Fachbereich Informatik - Ang. Informatik (Master)
Institut für Internet-Sicherheit – if(is)

Studie

Google – die zwei Seiten des mächtigen Internet-Konzerns

Google's Strategien und Dienste verstehen sowie Gefahren erkennen, Risiken minimieren und dennoch profitieren

Nikolai Spogahn

Überarbeitete Version vom 25. Januar 2011

In Zusammenarbeit und betreut durch:

Prof. Dr. (TU NN) Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
https://www.internet-sicherheit.de

Inhaltsverzeichnis

Vorwort 4

Zusammenfassung 5

1 Einleitung 9

2 Google's Strategien 12

3 Wie mächtig ist Google? 15

3.1 Wirtschaftliche und allgemeine Daten 15

3.2 Technische Daten 18

4 Chancen und Risiken 19

4.1 Das Google-Konto 19

4.1.1 Die Webhistorie 19

4.1.2 Das Dashboard 20

4.2 Dienste und Produkte 21

4.2.1 Android und mobile Anwendungen 21

4.2.1.1 Google Sync 22

4.2.1.2 Near me now 22

4.2.1.3 Goggles 23

4.2.1.4 Latitude 24

4.2.1.5 Navigation 25

4.2.1.6 Allgemeine mobile Datenschutzbestimmungen 26

4.2.2 Google Street View und WLAN-Daten-Erfassung 27

4.2.2.1 Street View 27

4.2.2.2 Google Geolocation API 29

4.2.3 Weitere Dienste 30

4.2.3.1 Google Analytics 30

4.2.3.2 Google Base 31

4.2.3.3 Blogger.com 32

4.2.3.4 Google Books 33

4.2.3.5 Google Buzz 34

4.2.3.6 Google Checkout 35

4.2.3.7 Google Chrome 36

4.2.3.8 Google Code 37

4.2.3.9 Google Desktop und Gadgets 37

4.2.3.10 Google Earth 39

4.2.3.11 Google Finanzen 41
4.2.3.12 Google Flu Trends 42
4.2.3.13 Google Groups 43
4.2.3.14 Google Health 43
4.2.3.15 iGoogle 44
4.2.3.16 Google Kalender 45
4.2.3.17 Google Knol 46
4.2.3.18 Google Mail 47
4.2.3.19 Google Maps 48
4.2.3.20 Orkut 49
4.2.3.21 Panoramio 50
4.2.3.22 Google Picasa / Picnic 51
4.2.3.23 Google Profiles 52
4.2.3.24 Google Scholar 54
4.2.3.25 Google Talk/Voice 55
4.2.3.26 Google Text & Tabellen 56
4.2.3.27 Google Toolbar 57
4.2.3.28 Google TV 58
4.2.3.29 Google Wave 59
4.2.3.30 Google Websuche 60
4.2.3.31 YouTube 62
4.2.4 Cloud Computing 64
4.3 Chancen 67
4.4 Risiken 68
4.4.1 Datenschutz, informationelle Selbstbestimmung und allgemeine Risiken 71
4.4.1.1 Datenschutz 71
4.4.1.2 Informationelle Selbstbestimmung 71
4.4.1.3 Die Datenschutz-Risiken 73
4.4.1.4 Datenmissbrauch: Ausgewählte Fallbeispiele 74
4.4.1.5 Die Grundprinzipien des Datenschutzes 76
4.4.2 Dienstübergreifende Verknüpfung von Daten 77
4.5 Das Opt-out-Problem und Risikoverminderung 80
4.5.1 Browser-Add-ons 82
5 Widerstand, Abhängigkeiten und Konkurrenz 84
5.1 Politische Institutionen 84

5.2 Die Abhängigkeit von Nutzern und Werbetreibenden 85
5.3 Konkurrenz 85
5.3.1 Yahoo und Microsoft 86
5.3.2 Facebook 87
5.3.3 Amazon 89
5.3.4 Der Konkurrenzkampf mit dem Datenschutz 89
6 Fazit & Ausblick 90
Literaturverzeichnis 93
Abbildungsverzeichnis 103
Anhang A: Die Google-Webhistorie 104
Anhang B: Lokalisierung mit Firefox und der Google Geolocation API 106

Vorwort

In dieser Studie geht es um die Strategien und Dienste von Google. Es wird dargestellt, wie sich Nutzer im Google-Umfeld zu verhalten haben, wenn sie ihre Privatsphäre schützen und ihr Recht auf informationelle Selbstbestimmung ausüben wollen. In Form eines kleinen Leitfadens wird beschrieben, was für Risiken in diesem Umfeld lauern und wie man diese minimiert oder im Idealfall sogar eliminiert.

Die folgenden Ausführungen dieses Vorworts richten sich speziell an die Leser der ersten Version dieser Studie. Es soll kurz erläutert werden, welche Teile ergänzt bzw. überarbeitet wurden. Allen Erstlesern sei nahe gelegt, direkt mit der Einleitung zu beginnen. Für den eiligen Leser empfiehlt es sich, zumindest die Zusammenfassung zu lesen.

Bei der Betrachtung der Risiken, die eine Nutzung von Google's Angeboten mit sich bringen kann, wird die Datenschutz-Problematik näher erläutert. Dabei geht es darum, was Datenschutz eigentlich bedeutet und warum die informationelle Selbstbestimmung ein wichtiges Grundrecht ist. Weshalb sind also Eingriffe in die Privatsphäre und ausführliche Persönlichkeitsprofile auf Google-Servern überhaupt so problematisch? Dieser Frage wird in Kapitel 4.4.1 nachgegangen. Die angestellten Betrachtungen führen zur Problematik der dienstübergreifenden Verknüpfung von Daten, die in Kapitel 4.4.2 thematisiert wird. Kapitel 4.5.1 stellt die Möglichkeit vor, die genannten Datenschutz-Risiken mit entsprechenden Add-ons für den Webbrowser zu vermindern.

Im Rahmen der einzelnen Dienste und Produkte, die in Kapitel 4.2 detailliert untersucht werden, wurden *Street View*, *Google TV* und die *Websuche* aktualisiert bzw. erweitert. Ebenfalls geringfügig bearbeitet wurden *Google Chrome* und *Google Earth*. Außerdem wurde nun eine Reihe weiterer Dienste untersucht: *Google Base*, *Blogger.com*, *Google Finanzen*, *Google Groups*, *Google Kalender*, *Knol*, *Orkut* und *Panoramio*. Die Liste der Dienste wurde entsprechend ergänzt. In Kapitel 4.2.4 wird die Thematik Cloud Computing aufgegriffen und Google's Engagement in diesem Segment durchleuchtet. Dazu gehören die Projekte *Chrome*, *Chrome OS*, *Gears* und *Native Client*. Die Einleitung und das Kapitel „Fazit und Ausblick" sind ebenfalls überarbeitet worden.

Zusammenfassung

Google, ein Gigant in der Internetökonomie, stellt den Nutzern des Internets ein sehr breites Spektrum an Diensten und Produkten bereit. Neben der bekannten Suchmaschine, mit der alles begann, bietet Google mittlerweile Betriebssysteme, Office-Programme, Webbrowser sowie diverse Plattformen für Kommunikation, Kollaboration, Multimedia, Organisation und Softwareentwicklung. Aus Sicht des Nutzers ist Google's Angebot einerseits deshalb so interessant, weil viele Dienste qualitativ hochwertig, intuitiv bedienbar und innovativ sind, was sie zum Teil wirklich einzigartig macht. Anderseits ist das Angebot zum Großteil kostenlos nutzbar, was wohl der größte Vorteil für den Nutzer und der Hauptgrund für die Beliebtheit der Google-Produkte ist. Kostenlose Angebote gibt es jedoch viele im World Wide Web, diese finanzieren sich, genau wie Google, durch Werbung. Google erwirtschaftet in etwa 97 Prozent seiner Umsätze mit Werbung. Der Unterschied zu anderen werbefinanzierten Webangeboten ist allerdings, dass die Werbung bei Google nicht wirklich bei der Nutzung der Dienste stört und unaufdringlich ist. Es ergibt sich die Chance, von diesem Angebot, das zweifelsfrei einen Mehrwert darstellt und seinesgleichen sucht, zu profitieren.

Im Jahre 2009 hatte Google einen Umsatz von 24 Milliarden US-Dollar, das sind ca. 1,34 Millionen US-Dollar pro Mitarbeiter; doppelt so viel wie ein Microsoft-Mitarbeiter durchschnittlich umgesetzt hat. Außerdem erwirtschaftete Google in dem Jahr einen Gewinn von 6,5 Milliarden US-Dollar und war 2010 mit einem Marktwert von 114,3 Milliarden US-Dollar die wertvollste Marke der Welt. Im Jahr 2008 lag der Anteil am Gesamtvolumen der Werbeumsätze im Internet bei 42,2 Prozent. Beeindruckende Zahlen, aber was bedarf es neben den vielen Werbeflächen in den Diensten noch um solche Erfolge zu verzeichnen? Die Masse alleine macht es nicht, sondern auch die Klasse, die die Werbeflächen so wertvoll macht, dass Werbepartner bereit sind, stolze Preise dafür zu zahlen. Mit dieser Klasse ist die Kontextsensitivität der Werbung gemeint: Kontextsensitive Werbung soll die richtige Werbung für den richtigen Nutzer an der richtigen Stelle und zur richtigen Zeit liefern. Je mehr Informationen Google über die Interessen und das Verhalten seiner Nutzer zur Verfügung stehen, desto besser gelingt dies und desto mehr sind die Werbetreibenden bereit an Google zu zahlen. Ein Teil der kontextsensitiven Werbung ist interessensbasierte Werbung, bei der Google versucht, anhand des Verhaltens seiner Nutzer Interessen abzuleiten, um dann gezielt Werbung zu schalten. Ein anderer Teil ist mobile Werbung, momentan ein riesiger Wachstumsmarkt. Hier kommt der Aufenthaltsort des Nutzers als zusätzliche Dimension ins Spiel: Mit *Android* und mobilen Produkten wie *Goggles*, *Latitude*, *Navigation*, *Near Me Now* und *Sync* drängt Google in diese Nische vor. Aber auch andere Produkte der *Google Geolocation API* wie *Earth*, *Maps* oder *Street View* verschaffen Google ortsbezogene Informationen und stellen diese bereit. Als die Autos von Street View beispielsweise durch die Straßen Deutschlands gefahren sind, wurden WLAN-Netze erfasst, um so eine Ortung auf Basis von WLAN zu ermöglichen.

Das führt unmittelbar zur Kehrseite der zuvor betrachteten Chancen, denn die Währung in der Google-Nutzer für die Dienste und Produkte zahlen müssen, sind nicht etwa US-Dollar oder Euro, sondern persönliche Informationen. Hier hat Google sich den Ruf als sammelwütige Datenkrake eingehandelt. Die von Google erhobenen Daten sind direkt personenbezogen oder personenbeziehbar. Zu den direkt personenbezogenen Daten gehören unmittelbar erfasste Daten wie Name, Geburtsdatum, Adresse, berufliche Laufbahn etc. Diese können bzw. müssen

beispielsweise im Google-Profil oder bei *Google Checkout*, dem Online-Bezahldienst von Google, angegeben werden. Im Google-Konto, das für viele Funktionalitäten der Dienste erforderlich ist, laufen solche und weitere Daten zusammen. Zu den weiteren Daten, die mit dem Google-Konto verknüpft werden, gehören Inhalte der Webhistorie (eigentl. Webprotokoll), die beim Anlegen eines Google-Kontos standardmäßig aktiviert ist und dienstübergreifende Suchanfragen speichert. Zu den personenbeziehbaren Daten gehören vor allen Dingen Protokollinformationen, die nicht auf Basis des Google-Kontos, sondern per IP-Adressen, Cookies oder Browser-IDs erfasst werden. Dazu gehören u.a. Daten über Suchanfragen, angebotene Inhalte, Benutzernavigation aber auch Daten, die auf Webseiten Dritter erfasst werden. Die auf Basis von IP-Adressen und Cookies erhobenen Daten werden bei Google nach 9 bzw. 18 Monaten anonymisiert. Aber auch danach ist ein Rückschluss auf die wahre Identität des Nutzers nicht ausgeschlossen, speziell, wenn man einzeln erhobene Datensätze dienstübergreifend korreliert. Ähnliches konnte auch bei einer Datenschutzpanne bei AOL festgestellt werden, als ein Mitarbeiter versehentlich Suchanfragen von mehr als 600.000 Nutzern online stellte: Mehrere Nutzer konnten trotz Anonymisierung identifiziert werden.

