20.

[W3Cb] World Wide Web Consortium (W3C) (2007): *Platform for Privacy Preferences (P3P) Project P3P 1.0. Implementations.*
http://www.w3.org/P3P/implementations, Abruf am 2008-06-19.

[W3Cc] World Wide Web Consortium (W3C) (2008): *The P3P Implementation Guide.*
http://p3ptoolbox.org/guide/, Abruf am 2008-07-07.

[W3Cd] World Wide Web Consortium (W3C): *The Enterprise Privacy Authorization Language (EPAL) – How to Enforce Privacy throughout an Enterprise.*
http://www.w3.org/2003/p3p-ws/pp/ibm3.html/, Abruf am 2008-06-05.

[W3Ce] World Wide Web Consortium (W3C): *A P3P Preference Exchange Language 1.0 (APPEL 1.0).* 15 April 2002.
http://www.w3.org/TR/P3P-preferences/#P3Ppolicies/, Abruf am 2008-07-05.

[W3Cf] World Wide Web Consortium (W3C): *A P3P- Validator*.
http://www.w3.org/P3P/validator.html, Abruf am 2008-07-05.

[WolfIR97] Wolf, Ilse; Wolf, Rudi: In: Computerwelt, 15/97 vom 7.4.1997, S.28

[Wörndl03] Wörndl, Wolfgang (2003): *Privatheit bei dezentraler Verwaltung von Benutzerprofilen.* Dissertationsarbeit. Fakultät für Informatik der Technischen Universität München.

[Zehentner02] Zehentner, Johann (2002): *Privatheit bei Anwendungen für Identitätsmanagement im Internet.* Diplomarbeit. Institut für Informatik der Technischen Universität München.

[ZD05] Zdziarski, Jonathan A. (2005): Ending Spam. *The Bayesian content filtering and the art of statistical language classification.* No Starch Press, Inc., San Francisco.

[Val08] Valcke von Vasko, Jan (2008): Spear Phishing – gezielte-Attacken auf naive Web-User. September 2008.
http://www.searchsecurity.de/themenbereiche/identity-und-access-management/tokens-smart-cards-rfid/articles/142809/index2.html, Abruf am 2008-11-24.