Es entsteht ein Datenschutz-Risiko: Einerseits findet ein Eingriff in die Privatsphäre statt, wenn das Verhalten im Internet aufgezeichnet wird oder beispielsweise Fotos, die nicht für die Öffentlichkeit gedacht sind, in Street View oder ähnlichen Diensten abgebildet werden. Andererseits entstehen ausführliche Persönlichkeitsprofile auf den Servern von Google. Diese können gerade bei Google aufgrund seiner vielen Dienste besonders umfangreich sein. Zu den Risiken, die mit Persönlichkeitsprofilen im Internet verbunden sind, gehören Identitätsdiebstahl (Kriminaltaten unter gestohlener Identität), Belästigungen (z.B. durch Werbetreibende), Verfolgungen (Stichwort Rasterfahndung, aber auch Stalker), Demütigungen (speziell bei intimen Informationen) und verzerrte Persönlichkeitsbilder (Google und andere unterscheiden nicht zwischen richtigen und falschen Informationen). Dass diese Risiken tatsächlich vorhanden sind, zeigen viele Fälle von Datenmissbrauch, die in den letzten Jahren vermehrt auftreten. Wie sicher die Daten bei Google sind, ist fraglich. Augenscheinlich sind sie dort sicher, vielleicht sogar sicherer als bei anderen Anbietern, aber auszuschließen sind Datenschutzpannen und Datenmissbrauch z.B. durch kriminelle Hacker wohl nicht. Entsprechende Fälle hat es auch bei Google schon gegeben als z.B. in *Google Buzz* Kontaktdaten aus *Gmail* veröffentlicht wurden, indem sie automatisch mit den Kontakten anderer Nutzer verknüpft wurden. Außerdem waren die Kontakte, mit denen man am häufigsten über sein Konto kommuniziert, frei abrufbar. Man sollte sich stets vor Augen halten, dass Datenschutz nicht den Schutz von Daten bedeutet, sondern den Schutz des Einzelnen vor Beeinträchtigung bzw. unerwünschten Folgen, insbesondere durch zweckwidrigen Missbrauch, beim Umgang mit seinen personenbezogenen Daten.

Weitere Kritikpunkte bei Google sind, dass bei einigen Diensten die Einwilligung des Nutzers in die Datenerhebung zum Teil vollständig fehlt (z.B. bei Google Analytics) oder unzureichend realisiert ist. Hinzu kommt, dass bei vielen Diensten datenschutzrechtliche Grundprinzipien wie Zweckbindung, Erforderlichkeit, Datenvermeidung und -sparsamkeit sowie das Transparenzgebot nicht eingehalten werden. Es wird nämlich nicht ausführlich definiert, welche Daten genau für welche Zwecke erhoben werden. Daher ist auch schwer ersichtlich, ob erhobene Daten wirklich erforderlich sind. Personenbezogene Daten zu erheben, um einen Dienst erbringen zu können oder die Systemsicherheit zu gewährleisten sei viel zu allgemein gehalten.

Es entsteht ein Zwiespalt, möchte man doch von den Möglichkeiten, die Google einem bietet und dem resultierenden Mehrwert profitieren, ohne dabei jedoch mit den Gefahren in Berührung zu kommen. Mit anderen Worten: Der bereits erwähnte Preis für die Nutzung der Dienste sind personenbezogene Informationen und warum sollte man hier mehr bezahlen als man muss? Bei der Untersuchung von über 40 Google-Diensten fiel neben dem Mehrwert und der Sammelwut nämlich auch auf, dass diesbezüglich viel Potenzial zur „Preissenkung" vorhanden ist. Gewusst wie, kann man dafür sorgen, deutlich weniger über sich preiszugeben. Immerhin erkennt Google an, dass „jeder Nutzer seine eigene Einstellung zum Datenschutz hat" und will „möglichst allen Nutzern gerecht werden, in dem detaillierte Wahlmöglichkeiten angeboten werden". Diese Wahlmöglichkeiten bietet Google tatsächlich an und sollten genutzt werden. In den Nutzungsbedingungen und Datenschutzbestimmungen zu einem Dienst ist oft grob skizziert, welche Informationen erfasst werden und was für Möglichkeiten bestehen, um dies zu verhindern. Dementsprechend findet man in vielen Diensten in den Einstellungen eine Rubrik, in der die Erfassung diverser Daten deaktiviert werden kann. Auf diese Art und Weise kann man schon einiges für den Schutz seiner Daten tun. Man muss hier jedoch selbst aktiv werden, da es sich um optionale Wahlmöglichkeiten zur Deaktivierung (Opt-out) handelt. Dieses Opt-out-Problem, das nicht mit dem Regelungsgrundsatz „Verbot mit Erlaubnisvorbehalt" deutscher und europäischer Datenschutzgesetze in Einklang zu bringen ist, ist im Geschäftsmodell von Google verankert. Wenn man solchen Wahlmöglichkeiten explizit zustimmen müsste (Opt-in), damit mehr Informationen über sich preisgegeben werden, würde wohl kein Nutzer dies freiwillig tun. Bei einigen Diensten gehen die Wahlmöglichkeiten allerdings nicht weit genug. Das Datenschutz-Risiko wird somit nicht ausreichend vermindert und daher ist von der Nutzung dieser Dienste abzuraten.

Neben diesen von Google bereitgestellten Wahlmöglichkeiten gibt es auch noch eine Reihe weiterer Maßnahmen zur Risikoverminderung. Ganz allgemein sollte der Nutzer keine Angaben in Diensten machen, die nicht erforderlich sind, speziell wenn es sich um sensible Informationen handelt. Außerdem sollte man nie mit dem Google-Konto angemeldet werden, wenn es nicht notwendig ist, denn dann können erfasste Daten erst gar nicht unmittelbar mit dem Google-Konto verknüpft werden. Vermindert werden können Datenschutz-Risiken auch mit Add-ons für den Webbrowser. Speziell bei Open-Source-Browsern, aber auch bei anderen setzen diese dem uneingeschränkten Sammeln von Informationen ein Ende. Solche Add-ons stammen dann vor allem aus der dazugehörigen Community aber auch Google selbst bietet solche an. Zu den Add-ons von Google gehören z.B. das *Plugin zum Deaktivieren des Cookies für Anzeigevorgaben* (DoubleClick) oder das *Google Analytics Opt-out Browser Add-on*. Beispiele für Firefox-Add-ons sind *GoogleSharing* („Teilen für mehr Privatsphäre"), *TrackeMeNot* (sendet willkürlich gewürfelte Suchanfragen an bekannte Suchmaschinen) und *BetterPrivacy* (schützt vor Langzeit-Cookies wie Flash- und DOM-Storage-Cookies).

Darüber hinaus ist nicht jeder der vielen Dienste gut, nur weil er im Angebot von Google steht. Bei Google's sozialen Netzwerken, seinem Online-Bezahlverfahren und bei einigen weiteren Diensten konnten sich keine besonderen Vorteile gegenüber vergleichbarer Dienste anderer Hersteller herauskristallisieren. In diesen Fällen lohnt es sich erst gar nicht den Dienst zu nutzen und Google somit persönliche Informationen über sich zu überlassen. Das Recht auf Auskunft (ein weiterer anerkannter Grundsatz beim Datenschutz) bezüglich der von Google erhobenen Daten ist ansatzweise durch das *Google Dashboard* realisiert. Hier werden viele Daten aufgelistet,

die mit dem Google-Konto verknüpft sind (Suchanfragen, berechnete Routen etc.). Allerdings ist die Liste unvollständig, ein Blick darauf lohnt sich aber auf jeden Fall (siehe auch Anhang A).

1 Einleitung

Was 1998 als Suchmaschine startete, ist mittlerweile die wertvollste Marke der Welt und mit über einhundert weiteren Diensten der Marktführer in der Internetökonomie. Die Rede ist natürlich von dem Unternehmen Google Inc., im Folgenden kurz Google genannt. Kaum jemand kann noch im Internet surfen, ohne irgendwie auf Google zu stoßen, sei es bewusst oder unbewusst. Google veröffentlicht eine Innovation nach der anderen und dringt immer wieder in neue, zuvor schier undenkbare Märkte vor. Infolgedessen entstehen die unterschiedlichsten Produkte und Dienste und das Beste daran: Sie können fast alle kostenfrei genutzt werden. Andererseits ist Google ein börsennotiertes Wirtschaftsunternehmen, das seinen Aktionären gegenüber verpflichtet ist, Gewinne zu erwirtschaften. Also kann die Nutzung der Dienste nicht vollkommen kostenfrei sein, irgendeinen Preis wird der Nutzer schon dafür zahlen müssen. Wie sonst könnte Google seine immensen Investitionen in neue Anwendungen refinanzieren? Alleine die Digitalisierung von 15 Millionen angestrebten Büchern beim Projekt „Google Books" kostet Google eine halbe Milliarde Dollar und das ohne die Kosten für die entsprechende Hardware und Forschung sowie ohne die rückwirkenden Zahlungen an Rechteinhaber (Kaumanns/Siegenheim 2009: 244). Hierbei handelt es sich wohlbemerkt nur beispielhaft um einen von vielen Diensten. Insgesamt werden Milliarden in neue Dienste und Produkte investiert.

Es gibt also viele verschiedene, innovative und größtenteils kostenfreie Dienste. Hinzu kommt noch, dass diese überwiegend qualitativ hochwertig sind. Es handelt sich hier um ein wahres Benutzererlebnis, wie Google nicht zu Unrecht verspricht. Dies findet sich auch in einigen Punkten der Google-Unternehmensphilosophie wieder:

- Punkt 1: Der Nutzer steht an erster Stelle, alles Weitere ergibt sich von selbst.
- Punkt 2: Es ist das Beste, eine Sache richtig gut zu machen.
- Punkt 3: Schnell ist besser als langsam.
- Punkt 10: Großartig ist einfach nicht gut genug.

Hier muss man Google in der Tat einräumen, immer wieder richtig gute, schnelle und großartige Produkte auf den Markt zu bringen und der Konkurrenz fällt es sehr schwer, Schritt zu halten: Google ist eigentlich fast immer einen entscheidenden Schritt voraus. Dass der Kunde „König" ist, wie aus dem ersten Punkt zu entnehmen ist, entspricht eigentlich der Außendarstellung eines jeden Unternehmens, daher ist dies nicht wirklich als Besonderheit zu betrachten. Allerdings ist der Nutzer eigentlich bei Google gar nicht der zahlende Kunde des Unternehmens. Dennoch steht er an erster Stelle. Warum dem so ist, wird im Verlauf dieser Ausarbeitung noch deutlich.

Weiter heißt es im ersten Punkt der Unternehmensphilosophie: „Von der Entwicklung eines neuen Internetbrowsers bis zum letzten Schliff des Startseitendesigns ist unser höchster Anspruch, dass Sie von diesen Verbesserungen profitieren. Interne Ziele oder Gewinne treten dahinter zurück. […] Neue Tools und Anwendungen sollten unserer Ansicht nach so gut funktionieren, dass Sie sich keine Gedanken darüber machen werden, was man hätte anders machen können." Dies ist eine Stelle, in der man sich fragen muss, ob Google sich da nicht vielleicht etwas weit aus dem Fenster lehnt. So schön und edel sich dieser und die weiteren Punkte der Unternehmensphilosophie auch anhören, so darf Eines nicht vergessen werden: Dieser schon angesprochene Preis, den der Nutzer zu zahlen hat, damit er in den Genuss der Dienste und Produkte von Google kommen kann. Dabei handelt es sich im schlimmsten Fall um

die Aufgabe der Privatsphäre und des Grundrechts auf informationelle Selbstbestimmung. Google-Nutzer stellen dem Unternehmen nämlich persönliche Informationen über sich zur Verfügung, einfach nur in dem sie die Dienste nutzen. Solche personenbezogenen Daten sind im Internet wohl das vielversprechendste Gut, um Geld zu verdienen.

Die Kehrseite der kostenlosen, qualitativ hochwertigen Anwendungen ist also der Datenhunger von Google, der gestillt werden will, um diese kostenlosen Dienste nicht nur zu refinanzieren, sondern satte Gewinne zu erwirtschaften (im Jahr 2009 mehr als 6,5 Milliarden US-Dollar). Um solche Gewinne möglich zu machen, muss Google so viele Daten sammeln, dass es sich den Ruf als Datenkrake eingehandelt hat. Wie hungrig diese Datenkrake ist, kann man der Unternehmensphilosophie auch sehr schön entnehmen. So heißt es dort im siebten Punkt: „Irgendwo gibt es immer noch mehr Informationen." Die ursprünglichen Informationen des World Wide Web stehen dabei schon lange nicht mehr im Vordergrund. Vielmehr strebt Google an, „die weltweit verfügbaren Informationen zu organisieren". So ist es auch nicht verwunderlich, dass Google faktisch in Besitz eines eigenen Satelliten für Luftaufnahmen ist (Kaumanns/Siegenheim 2009: 280), mit Autos durch die Städte fährt und die Straßenumgebungen „scannt" oder Millionen Bücher aus Bibliotheken erfasst.

Es kommt einem nicht zu Unrecht vor, als wenn Google vor Nichts Halt macht, um an noch mehr Daten zu gelangen. Ein großes Problem für den Internetnutzer stellen dabei die personenbezogenen Informationen dar. Diesbezüglich werden hier, wie an vielen weiteren Stellen im Internet auch, international anerkannte datenschutzrechtliche Grundprinzipien nicht eingehalten bzw. unzureichend umgesetzt. Ein weiteres Problem ist, dass sich die Erhebung von Daten durch Google aufgrund seiner Marktdominanz und der vielen vollkommen unterschiedlichen Dienste auf einen enorm großen Bereich ausdehnt. Die personenbezogenen Daten aus den einzelnen Diensten können zu einem ausführlichen Persönlichkeitsprofil verknüpft werden. Die Datenschutz-Problematik spiegelt sich in Berichterstattungen und Diskussionen bzgl. Google in den Medien wider, die oft eher negativ ausfallen. Als Beispiel sei die aktuelle Diskussion um Google Street View genannt. Auch eine Untersuchung der Bürgerrechtsorganisation Privacy International bestätigt die bestehende Gefahr: Als einzigem von 23 untersuchten Internetunternehmen, einschließlich Microsoft, Yahoo, Amazon und eBay, wurde Google das Prädikat „datenschutzfeindlich" verliehen (Kaumanns/Siegenheim 2009: 135).

Es entsteht ein Zwiespalt, möchte man doch von den Vorteilen bzw. Chancen, die sich aus der Nutzung von Google's Diensten und Produkten zweifelsfrei ergeben, profitieren, ohne jedoch mit den Gefahren bzw. Risiken in Berührung zu kommen. Schließlich möchte wohl niemand seine Privatsphäre und sein Grundrecht auf informationelle Selbstbestimmung verlieren, was wohl die größte Gefahr darstellt, wenn Informationen rund um die eigene Person im Internet kursieren. Dass dieses Nutzen der Chancen ohne eine Beeinträchtigung durch Risiken zumindest ansatzweise möglich ist, verspricht Google's viertes Datenschutzprinzip: „Jeder Nutzer hat eine eigene Einstellung zum Datenschutz. Um möglichst allen Nutzern gerecht zu werden, bieten wir ihnen detaillierte Wahlmöglichkeiten hinsichtlich der Nutzung ihrer Daten." Diese Wahlmöglichkeiten sollen in dieser Ausarbeitung einmal näher betrachtet werden, damit Internetnutzer sie in Anspruch nehmen können, um etwaige Risiken zu eliminieren oder sie zumindest zu vermindern. Sind diese Wahlmöglichkeiten nicht ausreichend, so kann es allerdings auch sein, dass von der Nutzung eines Dienstes komplett abgeraten wird. Außerdem sollen einige weitere Maßnahmen vorgestellt werden, die alle zu einer Verminderung des Datenschutz-Risikos

beitragen. Mit anderen Worten: Die Währung, in der Google-Nutzer für die Nutzung des Angebots an Diensten und Produkten zahlen, ist weder Euro noch Dollar, sondern personenbezogene Daten und genau diesbezüglich gilt es, den Preis zu weit wie möglich zu drücken.

Ziel dieser Ausarbeitung ist es nicht, pauschale Urteile zu fällen wie „Google weiß alles“ oder „Google ist böse“ und dass man Google-Software deshalb, sofern nur irgendwie möglich, meiden sollte. Ziel ist es vielmehr, sachlich und neutral herauszuarbeiten, wie man die Chancen bzw. den Mehrwert der Dienste, der zweifelslos vorhanden ist, nutzen kann und die damit verbundenen Risiken minimiert. Dazu werden in den folgenden beiden Kapiteln zunächst die Strategien und die Macht von Google betrachtet, um die Basis für das Verständnis von Chancen und Risiken zu legen. Um die geht es nämlich im vierten Kapitel. Dabei wird versucht, die interessantesten und wichtigsten Dienste bzgl. ihres Mehrwerts und/oder ihrer Risiken im Einzelnen und anschließend im Ganzen, also bezogen auf die Anhäufung und Konzentration der Daten bei der Nutzung mehrerer Dienste, zu untersuchen. Es wird also im Gesamtkontext aller Dienste bewertet, ob und wie man Google’s Dienste und Produkte nutzen sollte. Im letzten Teil soll betrachtet werden, was die Marktdominanz von Google beeinträchtigen könnte und welche Parteien hier eine Rolle spielen. Dies soll einen Ausblick auf Google’s Zukunft ermöglichen.

2 Google's Strategien

In der Einleitung wurde bereits erwähnt, dass Google dem Nutzer die meisten Dienste kostenfrei zur Verfügung stellt und dass diese kostenlosen Leistungen auch ihre Kehrseite haben. Dabei handelt es sich um die personenbezogenen Informationen, die der Nutzer Google bei der Nutzung dieser Dienste überlässt. Nicht erwähnt wurde allerdings, wie Google mit diesen Datenmassen Geld verdient und wer die eigentlichen Kunden von Google sind. Das und die damit verbundenen Strategien sollen in diesem Kapitel nun anhand des Geschäftsmodells behandelt werden.

> *There is a new business model that's funding all of the software innovation to allow people to have platform choice, client choice, data architectures that are interesting, solutions that are new – and that's being driven by advertising.* (Google CEO Eric Schmidt nach Bogatin 2006)

Neben den vielen kostenlosen Diensten gibt es zwei Werbeprogramme namens AdWords und AdSense, die das eigentliche Kerngeschäft von Google bilden. Mit AdWords generiert Google den Hauptteil seiner Umsätze. Dabei handelt es sich um ein Programm für Werbetreibende, bei dem Google Werbeanzeigen für zahlende Kunden in seine Dienste integriert. AdSense ist ein Programm für Webseitenbetreiber, die somit die Möglichkeit haben, Google-Werbung auf ihren Webseiten zu platzieren, um an eventuellen Werbeerlösen, die durch Klicks auf ihrer Webseite generiert werden, beteiligt zu werden (vgl. Google 2010a). Im Grunde genommen erweitert Google mit AdSense seine Werbefläche. Im Jahr 2008 hatte Google 42,2% Anteil am Gesamtvolumen der Werbeumsätze im Internet (Stöcker 2009). Die zwei wichtigsten Säulen für diesen enormen Erfolg bilden die Kontextsensitivität und die Schlichtheit der Werbung.

Kontextsensitive Werbung soll die richtige Werbung für den richtigen Nutzer an der richtigen Stelle und zur richtigen Zeit liefern. Je mehr Informationen Google über die Interessen und das Verhalten seiner Nutzer zur Verfügung stehen, desto besser gelingt dies und desto mehr sind die Werbetreibenden bereit an Google zu zahlen. Somit wäre auch der Grund für den Datenhunger von Google geklärt. Die Zukunft gehört dem mobilen Internet. Kein Wunder also, dass Google auch hier sehr aktiv ist, ermöglicht es Google bzgl. seiner Werbung doch, in eine neue Dimension, nämlich der örtlichen, vorzustoßen. Die Werbung, die der Nutzer auf seinem mobilen Endgerät erhält, soll auf den Wirklichkeitsausschnitt, in dem er sich gerade befindet, zugeschnitten sein. Solche Werbung wird auch real-kontextsensitiv genannt und basiert auf einer Ortung der mobilen Endgeräte. Laut Eric Schmidt ist mobile Werbung doppelt so lukrativ wie normale, da sie generell persönlicher ist (Sagawe 2009: 65). Dies ist der Fall, weil ein mobiles Endgerät wie z.B. ein Smartphone in der Regel deutlich personenbezogener ist, als ein herkömmlicher Rechner. Mit dem mobilen Betriebssystem Android und den zahlreichen mobilen Diensten wie Navigation oder „Near You Now", einer ortsbezogenen Suche nach Informationen sowie mittlerweile auch mit dem eigenen Smartphone „Nexus One" drängt Google ganz offensiv in den mobilen Markt vor. Die Basis für diese neuen Mobilfunkangebote, in die dann real-kontextsensitive Werbung integriert werden kann, bilden die Location-Based-Services wie Google Maps, Google Earth oder Street View. Diese können die Koordinaten, die bei der Ortung per GSM-Zelle, GPS oder WLAN-Daten (siehe Kapitel 4.2.1/4.2.2) erfasst werden, verwerten. Google sieht in seiner kontextsensitiven Werbung einen wichtigen Mehrwert für den Nutzer. Irrelevante Werbung, die nur störend wirkt und dem Nutzer nicht wirklich weiter hilft, würde so vermieden.

> *Wir glauben, dass Werbung effektiv sein kann, ohne aufdringlich sein zu müssen. Google akzeptiert keine Popup-Anzeigen, die den gesuchten Inhalt möglicherweise überdecken.* (Ausschnitt aus dem sechsten Punkt der Google-Philosophie)

Die zweite Säule, die Schlichtheit, bezieht sich sowohl auf die Werbung, als auch auf die grafischen Oberflächen der Anwendungen und zwar nicht im negativen Sinne. Dies wird einem wohl sofort deutlich, vergleicht man beispielsweise die Webseiten von Google (z.B. www.google.com) mit denen von Yahoo (www.yahoo.com) oder anderen Portallösungen. Bei Google konzentrierte man sich schon seit jeher auf die wesentlichen Dinge. So ist 28 die maximale Anzahl an Wörtern, die auf der Google-Seite erscheinen dürfen, von Suchergebnissen mal abgesehen (Brandt 2010: 70). Auch in anderen Diensten und Produkten findet man relativ wenig, das beim Nutzen störend wirken könnte. Diesen großen Vorteil für den Nutzer hat auch Microsoft mittlerweile erkannt und seiner Websuche Bing ein vergleichbar schlichtes Erscheinungsbild verpasst. So viel zu den Diensten; sehr ähnlich sieht es bei den Werbeanzeigen aus: Bei der Nutzung von Google's Diensten stößt man weder auf Popups und Banner noch auf andere nervig wirkende Formen der Online-Werbung.

> *Anzeigen werden bei Google immer klar als solche gekennzeichnet. Ein äußerst wichtiger Grundsatz von Google ist, dass es keine Kompromisse bezüglich der Integrität unserer Suchergebnisse geben darf.* (Ausschnitt aus dem sechsten Punkt der Google-Philosophie)

Ein weiterer Aspekt ist die strikte Trennung von Inhalten und Werbung: Die Gründer von Google, Larry Page und Sergey Brin, betrachten eine Mischung aus Content und Werbung als etwas „Böses". Larry Page vergleicht Suchergebnisse mit Zeitungsartikeln, die ebenfalls frei vom Einfluss der Anzeigenkunden sein sollten. Diese Selbstverpflichtung auf saubere Werbung war und ist der Schlüssel für Google's Erfolg (vgl. Brandt 2010: 81f).

Das Geschäftsmodell von Google sieht also wie folgt aus: Kostenfreie Dienste und Produkte dienen dem Sammeln von Informationen und gleichzeitig als Werbefläche für kontextsensitive Werbung. Somit ist Google von seinen Nutzern abhängig, was erklärt, warum die Nutzer für Google an erster Stelle stehen. Diese weiß Google durch innovative, qualitativ hochwertige Dienste und Produkte zu überzeugen. Sie sind so gut und innovativ, dass Google kaum Werbung benötigt, um sich selbst zu vermarkten: Google war und ist auch ohne besondere Marketingkampagnen in aller Munde.

Je mehr großartige Dienste und Produkte Google rausbringt, desto mehr Nutzer hinterlassen Informationen und desto mehr Nutzer werden mit der kontextsensitiven Werbung erreicht. Für eine möglichst große Bandbreite an Nutzern und Informationen sorgt die umfangreiche Palette an Diensten und Produkten. Neben den vielen „normalen" Online-Diensten ist Google auch dabei, die Nutzer schon beim Zugang zum Internet für sich zu gewinnen. Dafür spricht der eigene Webbrowser Chrome, das mobile Betriebssystem Android und das reine Betriebssystem Chrome OS. Auch als Netzbetreiber ist Google tätig: Mit FON und Meraki ist man mit dem Projekt Open-Mesh im Bereich des kostenlosen Zugangs zum Internet per WLAN-Sharing aktiv. Mit San Francisco sollte sogar eine komplette Großstadt mit kostenlosem WLAN versorgt werden. Außerdem treibt Google mit Google Fiber den schnellen Internetzugang über Glasfaserleitungen voran und hat ernsthaft bei der Versteigerung von Mobilfunkfrequenzen in den USA mitgeboten. Unabhängigkeit auf dem Weg vom Nutzer zu Google's Diensten ist hier der wohl wichtigste Faktor. Fernab vom Web werden Millionen von Büchern aus Bibliotheken

eingescannt, Fotos von der Erdoberfläche, von den Straßen der Städte und sogar vom Mond und anderen Planeten geschossen und online verfügbar gemacht. Aber auch im Gesundheitswesen ist Google mit Google Health aktiv, handelt es sich hier doch um einen gigantischen Zukunftsmarkt (vgl. Brandt 2010: 165ff, Kaumanns/Siegenheim 2009: 275ff). Wie weit die Palette der Dienste und Produkte reicht, wird in Kapitel 4.2 deutlich, wenn einige davon etwas näher betrachtet werden. Bei den vielen unterschiedlichen Diensten und Produkten bleibt das Geschäftsmodell immer das gleiche: Refinanzierung durch kontextsensitive Werbung.

> *Wir wollen uns nicht mit Konkurrenten um den 4-Prozent-Anteil der Onlinewerbung streiten. Wir wollen an die restlichen 96 Prozent des Werbemarktes.* (Google's Nordeuropa-Geschäftsführer nach Kaumanns/Siegenheim 2008)

Dass Google den Markt der Online-Werbung dominiert, reicht ihm noch nicht aus, sind es doch nur ca. 4-5 Prozent, die vom gesamten Werbeumsatzvolumen auf die Online-Werbung fallen. So verwundert es auch wenig, dass Google mit Google TV momentan bis zu den Fernsehgeräten seiner (potentiellen) Nutzer vordringt oder Google sich mit Google Books und Google News als Online-Verleger sieht. Ein weiteres Beispiel für das immer weiter wachsende Spektrum der Werbekanäle ist, dass Google ein Patent angemeldet hat, um psychologische Profile von Video-Spielern zu erstellen. Dabei geht es darum, Verhaltensmuster von Spielern zu erstellen, um deren persönliche Eigenschaften wie Kooperation, Aggression, Risikobereitschaft etc. zu erfassen (vgl. Sagawe 2009: 8f). „Google zielt aktiv darauf ab, ein Betriebssystem für die Werbeindustrie zu schaffen, um so zur weltweit größten Werbeplattform zu werden" (Sagawe 2009: 63).

3 Wie mächtig ist Google?

In diesem Kapitel geht es darum, einen Blick darauf zu werfen, wie mächtig Google denn nun wirklich ist. Im fünften Kapitel geht es dann darum, wer Google Paroli bieten kann und wer oder was diese Macht zerstören oder zumindest beeinflussen könnte. Dabei geht es im Folgenden weniger um eine detaillierte Diskussion, sondern vielmehr um die Auflistung einiger wirtschaftlicher, technischer und allgemeiner Daten und Fakten. Google ist ein Unternehmen, das zwar viele Informationen über seine Nutzer sammelt, über sich selbst jedoch relativ wenig preisgibt. Daher beruhen folgende Daten überwiegend auf Schätzungen. Sofern keine Quelle angegeben ist, wurden die Schätzungen selbst durchgeführt. Nebenbei wird kurz erläutert, worauf diese Schätzungen beruhen. Umsätze und Gewinne beispielsweise mussten hingegen nicht geschätzt werden, denn diesbezüglich unterliegt Google den Mitteilungs- und Veröffentlichungspflichten für börsennotierte Gesellschaften. Daten alleine sind oft relativ wenig aussagekräftig, daher werden einige Referenzdaten, vor allem von Konkurrenten, angegeben.

3.1 Wirtschaftliche und allgemeine Daten

- Umsätze 2009 (vgl. CNN 2010)
  - Google: ca. 24 Milliarden $ (Platz 355 aller weltweit agierenden Unternehmen)
  - IBM: ca. 96 Milliarden $ (Platz 48)
  - Microsoft: ca. 58 Milliarden $ (Platz 115) – darunter gerade mal ca. 4 Mrd. Dollar aus Internetaktivitäten (Kaumanns/Siegenheim 2009: 365)
  - Apple: ca. 43 Milliarden $ (Platz 197)
  - Amazon: ca. 25 Milliarden $ (Platz 340)
  - Oracle: ca. 23 Milliarden $ (Platz 366)
  - Yahoo: ca. 7 Milliarden $ (nicht mehr in den Top 500)
  - Facebook: ca. 0,1 Milliarden $
- Umsatz pro Mitarbeiter 2009
  - ca. 1,34 Millionen $ (Worldsites 2010)
  - damit in etwa doppelt so viel wie bei Microsoft (Brandt 2010: 65) und
  - dreimal so viel wie bei Yahoo (Siegenheim 2010)
- Gewinne 2009 (vgl. CNN 2010)
  - Google: ca. 6,5 Milliarden $
  - IBM: ca. 13,4 Milliarden $
  - Microsoft: ca. 14,6 Milliarden $
  - Apple: ca. 5,7 Milliarden $
  - Amazon: ca. 0,9 Milliarden $
  - Oracle: ca. 5,6 Milliarden $
  - Yahoo: ca. 0,6 Milliarden $
- Marktwert 2010 (vgl. AlpaxX 2010)
  - Google: 114,3 Milliarden $ und damit die wertvollste Marke der Welt
  - IBM: 86,4 Milliarden $ (Platz 2)
  - Apple: 83,2 Milliarden $ (Platz 3)
  - Microsoft: 76,3 Milliarden $ (Platz 4)

- Nutzer (vgl. Brownlow 2010)
    - Google
        - Mindestens 200 Millionen mit Google-Konto – selbst geschätzt, Basis: 2007 waren es ca. 52 Millionen, 2008 bereits ca. 92 Millionen
        - insgesamt über eine Milliarde Nutzer (vgl. Diedrichs 2010)
    - Yahoo: ca. 500 Millionen (Kaumanns/Siegenheim 2009: 357), darunter ca. 250 Millionen mit E-Mail-Konto
    - Microsoft: ca. 250 Millionen mit E-Mail-Konto
    - Facebook: 500 Millionen im Juli 2010 (Zeit 2010)
    - Twitter: 100 Millionen im April 2010 (The Economic Time 2010)
- Suchmaschine
    - Marktanteile im Dezember 2009 (Stöcker 2009)
        - Google: 84,91%
        - Yahoo: 6,22%
        - Baidu: 3,28%
        - Bing: 3,26%
        - Ask: 0,58%
        - AOL: 0,49%
        - Andere: 0,22%
    - Monatliche Suchanfragen bei Google weltweit: 87,8 Billionen (Pingdom 2010)
    - Tägliche Besucher auf google.com: 620 Millionen (Pingdom 2010)

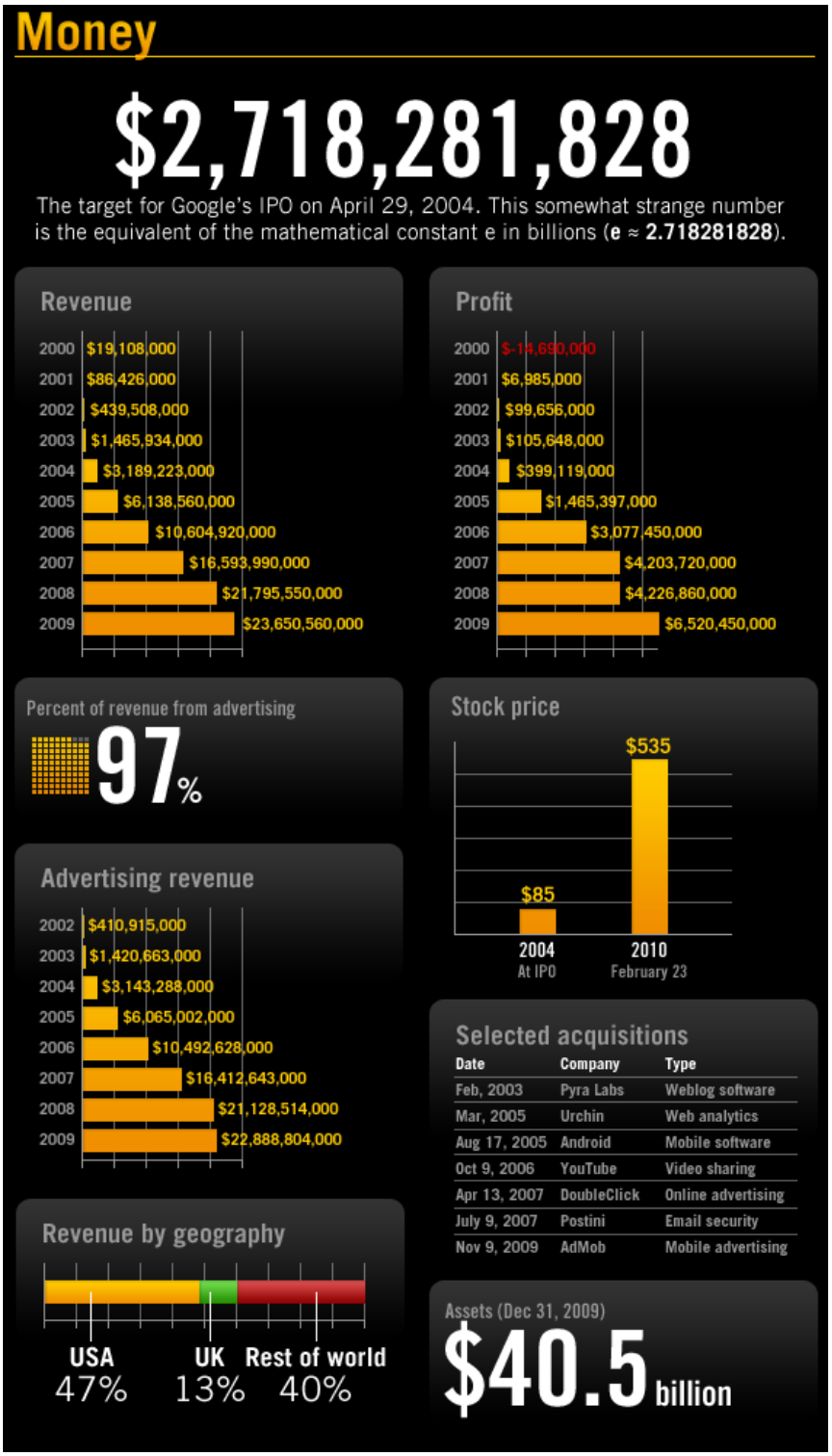


Abbildung 1: Weitere wirtschaftliche Daten (Pingdom 2010)

3.2 Technische Daten

- Rechenzentren
  - Google: Mind. 36-38 (vgl. CloudTweats 2010, Miller 2008, Pingdom 2008)
- Rechner (vgl. Intac 2010, Miller 2009)
  - Google: ca. 1.900.000 Rechner
    - Ca. 52.200 Rechner pro Rechenzentrum
    - Ein konkretes Rechenzentrum hat 45 Container mit jeweils 1.160 Servern (CloudTweats 2010, Ihlenfeld 2009)
    - Andere Schätzungen gehen von mindestens 1.000.000 Rechnern aus
  - Microsoft: ca. 800.000 (+)
  - Yahoo: ca. 50.000 (+)
  - Facebook: ca. 30.000-60.000
- Ca. 66,7 PetaFLOPS Rechenleistung
  - Ca. 33 GigaFLOPS bei einem "3 GHz Xeon"
  - Im Januar 2008 hatte ein Standard Google-Rechner zwei 2 GHz Intel Xeon Prozessoren und 4 GB RAM (Dean/Ghemawat 2008: 8)
  - Auch wenn die Rechenleistung eines einzelnen Rechners in einem verteilten System nicht mit der Einzelleistung multipliziert werden kann, so werden doch einige, mittlerweile vielleicht sogar viele Rechner mehr als 33 GigaFLOPS haben
  - Vergleich: Cray XT5 (Jaguar), der leistungsfähigste Supercomputer der Welt hat eine Rechenleistung von 1,759 PetaFLOPS bei 224.162 Prozessorkernen
- Ca. 2 Exabyte (2.000.000 Terabyte) Speicherkapazität
  - Ca. 1 Terabyte pro Rechner
  - Im Januar 2008 hatte ein Standard Google-Rechner zwei 160 Gigabyte Festplatten (Dean/Ghemawat 2008: 8)

4 Chancen und Risiken

In diesem Hauptkapitel geht es darum, welche Chancen bzw. Möglichkeiten und welche Risiken aus den Diensten und Produkten von Google resultieren. Dazu werden knapp 40 von ihnen unter die Lupe genommen und bzgl. ihrer Vorteile (Chancen) und ihrer datenschutz- bzw. sicherheitstechnischen Nachteile (Risiken) bewertet. Ein besonderes Augenmerk liegt dabei auf den mobilen Anwendungen, auf der aktuellen Debatte um Street View und die damit verbundene Erfassung von WLAN-Netzen sowie auf dem Thema Cloud Computing. Zunächst werden jedoch einige Grundlagen zur Nutzung der Dienste betrachtet. Dazu gehören das Google-Konto, die Webhistorie und das Dashboard. Den Schluss des Kapitels bildet eine Gesamteinschätzung. Dabei wird vertieft auf die Datenschutzproblematik einschließlich des Problems einer dienstübergreifenden Korrelation von Daten eingegangen. Dieser Darstellung des Gesamtrisikos folgen dienstübergreifende Möglichkeiten um es zu vermindern.

4.1 Das Google-Konto

Das Google-Konto ist Voraussetzung für viele Funktionalitäten von Google's Diensten. Einige Dienste können ohne ein Google-Konto gar nicht genutzt werden, so dass eine entsprechende Registrierung und Anmeldung zwingend erforderlich ist. Das Google-Konto ist notwendig, um den Benutzer zu identifizieren und auf ihn bezogene Daten auf Google-Servern zu speichern (z.B. E-Mails). Gemäß Single Sign-On handelt es sich immer um dasselbe Konto, unabhängig davon, welchen Dienst man nutzt. Dementsprechend laufen alle benutzerbezogenen Informationen im Google-Konto zusammen. Beim Login bzw. Registrieren ist standardmäßig die Option „Angemeldet bleiben" selektiert. Deaktiviert man diese Option und vertippt sich beim Login einmal, ist diese Option anschließend direkt wieder selektiert. Hier könnte man Google vorwerfen, es wolle forcieren, dass der Nutzer in möglichst vielen Situationen, in denen er im Web unterwegs ist, auch mit dem Google-Konto angemeldet ist, um ein User-Tracking auf Basis dieses personalisierten Kontos durchzuführen. Immerhin muss man Google zu Gute halten, dass man sich doch relativ oft durch eine erneute Eingabe des Passworts neu authentifizieren muss (zumindest, wenn es darum geht, Kontoeinstellungen einzusehen und anzupassen). Andererseits bietet das Google auch die Verifikation der Personalisierung. So kann Google sicher gehen, dass auch wirklich noch die richtige Person den Dienst nutzt bzw. getrackt wird. Mit dem Konto verknüpfte Daten unterliegen nicht den allgemeinen Fristen zur Anonymisierung der auf Basis von IP-Adressen und vor allem Cookies erhobenen Daten. IP-Adressen werden nämlich nach 9 Monaten anonymisiert und Cookie-Informationen nach 18 Monaten gelöscht (vgl. Google 2010b).

4.1.1 Die Webhistorie

Legt man ein neues Google-Konto an, so ist standardmäßig die Webhistorie aktiviert. Eigentlich heißt sie bei Google durchgehend „das Webprotokoll". Diese Übersetzung aus dem ursprünglichen englischen „Web History" scheint allerdings aufgrund der Verwechslungsgefahr zu Kommunikationsprotokollen etwas unglücklich. In der Webhistorie werden verschiedene Suchanfragen und abgerufene Inhalte gespeichert: Webseiten, Bilder, Nachrichten, Produkte, Anzeigen, Videos, Karten, Blogs, Bücher etc. Neben den eingegebenen Suchbegriffen bei den

dazugehörigen Diensten (z.B. die Suchmaschine bei Webseiten, Picasa Webalben bei Fotos, Maps bei Adressen, Books bei Büchern, Products bei Produkten usw.) werden die Webseiten, die Fotos, die Adressen, die Bücher, die Produkte etc., die man letztlich abruft und sich anschaut, zusätzlich gespeichert. Wie im vorherigen Abschnitt bereits erwähnt, unterliegen diese nicht den allgemeinen Fristen zur Anonymisierung der erfassten Daten bei Google, wie es z.B. bei den Daten der Fall ist, die Google erhebt, wenn man nicht mit dem Google-Konto eingeloggt ist (z.B. IP-Adresse, Cookie-ID und angeforderte URL). Sinn und Zweck der Webhistorie ist es laut Google zum einen, dem Nutzer einen schnellen, ortsunabhängigen Zugriff auf seine eigene Historie zu ermöglichen und zum anderen sollen die Suchergebnisse mit der Zeit besser auf die persönlichen Anforderungen zugeschnitten sein (vgl. Google 2010c).

4.1.2 Das Dashboard

Das Google Dashboard soll dem Nutzer eine praktische Übersicht über die verwendeten Google-Dienste bieten und ihm zeigen, welche Informationen Google mit dem Google-Konto verknüpft und speichert. Zusätzlich enthält es Funktionalitäten, um solche Daten zu löschen.

> *Wir wissen wie wichtig es ist, Ihnen auf einer übersichtlichen Seite vollen Zugriff auf Ihre Daten zu ermöglichen. Deshalb haben wir Google Dashboard entwickelt. Das Dashboard bietet Ihnen mehr Transparenz und eine bessere Übersicht. Sie können Ihre Daten löschen, Ihre Einstellungen ändern und Ihre gesamten Google Nutzererfahrungen jetzt noch einfacher mitgestalten.* (Google 2010d)

Laut Google werden sämtliche Daten angezeigt, die im Google-Konto zusammenlaufen. Nicht angezeigt hingegen werden Daten, die auch erhoben würden, wenn man nicht mit dem Google-Konto angemeldet ist. Dazu gehören z.B. Serverlogs (vor allem auf IP-Adressen bezogene Daten), die Browser-Identifikation (Cookies) und Interessenskategorien für interessensbasierte Werbung. Wohlbemerkt nennt Google diese nur als Beispiele (vgl. Google 2010b). In Anhang A ist das Dashboard zu sehen, das sich nach den Tests der verschiedenen Google-Dienste ergab. Der erste Eindruck von der möglichen Kontrolle über seine eigenen persönlichen Daten war sehr positiv. Allerdings fiel kurz später auf, dass die angezeigten Daten niemals alle sein können, die mit dem Google-Konto verknüpft sind. Schließlich kündigt Google selbst an, dass man alle Daten dort sehen kann. Dementsprechend kann man bei dieser Ankündigung eigentlich nur enttäuscht sein, obwohl die Kontrolle über viele persönliche Daten schon beachtlich ist. Als Beispiele für nicht gelistete Daten seien z.B. die persönlichen Notizen und Termine genannt, die bei iGoogle eingegeben wurden, oder der noch nicht im Dashboard erfasste Dienst „Google Wave“. Außerdem fehlen z.B. Daten, die Google Toolbar mit dem Konto verknüpft.

> *Es mag stimmen, dass "Google Dashboard einen bisher nicht gekannten Grad an Transparenz und Kontrolle über die eigenen Daten" ermöglicht, wie es in der Ankündigung heißt. Allerdings startet man von niedrigem Niveau. Und es mag auch stimmen, dass die Firmenphilosophie vorschreibe, die Erhebung von persönlichen Informationen transparent zu machen, wie der Betriebliche Datenschutzbeauftragte Per Meyerdierks sagt. Wie transparent aber, das sagt die Philosophie nicht. Serverlogdateien oder Nutzerprofile beispielsweise wird man wohl niemals rausrücken. Und wer diese versprochene Transparenz nutzen will, der muss erst einmal noch mehr Daten hinterlassen. Und soll beispielsweise seine Interessen angeben, um besser personalisierte Werbung zu erhalten. Für Google ist das eine Win-Win-Situation. Egal, was der Nutzer macht, die Firma profitiert. Wer*

nicht kooperiert, über den wird gesammelt, was möglich ist. Wer mitmacht und seine Daten gewichtet, von dem erhält Google dadurch im Zweifel noch viel nützlichere Informationen. […] Kontrolle sieht anders aus. (Biermann 2009)

4.2 Dienste und Produkte

Dieser Abschnitt befasst sich nun mit einzelnen Diensten und Produkten aus dem Angebot von Google und stellt die Ergebnisse entsprechender Untersuchungen vor. Die meisten der untersuchten Anwendungen wurden selbst getestet, einige wie z.B. Google Checkout und Health hingegen nicht, da hier zwingend persönliche Informationen notwendig sind, die Google nicht mitgeteilt werden sollten. Auch ein eigens durchgeführter, ausführlicher Test von Android und den mobilen Anwendungen entfällt. Allerdings stützen sich die folgenden Betrachtungen immer auch auf einen theoretischen Teil, also den entsprechenden Nutzungs- und Datenschutzbestimmungen von Google sowie verschiedene, möglichst unabhängige Meinungen und Berichte, die recherchiert wurden.

4.2.1 Android und mobile Anwendungen

Android ist ein auf Linux basiertes Open-Source-Betriebssystem für Smartphones. Anfang August 2010 vermeldete Eric Schmidt, dass zu diesem Zeitpunkt ca. 200.000 „Android-Handys" täglich verkauft wurden (Labs 2010). Warum Google überhaupt auf diesem Markt tätig ist, wurde bereits in Kapitel 2 diskutiert: Unabhängigkeit von Herstellern und Netzbetreibern sowie mobile, personalisierte Werbung. Die folgenden Ausführungen sollen sich speziell mit Anwendungen von Google beschäftigen, die sich allgemein auf mobilen Endgeräten befinden oder von dort ausgeführt werden. Will man Google nämlich Glauben schenken, so sendet ein Android-Handy nicht mehr Daten an Google als jedes andere Smartphone, auf dem diese Anwendungen genutzt werden. Außer vielleicht anonymisierte Daten über die Internetnutzung aber nicht wer mit wem telefoniert oder wo sich eine Person im Moment aufhält etc. Diese Aussage scheint nachvollziehbar, handelt es sich doch bei Android um ein Open-Source-Betriebssystem (vgl. Hesselbach 2009). Folgende Anwendungen von Google sind am Beispiel des HTC Desires vorinstalliert:

- Gmail
- Talk
- Maps/Latitude
- Sync
- Chrome bzw. eine abgespeckte Version des Browsers

Die Dienste bzw. Funktionalitäten Google Sync, Goggles, Near Me Now, Latitude und der Navigationsdienst sollen nun einmal etwas näher betrachtet werden.

4.2.1.1 Google Sync

Google-Konto erforderlich: Ja

Beschreibung: Automatischer Synchronisierungsdienst, mit dem E-Mails aus Gmail, Kontakte und der Kalender des Smartphones, online, mit dem Google-Konto synchronisiert werden. Dieser Dienst ist nicht nur für Android-Handys verfügbar, sondern auch für iPhone, BlackBerry, Nokia S60 und Windows Mobile (Google 2010e).

Mehrwert: Zentrale, konsistente Datenhaltung für E-Mails, Kontakte und Kalendereinträge. Unabhängig davon, an welchem mobilen Endgerät sich ein Nutzer befindet, oder ob er sich daheim am Desktop-PC oder Laptop befindet, seine Daten sind synchron. Der Datenaustausch funktioniert innerhalb von Sekunden, ohne dass man davon etwas mitbekommt (natürlich nur sofern man Empfang hat).

Risiken: Fortan sind persönliche Kontakte und Kalendereinträge des Smartphones mit dem Google-Konto verknüpft.

Risikoverminderung: Wenn man nicht möchte, dass Kontakte und Termine mit dem Google-Konto synchronisiert werden, dann darf man diese Funktion nicht aktivieren.

4.2.1.2 Near me now

Google-Konto erforderlich: Nein

Beschreibung: Bei „Near me now“ handelt es sich um eine Funktionalität der mobilen Websuche (siehe Abbildung 2) mit der die Suche um die Information des eigenen Standorts als Eingabeparameter erweitert wird. Dementsprechend kann man in diversen Kategorien z.B. nach Restaurants oder Geldautomaten in seiner Nähe suchen. Zu den Suchergebnissen kann man sich dann Angebote, Bewertungen etc. anzeigen lassen, oder sich einfach nur den Weg dorthin berechnen lassen. „Explore right here” steht in der unteren Abbildung übrigens für eine Kategorie übergreifende Suche. (vgl. Hoffman/Myllymaki 2010.)

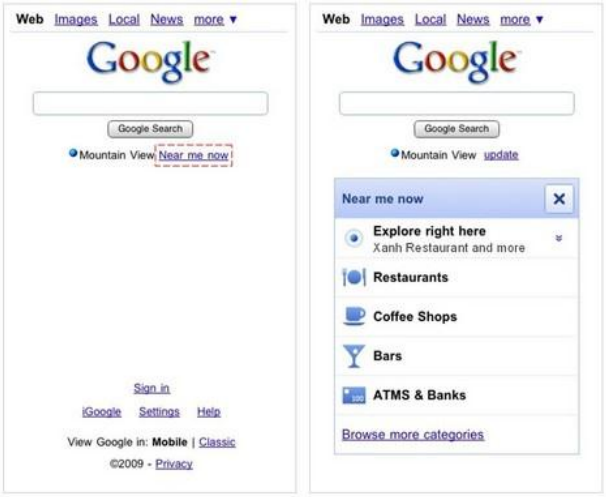


Abbildung 2: Near me Now - Die ortsbezogene Suche

Mehrwert: Ortsbezogene Informationen sind selbstverständlich ein echter Mehrwert und eine gute Hilfe sich in seiner aktuellen Umgebung zurechtzufinden. Dies ist vor allem dann hilfreich,

wenn man sich in fremden Gegenden aufhält, was z.B. im Urlaub oder auf einer Dienstreise der Fall sein kann.

Risiken: Wer die Funktionalität nutzt, gibt natürlich seinen aktuellen Aufenthaltsort preis und das, was er dort in der Nähe sucht. Diese Daten „sieht" natürlich nicht die Öffentlichkeit, sondern nur Google.

Risikoverminderung: Bis auf die allgemeinen Maßnahmen (z.B. nicht mit dem Google-Konto angemeldet sein) sind keine speziellen Möglichkeiten zur Risikoverminderung vorhanden. Möchte man nicht geortet werden, darf man „Near me Now" natürlich nicht nutzen.

4.2.1.3 Goggles

Google-Konto erforderlich: Nein

Beschreibung: Suchmaschine mit Bildern bzw. Fotos als Input für Suchanfragen. Man kann also z.B. Fotos von Sehenswürdigkeiten, Büchern, Visitenkarten, Gebäuden, Logos, Barcodes und Kunstwerken machen, um dann anhand dieser Fotos nach weiteren Informationen zu suchen. Auch eine GPS-Ortung wird verwendet, um bessere Suchergebnisse zu liefern. Mit einer Texterkennungs- und Übersetzungsfunktion kann man sich Fotos mit Texten direkt in eine andere Sprache übersetzen lassen.

Mehrwert: Goggles erlaubt es, ein Buchcover zu fotografieren, um nach dem Buch bei Google Books zu suchen, ein beliebiges Produkt zu fotografieren, um nach Preisen oder Bewertungen zu suchen etc. Ein anderes Beispiel wäre das Übersetzen einer Speisekarte in einem ausländischen Restaurant per Foto. Man kann also nach allen möglichen Informationen anhand eines Bildes suchen inkl. Übersetzungsfunktion.

Risiken: Die Gesichtserkennung ist zurzeit noch deaktiviert. Ansonsten ist der Dienst aus datenschutzrechtlicher Sicht ähnlich zu bewerten, wie die Suchmaschine. Allerdings mit dem Unterschied, dass hier mit Bildern statt Texten gesucht wird und bei eigenen Versuchen GPS verwendet wurde, um den Aufenthaltsort, vermutlich als zusätzlichen Eingabeparameter für die Suche, zu bestimmen. Ähnlich wie bei den Suchbegriffen kann die Historie der Suchanfragen, also die 1000 letzten Fotos, gespeichert werden. Dies ist allerdings optional (Opt-in). Sollte die Gesichtserkennung in Zukunft verfügbar sein, könnte man jeden beliebigen Menschen auf der Straße fotografieren und nach näheren Informationen über ihn suchen. Man wäre also in der Öffentlichkeit nicht mehr anonym (vgl. Debatin 2010).

Risikoverminderung: Die Suchhistorie sollte man deaktiviert lassen, damit die letzten 1000 Fotos nicht im Google-Konto gespeichert werden. Was aber viel wichtiger ist: Anscheinend ist die GPS-Ortung derzeit nicht abschaltbar. Daher darf man Goggles nicht verwenden, wenn man nicht geortet werden will. Sofern die Gesichtserkennung mal live geschaltet wird, sollte man darauf achten, dass ein Foto in Zusammenhang mit dem Namen nicht bei der Google-Suche indiziert ist (sofern man in der Öffentlichkeit anonym bleiben möchte). Dies kann z.B. geschehen, wenn man ein Google-Profil samt Foto besitzt, wenn man die Picasa-Software nutzt, bei der die Gesichtserkennung schon funktioniert, ein Foto in seinem Google Buzz-Profil hat usw. Dann bräuchte nämlich nur noch irgendwer ein Foto von jemandem auf der Straße zu machen, es bei Goggles „eingeben" und würde dort den Namen der Person sowie weitere Suchergebnisse finden.

4.2.1.4 Latitude

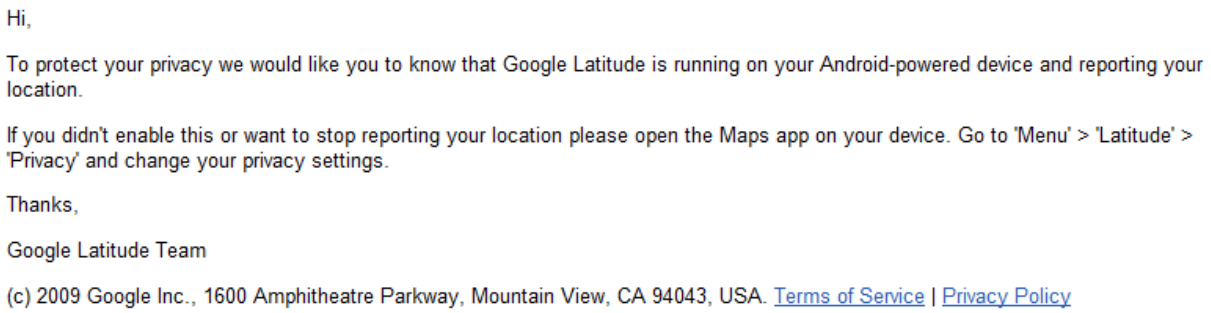
Google-Konto erforderlich: Ja

Beschreibung: Lokalisierungssoftware, bei der Nutzer – oder zumindest ihre Smartphones – über GPS, WLAN-Messdaten oder GSM-Zellen geortet werden und auf einer Karte von Google Maps angezeigt werden können. Natürlich sind die Nutzer nicht für alle sichtbar, sondern nur für andere, explizit ausgewählte Latitude-Nutzer.

Mehrwert: Ob es einen Mehrwert darstellt, wenn andere Leute sehen können, wann man sich wo aufhält, darf zumindest stark bezweifelt werden. Im Grunde genommen fällt es, bis auf vielleicht wenige individuelle Ausnahmen, in die Kategorie Überwachung im Stile von Big Brother oder aber in die Kategorie Spielerei. Der Werbespot auf der entsprechenden Latitude-Webseite konnte jedenfalls überhaupt nicht überzeugen.

Risiken: Vielleicht weiß nicht jeder, wo man sich gerade aufhält, da man sich die Leute, die einen auf der Maps-Karte sehen können, frei auswählen kann, aber zumindest lagern diese Informationen auf Google-Servern und sind mit dem Google-Konto verknüpft. Es scheint als ob Google den Standort bei laufender Anwendung standardmäßig ständig abfragt, unabhängig davon, ob man ihn für Freunde sichtbar macht oder nicht. Zumindest bekommt man eine E-Mail, die hierauf schließen lassen könnte, nachdem der Dienst das erste Mal gestartet wurde (siehe Abbildung 3).

Risikoverminderung: Diesen Dienst sollte man generell nicht starten, da der Nutzwert nicht im Verhältnis zu den durchaus vorhandenen Risiken steht. Auch das situative Aktivieren und Deaktivieren von Latitude wäre vermutlich ein großer Fehler, denn nachher vergisst man vielleicht doch, genau in der falschen Situation, Latitude wieder abzuschalten.



Hi,

To protect your privacy we would like you to know that Google Latitude is running on your Android-powered device and reporting your location.

If you didn't enable this or want to stop reporting your location please open the Maps app on your device. Go to 'Menu' > 'Latitude' > 'Privacy' and change your privacy settings.

Thanks,

Google Latitude Team

(c) 2009 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. Terms of Service | Privacy Policy

Abbildung 3: Ortungshinweis von Google, den man nach dem Latitude-Start per Mail erhält

4.2.1.5 Navigation

Google-Konto erforderlich: Ja

Abbildung 4: Google Navigation auf einem Android-Endgerät

Beschreibung: Google Maps Navigation macht das Android-Handy zum GPS-Navigationsgerät (siehe Abbildung 4). Statt der Eingabe von Adressen kann dabei direkt eine spezielle Suchfunktion verwendet werden. Eine Spracheingabe ist dabei auch möglich. Außerdem bietet die Navigationsfunktion eine Verkehrs- und Satellitenansicht. In den USA ist sogar Street View schon integriert (siehe Abbildung 5). Alle Daten (auch das Kartenmaterial) werden fortlaufend aus dem Internet heruntergeladen. Eine ständige Internetverbindung ist daher notwendig. Um die Navigationsfunktion zu erhalten, muss nur die aktuelle Version von Google Maps heruntergeladen werden. Allerdings befindet sich Google Maps Navigation momentan noch im Betastatus (vgl. Google 2010f).

Mehrwert: Das Smartphone wird zum vollständigen, kostenlosen Navigationssystem mit tollen Features, wie man es von Google gewöhnt ist. Die Karten und sonstigen Daten sind immer aktuell, da sie, wie bereits erwähnt, stets nachgeladen werden.

Risiken: Google erfährt natürlich unmittelbar, wo man sich gerade aufhält und wo man hinwill und könnte die Informationen mit dem Google-Konto verknüpfen. Bis jetzt wird bei diesem Dienst nur auf die allgemeinen mobilen Datenschutzbestimmungen (siehe Abschnitt 4.2.1.6) verwiesen. Die Satellitenansicht ist so stromintensiv, dass sich der Akku eines HTC-Smartphones bei Tests trotz angeschlossenem Ladekabel noch entladen hat. Auch der Traffic hat sich mehr als verzehnfacht: Statt 1 MB Traffic bei einer Fahrt über 55 km in der normalen Ansicht, wurden 11 MB Traffic verursacht (Dirscherl 2010). Ähnlich oder noch verheerender sieht das Ganze vermutlich bei „Street View“ aus. Vielleicht müsste man bei der Ansicht „Street View“ sogar aufpassen, dass man die entsprechende Ansicht nicht mit der aktuellen, realen Verkehrssituation verwechselt.

Risikoverminderung: Derzeit ist noch unklar, in wie fern es Wahlmöglichkeiten geben wird. Vermutlich werden geplante Routen, genau wie beim normalen Google Maps, in der Webhistorie

gespeichert. Außerdem könnte es sehr gut sein, dass der „Heimatort“ mit dem Google-Konto verknüpft wird.

Abbildung 5: Google Navigation in der Ansicht "Street View"

4.2.1.6 Allgemeine mobile Datenschutzbestimmungen

Google hat eine Liste der Informationen zusammengestellt, die allgemein von mobilen Google-Diensten erfasst werden könnten (vgl. Google 2010g). Die wichtigsten und interessantesten Daten sollen nun aufgelistet werden:

- Telefonnummer: Dies geschieht, wenn man sie bei Google speichert oder mit Google in Kontakt getreten ist, also bei Google angerufen oder eine SMS an Google (z.B. in einem Dienst) geschickt hat. Die Telefonnummer wird mit dem Google-Konto verknüpft. Sollte man nicht über ein Google-Konto verfügen, wird sie mit der Geräte-ID des Smartphones verknüpft.
- Allgemeine Informationen zu Ereignissen auf Geräteebene: Diese werden für Kundenserviceaufgaben vorrübergehend dem Google-Konto zugeordnet.
- Mobilfunkdaten: Akkustatus, Geräte- und Hardware-ID, Gerätetyp, Anforderungsart, Mobilfunkanbieter, Nutzerkennung beim Mobilfunkanbieter und allgemeine Nutzer-statistiken zu Gerät und Diensten. Die Geräte-ID und der Akkustatus werden dabei mit dem Google-Konto verknüpft.
- Informationen zu Downloads und Einstellungen bei Produkten aller Art.
- GPS-Daten bei standortbezogenen Diensten.
- Aufzeichnung von Spracheingaben bei entsprechenden Diensten mit Spracherkennung.

Hinzu kommen natürlich noch die ganzen Informationen, die man bewusst übermittelt, wie z.B. die Kontakte und Kalendereinträge bei der Nutzung von Google Sync. Anfangs war ein Google-Konto Voraussetzung für die Benutzung eines Android-Handys. Seit Version 1.5 (30. April 2009) ist dies jedoch nicht mehr der Fall; man kann die entsprechende Eingabe dieser Daten beim Start des Smartphones überspringen. Viele Dienste kann man ohne Konto nur eingeschränkt nutzen,

den Android Market (zum Erwerb zusätzlicher Apps) allerdings z.B. gar nicht. Und da es keine echte Alternativen zu diesem Markt gibt, bleibt man bei Android Apps ohne Google-Konto außen vor (vgl. Lanzerath 2010). Als Nachtrag wäre noch zu erwähnen, dass es anscheinend mittlerweile zwei bis drei Alternativen zum Android Market gibt, die auch alle gängigen Apps anbieten.

4.2.2 Google Street View und WLAN-Daten-Erfassung

Seit einiger Zeit fahren „Google-Autos" durch Städte und Dörfer und fotografieren die Umgebung in einer 360°-Rundumsicht, um die Aufnahmen dann später über das Internet verfügbar zu machen. Jeder kann sich die Fotos dann in Google Maps anschauen und sich virtuell in den Straßen der Städte umsehen. Zusätzlich zu den Straßen-Aufnahmen erfassten die Google-Autos auch noch sämtliche WLAN-Netze der Umgebung. Dabei wurden MAC-Adressen, SSIDs und Verschlüsslungsmechanismen erfasst. Allerdings hatte Google schon zuvor ähnliche Daten aus anderen Quellen bezogen. Zur Kostenersparnis wurden die WLAN-Netze nun, bei dieser sich bietenden Gelegenheit, gleich mit gescannt (vgl. Tagesschau 2010). Später kam heraus, dass nicht nur diese Daten, sondern auch Nutzdaten erfasst wurden. Im entsprechenden Programmcode in der für die Erfassung zuständigen Software befanden sich nämlich noch Rückstände von Code aus Testzwecken. Daraufhin wurde der WLAN-Scan vorrübergehend eingestellt, Google lies die Angelegenheit von einer unabhängigen Partei untersuchen und löschte alle erfassten Nutzdaten (vgl. Google 2010h). Unter Berücksichtigung dieser Aspekte gliedert sich das Kapitel nun in zwei Teile. Als erstes erfolgt die Analyse und Bewertung von Street View, der zweite Teil beschäftigt sich dann mit der sogenannten Geolokalisierung, bei der die gesammelten WLAN-Daten eine maßgebliche Rolle spielen. In Anhang B ist außerdem dokumentiert, wie die Geolokalisierung in einem Browser genutzt wird, um den Standort eines Internetnutzers mit aktivierter WLAN-Funktion zu orten.

4.2.2.1 Street View

Google-Konto erforderlich: Nein

Beschreibung: Street View ist eine Erweiterung von Google Maps um 360°-Straßenansichten. Als wenn man direkt vor Ort wäre, kann man sich virtuell (aber bei realen Aufnahmen) durch die Straßen von Städten und Dörfern bewegen. In Deutschland ist Google mit Street View auf massive Gegenwehr von Datenschützern und Politikern gestoßen. Deshalb dauerte es in Deutschland besonders lange, bis der Dienst verfügbar war. Am 18. November 2010 wurde Street View in Deutschland, als 27. Land weltweit, schließlich freigeschaltet und seitdem sind 20 deutsche Großstädte online: Berlin, Bielefeld, Bochum, Bonn, Bremen, Dortmund, Dresden, Duisburg, Düsseldorf, Essen, Frankfurt, Hamburg, Hannover, Köln, Leipzig, Mannheim, München, Nürnberg, Stuttgart und Wuppertal (vgl. Fernsehen in Dresden 2010).

Mehrwert: Es ist großartig, wenn man sich irgendwo umsehen kann, als wäre man direkt vor Ort, auch wenn die Aufnahmen nicht ganz aktuell sind. Man kann sich detailliert in seinem zukünftigen (oder potentiellen) Urlaubsort umsehen, anderen zeigen, wo man schon überall war und vieles mehr.

Risiken: Problematisch ist es, wenn die Privatsphäre von fotografierten Personen verletzt wird, denn auch wenn diese Bilder eigentlich auch jeder machen könnte (und übrigens auch dürfte), der vor Ort ist, so sind diese Bilder nun online und weltweit für alle sichtbar. Hinzu kommt, dass die Kameras in einer Höhe von 2,50 m aufnehmen und damit deutlich über der Augenhöhe eines Normalbürgers. Hecken und Zäune, die als Sichtschutz gedacht sind, würden so umgangen (vgl. Sander 2010). Google versucht zu anonymisieren, indem Autokennzeichen und Gesichter automatisch durch Verwischen unkenntlich gemacht werden. Dieser Mechanismus scheint zwar prinzipiell sehr gut zu funktionieren, allerdings kann man sich nicht einhundertprozentig auf ihn verlassen. So waren im Schweizer Bern z.B. Kennzeichen von Autos, die vor einem Bordell geparkt hatten, sichtbar, weil der Mechanismus nicht griff (Thomi 2009). Auch kursieren diverse Hitlisten im Netz mit den peinlichsten Aufnahmen aus Street View. Das gesamte Verfahren zur Unkenntlichmachung nach Widersprüchen ist mittlerweile vom TÜV Rheinland zertifiziert worden. Dennoch ist es nicht gewährleistet, dass das Verfahren in allen Fällen einwandfrei funktioniert, so Andreas Türk, Produktmanager von Street View in Deutschland: „Leider treten jedoch bei jedem großen manuellen Prozess wie diesem auch Fehler auf. So kann es durchaus vorkommen, dass einige Häuser in den 20 Städten auf unseren Street View Bildern zu sehen sein werden, die eigentlich unkenntlich gemacht sein sollten. Wir entschuldigen uns dafür im Voraus!" Er verweist darauf, dass man in solchen Fällen den Link „Ein Problem melden" in Street View verwenden soll, genau, wie auch in Fällen, in denen noch Gesichter und Autokennzeichen erkannt werden (Türk 2010). Als weiteres Problem kommt hinzu, dass man Leute auch an anderen Merkmalen als das Gesicht erkennen kann. So wirkt die Unkenntlichmachung des Gesichts laut Christoph Kappes wie ein Pendant zum „schwarzen Balken" in Printmedien, was sie wiederum jedoch nicht mal sei, da kein redaktioneller Auswahlprozess des Bildmaterials vorausgeht (Kappes 2010). In der Tat wird einem beim Anschauen einiger Fotos in Street View schnell klar, dass Personen, deren Gesicht unkenntlich gemacht wurde, auch sehr gut aufgrund anderer Kriterien identifizierbar sind. Für Autos gilt das gleiche, so kann beispielsweise ein markanter Aufkleber ein Auto identifizieren, auch wenn das Kennzeichen unkenntlich gemacht wurde. Ein weiterer Punkt neben der Privatsphäre ist die „Kriminalitätsförderung":

> *Befürworter von Street View argumentieren gern mit der hohen sozialen Kontrolle gerade in Kleinstädten und Dörfern. Dies ist aber ein Trugschluss, weil sich die Kontrolle eben nur auf die Mitglieder der örtlichen Gemeinschaft bezieht, mögliche Täter jedoch von außen kommen und über den Dienst Daten über lokale Verhältnisse erfahren, die sie aufgrund der sozialen Kontrolle sonst nicht unbeobachtet erhalten würden. Plakativ formuliert: Bäuerin Erna „weiß alles über das Dorf". Dieb Detlev kommt nicht aus dem Dorf und erfährt über Street View, was er nicht erfahren würde, ohne von Erna beobachtet zu werden. Für dieses Problem sehe ich keine Lösung, kann aber auch nicht einschätzen, ob es nicht eher ein akademisches Problem ist. Gibt es einen nachweislichen Effekt zwischen Street View und Kriminalität? Ich habe dazu keine Daten gefunden.* (Kappes 2010).

Risikoverminderung: Es bestehen geringe Chancen zur grundsätzlichen Bewältigung des Problems, das im Zusammenhang mit der Privatsphäre entsteht, denn sonst müsste man sich auf öffentlichen Straßen verstecken oder sich durch Verschleierung o.ä. selbst unkenntlich machen. Man müsste höhere Zäune aufstellen usw. Das klingt etwas überspitzt, aber wäre wohl der einzige noch verbliebene Grundschutz. Das wahre Problem heißt hier nämlich Opt-out: Google hat die Aufnahmen bereits „im Kasten" und fragt niemanden vorher, ob es Fotos von einer

Person oder dessen Eigentum ins Internet stellen darf, sondern tut dies einfach. Allerdings hat man die Möglichkeit, einen Widerspruch gegen die Veröffentlichung von Aufnahmen der eigenen Person, eigenen Kraftfahrzeugen und selbst bewohnten oder genutzten Gebäuden sowie von Grundstückseigentum formlos bei Google einzureichen. In Deutschland hatte man sogar die Möglichkeit, vier Wochen vor dem Starten des Dienstes einen Widerspruch einzulegen. Diese Frist wurde nach einer entsprechenden, mehrfachen Aufforderung der Bundesverbraucherministerin Ilse Aigner um weitere vier Wochen verlängert. Auch in Street View selbst gibt es bei den jeweiligen Panoramaansichten einen Link, über den man „ein Problem melden" kann. Allerdings setzt das voraus, dass man sich selbst auf die Suche nach entsprechenden Bildern macht. Das Verbraucherministerium rechnete spätestens bis Ende des Jahres 2010 mit 200.000 Einsprüchen aus Deutschland (Kuhr 2010). Doch noch vor dem Start des Dienstes gingen rund 250.000 Widersprüche ein, das sind knapp drei Prozent der Bewohner der 20 genannten Städte (vgl. Dreuw 2010).

4.2.2.2 Google Geolocation API

Google-Konto erforderlich: Nein

Beschreibung: Die Google Geolocation API dient der Lokalisierung bzw. Ortung von Internetzugängen. Sie wird u.a. von Android, Google Chrome, Firefox und Opera genutzt. Firefox beispielsweise übermittelt die Messdaten des WLAN-Adapters bzgl. der WLAN-Netze in der Umgebung des PCs (auf dem Firefox ausgeführt wird) an diese API. Diese Messdaten bestehen aus der SSID, der MAC-Adresse und der Signalstärke des jeweiligen WLAN-Netzes. Die Geolocation API beschafft sich nun Koordinaten zu diesen Daten aus der entsprechenden WLAN-Datenbank, die vor allem auf den bei Street View erfassten Daten basiert. Google Maps bietet schließlich die Möglichkeit, die genaue Adresse zu diesen Koordinaten zu ermitteln.

Mehrwert: Man hat die Möglichkeit, auf ortsabhängige Informationen auch bei Desktop-PCs, Notebooks und Netbooks (sofern diese über einen aktivierten WLAN-Adapter verfügen) zuzugreifen. Diese Informationen können in Suchen integriert werden, um bessere Ergebnisse zu liefern. Man kann sich z.B. unmittelbar alle Geschäfte in der Umgebung anzeigen lassen, die ein bestimmtes Produkt verkaufen. Allerdings würde es m.E. an dieser Stelle vollkommen ausreichen, wenn man selbst seinen ungefähren Ort explizit angeben kann und dieser nicht implizit von Firefox etc. ermittelt wird. Die Ortung per WLAN-Messdaten spielt für Google auch im mobilen Bereich eine wichtige Rolle: Sollte keine Ortung per GPS möglich sein, was gerade innerhalb von Gebäuden häufig vorkommen kann, so hat Google noch die Möglichkeit, eine Ortung auf Basis der WLAN-Messdaten vorzunehmen (vgl. MDR 2010).

Risiken: In Tests konnte der eigene Standort ziemlich genau bestimmt werden (siehe Anhang B). Das eine Mal traf es den Nachbarn gegenüber, das andere Mal eine Adresse wenige Häuser weiter. Das Problem: Die WLAN-Messdaten des eigenen Adapters werden ans Internet übertragen und somit auch ein direkter Bezug zum Aufenthaltsort. Dieser Bezug kommt durch Google's WLAN-Datenbank zustande. Zwar fragt beispielsweise Firefox den Benutzer vorher, ob diese Daten ans Internet übertragen werden sollen, allerdings mag man sich nur mal vorstellen, wenn andere Tools, speziell Hackertools, auf dem PC dies auch ungefragt tun. Dann ist die Geolocation API mit der WLAN-Datenbank ein gefährliches Mittel um Personen bzw. Internetzugänge zu orten. Die bisherige „Pseudo-Anonymität" (an die Adresse des Zugangspunktes zum Internet über die IP-Adresse aus den Zuordnungstabellen der Internet-

Provider gelangt man gewöhnlich nur über einen richterlichen Beschluss) könnte in vielen Fällen verloren gehen. Man weiß zwar immer noch nicht, wo sich ein Internetnutzer exakt aufhält, kann dies dann aber durch weitere Informationen (z.B. gemessenes WLAN-Netz mit der besten Signal-Stärke) gut abschätzen. Softwarehersteller versuchen schon seit längerem, Nutzer unlizenzierter Softwareprodukte zu orten um sie anschließend zu überführen. Ein Beispiel für eine solche Software ist Code Armor Intelligence. Ob diese nun wirklich die Geolocation API von Google nutzt, ist ungewiss, denn das genaue Verfahren ist unklar. Ebenso unklar ist auch die Zulässigkeit. Jedenfalls verwendet die Software Google Maps. Ein weiteres Problem ist, dass sich aus den erfassten Informationen, wie WLAN-Netze gesichert sind, für Schwarzsurfer ableiten lässt, wo schlecht gesicherte WLAN-Netze sind. Diese könnten sich daraus beliebig viele aussuchen, um kostenlos zu surfen, oder noch schlimmer, illegale Daten hoch- bzw. runterzuladen. Das wäre natürlich nur dann möglich, wenn sie in den Besitz der WLAN-Datenbank kämen (vgl. Fenselau 2010).

Risikoverminderung: Hier müssen zwei Teile behandelt werden, zum einen, wie man verhindert, dass eigene WLAN-Netze und -Daten gescannt werden und zum anderen, wie man verhindert, selbst geortet zu werden. Bedacht werden sollte allerdings, dass die Daten über WLAN-Netze ja nun schon erfasst wurden und man wohl nur noch verhindern kann, nochmal „gescannt“ zu werden. Man könnte sein WLAN beispielsweise komplett deaktivieren, sofern es gerade nicht benötigt wird. Alternativ könnte man beispielsweise DLAN o.ä. benutzen, wenn WLAN nicht zwingend notwendig ist. Dies würde zumindest die Wahrscheinlichkeit verringern, noch einmal gescannt zu werden. Die WLAN-Funktionalität zu deaktivieren kann aber auch verhindern, dass man selbst geortet wird. Um eine personenbezogene Zuordnung zu den erfassten WLAN-Daten zu vermeiden, sollte man keine persönlichen Informationen, wie Name, Adresse o.ä. in seiner SSID aufnehmen. Generell bietet es sich an, die SSID komplett zu unterdrücken. Um weiteren unbefugten Zugriff zu vermeiden, sollte man immer eine WPA2-Verschlüsselung mit sicherem Schlüssel aktivieren und nur den eigenen Geräten per MAC-Filter Zugriff auf den WLAN-Router gewähren.

4.2.3 Weitere Dienste

In diesem Kapitel werden 31 weitere interessante Dienste von Google betrachtet. Wie bereits in der Einleitung erwähnt, sind das dann immer noch längst nicht alle. Hinzu kommen noch andere Dienste rund um Programmierung, Kommunikation, Datenbanken, Suche, Multimedia und Kartenmaterial.

4.2.3.1 Google Analytics

Google-Konto erforderlich: Ja (als Webseiten-Betreiber)

Beschreibung: Mit Google Analytics können Betreiber von Webseiten Daten (IP-Adressen, Verweildauern, besuchte Seiten und vieles mehr) zu ihren Besuchern durch Google erheben lassen, um sie anschließend zu analysieren. Ca. 80% der meistbesuchten deutschen Webseiten sollen im Jahr 2008 Google Analytics eingesetzt haben (Bonstein et al. 2008).

Mehrwert: Google Analytics ist ein sehr mächtiges Tool, das Webmaster kostenlos auf ihren Seiten einbinden können, um Zugriffe von Besuchern zu analysieren. Analytics bietet dazu viele

graphische Statistiken wie z.B. E-Commerce-Berichte und verzeichnet u.a. die Herkunft der Besucher auf einer Landkarte. Im Gegensatz zu anderen, vergleichbaren Tools, bietet Analytics eine Integration von AdWords und AdSense. Damit kann analysiert werden, welche Kampagnen etc. den besten Umsatz generieren. Zudem werden diesbezüglich Optimierungsmaßnahmen angeboten (vgl. Google 2010i).

Risiken: Die Speicherung und Auswertung der Daten findet auf den Servern von Google statt. Analytics erlaubt es Google also, auch Daten von solchen Benutzern zu sammeln, die gar nicht direkt auf Google's Webseiten und Dienste zugreifen, sondern auf solchen anderer Anbieter, die ihrerseits Analytics einsetzen. Das Benutzerverhalten auf diesen Seiten wird also aufgezeichnet und inkl. der IP-Adresse des Besuchers und ggf. Cookie-Daten bei Google gespeichert, ohne dass man dem unmittelbar gewahr wird (vgl. Bonstein et al. 2008). Für Datenschützer ist diese Art der Datenerfassung durch Google „schon per se ohne Einwilligung der Betroffenen nicht möglich" (Kraska 2010a), da es gegen das Telemediengesetz verstößt (vgl. ULD-SH 2010).

Risikoverminderung: Google reagierte auf die massive Kritik der Datenschutzbehörden etc. und stellt seit Mai 2010 das sogenannte „Google Analytics Opt-out Browser Add-on" unter http://tools.google.com/dlpage/gaoptout bereit. Dabei handelt es sich um ein Browser-Plug-in, das für Internet Explorer, Firefox und Google Chrome verfügbar ist. Es unterbindet das Senden von Informationen an Google Analytics, unabhängig davon, welche Webseiten besucht werden. Für die Browser Safari und Opera gibt es ein solches Add-on allerdings nicht. Das Plug-in lädt jedoch jedes Mal ein JavaScript von Google Analytics, das die weitere Datenerhebung unterdrücken soll. Dementsprechend kann Google dennoch erfahren, wer auf welche Webseiten zugreift. Außerdem können Webmaster mittlerweile "IP-Masking" aktivieren. Dabei werden die letzten acht Bit der IP-Adressen aller Besucher vor dem Speichern abgeschnitten. Allerdings handelt es sich hier um Opt-out und ist nicht, wie z.B. bei eTracker die Standardeinstellung (vgl. Braun 2010). Andere Möglichkeiten zur Unterbindung der Datenübertragung an Google bieten das selektive Deaktivieren von JavaScript oder das Unterbinden von Cookies (siehe https://www.datenschutzzentrum.de/tracking/schutz-vor-tracking.html). Diese Maßnahmen wirken zudem nicht nur bei Google Analytics, sondern beziehen sich auch auf ähnliche Tools anderer Anbieter. Für Webseitenbetreiber bieten sich Alternativen zu Google Analytics. Einige davon sind unter dem folgenden Link inkl. Vergleich zu Analytics beschrieben: http://www.gutestun.org/google/17-google-analytics-alternativen/

4.2.3.2 Google Base

Google-Konto erforderlich: Ja

Beschreibung: Bei Google Base handelt es sich um einen Datenbank-Dienst, mit dem auf einfache Weise Online- und Offline-Inhalte aller Art in Form von Artikeln veröffentlicht werden können. Anschließend sind diese Inhalte über Google auffindbar. Offline-Inhalte können hochgeladen werden. Alle Artikel können mit Attributen beschrieben werden, wodurch sie einfacher gefunden werden können. Je nach Relevanz können Artikel auf den Hauptseiten der Google Websuche sowie bei weiteren Suchergebnissen angezeigt werden. Beispiele für Artikeltypen sind „Veranstaltungen und Aktivitäten", „Immobilen" und „Stellenangebote". Darüber hinaus gibt es benutzerspezifische Artikeltypen. Die Attribute *Link* (URL zum Content), *Artikeltitel* und *Artikelbeschreibung* sind Pflichtangaben. Das Merchant Center ist eine Erweiterung von Google Base und dient der Verwaltung von Produkten, die über die Google Produktsuche

gefunden werden können. Produkte sind spezielle Artikel, die von Händlern kommerziell im Internet angeboten werden.

Mehrwert: Mit Google Base kann man so gut wie alles veröffentlichen. Voraussetzung ist, dass die Artikel mit den Google Base Programmrichtlinien übereinstimmen. Außerdem müssen alle in Google Base eingestellten Artikel den geltenden Gesetzen und Vorschriften Ihres Ziellands entsprechen. Per Attribute können Artikel mit beliebigen Metadaten verknüpft werden. Zudem kann man direkt im Online-Dienst einen FTP-Zugang anlegen, um seine Artikel per FTP zu verwalten. Des Weiteren bietet der Dienst eine API, um Inhalte abzufragen und anzuzeigen (vgl. Google 2011a, Google 2011b). Für den normalen Internetnutzer ist dieser Dienst vermutlich eher weniger interessant.

Risiken: Hochgeladene Inhalte aller Art sind fortan mit dem Google-Konto verknüpft. Entweder per Verlinkung oder per Upload ins Google-Konto. Dass die eigene E-Mail-Adresse als Kontakt veröffentlicht wird (sowohl auf Webseiten als auch in der API) ist standardmäßig deaktiviert (Opt-in). Ansonsten wird lediglich auf die allgemeinen Datenschutzbestimmungen von Google verwiesen.

Risikoverminderung: Da man die Inhalte, die man mit dem Google-Konto verknüpft selbst bestimmt, kann man unmittelbar kontrollieren, welche Daten mit dem Konto verknüpft und veröffentlicht werden.

4.2.3.3 Blogger.com

Google-Konto erforderlich: Ja, zumindest wenn man selbst bloggt

Beschreibung: Blogger.com ist ein Google-Dienst, bei dem Autoren eigene Blogs verfassen können. Andere Nutzer des Dienstes können Einträge der Blogs kommentieren, bewerten etc. Bei Blogger.com erhält der Autor eine eigene Webseite, auf der er nun chronologisch beliebige Posts veröffentlichen kann. Die Webseite zum Blog aus den eigenen Untersuchungen lautet http://datenschutz2010.blogspot.com

Mehrwert: Auf den ersten Blick handelt es sich bei Blogger.com lediglich um einen guten Blogger. Bei etwas genauerer Betrachtung zeichnet sich der Blogger von Google durch folgende Merkmale aus (vgl. Tikoim 2010, Google 2011c):

- Schnell auffindbar in der Google-Suche (Indizierung nach wenigen Minuten)
- Templates, die sich leicht bearbeiten lassen (WYSIWYG)
- Bearbeitung des Blogs auch auf Basis von HTML/CSS möglich
- Unterstützung eigener Domains
- Kopplung von AdSense, wodurch Google-Anzeigen im Blog geschaltet werden können
- Die Integration von Bildern und Videos ist inkl. Hosting ebenfalls möglich
- Blogger Mobile: Per Email, SMS und MMS können Posts von mobilen Endgeräten veröffentlicht werde.

Risiken: Bewusst veröffentlichte Inhalte wie eigene Posts, Bilder oder auch Kommentare werden im Google-Konto gespeichert. Außerdem kann, wie bei vielen Diensten, ein eigenes Profil erstellt

und veröffentlicht werden. Bei der Verwendung von Blogger Mobile wird die Handynummer mit dem Google-Konto verknüpft, sofern man einen Post per SMS oder MMS absendet.

Risikoverminderung: Man sollte keine sensiblen Inhalte veröffentlichen und das Profil nicht unnötig mit persönlichen Daten anreichern. Abbildung 6 zeigt die Optionen, die man bzgl. des Datenschutzes hat und zwar in ihrer Voreinstellung. Hier empfiehlt es sich, verfolgte Webseiten nicht zu veröffentlichen oder das Profil erst gar nicht freizugeben. Möchte man andere Blogs abonnieren, macht man dies im Normalfall öffentlich, man ist also für alle Nutzer als Abonnent sichtbar. Es besteht allerdings die Möglichkeit, dies auch anonym zu machen. Der entsprechende Dialog erscheint beim Abonnieren eines Blogs. Wenn man vom Handy Beiträge posten möchte, sollte man dies per E-Mail oder direkt im Browser machen, da ansonsten die Handynummer gespeichert wird (vgl. Google 2011d).

Abbildung 6: Datenschutzoptionen bei Blogger.com

4.2.3.4 Google Books

Google-Konto erforderlich: Nein, außer wenn man sich ein eigenes Verzeichnis im Sinne einer Favoritenliste anlegen möchte.

Beschreibung: Google Books bietet eine Online-Volltextsuche in digitalisierten Büchern. Die entsprechende Bücherdatenbank setzt sich aus zwei Quellen zusammen: Auf der einen Seite aus dem Partnerprogramm, einem Kooperationsprojekt von Google mit Verlagen und Autoren, bei dem die Verlage Google gedruckte oder digitalisierte Bücher zukommen lassen. Auf der anderen Seite stammen sie aus dem Bibliotheksprogramm, einer Zusammenarbeit mit großen Bibliotheken, deren Buchsammlungen massenweise eingescannt werden. Bei letzterer Bezugsquelle werden nicht nur urheberrechtsfreie Bücher erfasst (vgl. Google 2010j). Schaut man sich Bücher bei Google Books an, findet man in der Navigation Möglichkeiten, um das Buch bei diversen Anbietern zu kaufen oder sich Buchhändler in seiner Umgebung anzeigen zu lassen. Dies ist einer von mehreren Kompromissen aus dem Partnerprogramm mit den Verlagen und Autoren.

Mehrwert: Auch wenn die urheberrechtsfreien Werke komplett durchsucht und gelesen werden können, so sind bei urheberrechtlich geschützten Werken oft nur bestimmte Ausschnitte kostenlos verfügbar. Dennoch: Google Books bietet einem nicht nur die Volltextsuche in Büchern, sondern eine gute Möglichkeit, vor einer Kaufabsicht in Bücher zu schauen, um Fehlkäufe zu vermeiden. Zumindest das Inhaltsverzeichnis des Buches ist (fast) immer sichtbar.

Oft findet man aber auch genau die Passagen online, die man benötigt. Neben dem Zugriff auf urheberrechtsfreie Werke gibt es einen weiteren positiven Aspekt: Mit Google Books gibt es erstmals eine Lösung für das Problem der „verwaisten" Bücher. „Dabei handelt es sich um Bücher, deren Urheberrechtsfrist noch nicht abgelaufen ist, die jedoch im Handel nicht mehr verfügbar sind, deren Autoren und Erben als unauffindbar gelten oder deren Verlage nicht mehr existieren. […] Schätzungsweise 70% der sieben Millionen Titel, die bereits bei Google Books abrufbar sind, sind nicht mehr im Handel erhältlich" (Cloes/Schappert 2009).

Risiken: Google speichert alle Suchanfragen bei der Buchsuche (genau wie bei der Websuche) und zusätzlich die Bücher, die man sich letztlich angeschaut hat und verknüpft sie mit dem Google-Konto. Dies ist jedoch nur der Fall, wenn man angemeldet ist und die Webhistorie aktiviert hat (siehe Abbildung 7). Probleme ergeben sich außerdem für Urheber von gescannten Werken. Verleger, Autoren, Fotografen und Zeichner werfen Google vor, mit seinem Buchangebot von ihnen geschaffene Inhalte ungefragt zu nutzen – und klagen (Pluta 2010a). Urheberrechtliche Probleme sollen im Rahmen dieser Ausarbeitung jedoch nicht näher betrachtet werden.

Risikoverminderung: Wenn man Bücher sucht und anschaut, sollte man darauf achten, nicht mit seinem Google-Konto angemeldet zu sein. Dann wird die Historie nämlich erst gar nicht mit dem Google-Konto verknüpft, sei es im Kontext der Webhistorie oder vielleicht anders.

Abbildung 7: Webhistorie für Google Books

4.2.3.5 Google Buzz

Google-Konto erforderlich: Ja

Beschreibung: Google Buzz ist ein soziales Netzwerk, das in Gmail integriert ist und prinzipiell mit einer einfachen Formel verdeutlicht werden kann: Google Buzz = Gmail + Facebook + Twitter + Flickr (vgl. Lemm 2010, Steinlein 2010). Mit Orkut (siehe Kapitel 4.2.3.20) ist Google im Besitz eines weiteren sozialen Netzwerks, das vor allem in Indien und Brasilien populär ist. Eine deutschsprachige Version ist ebenfalls verfügbar.

Mehrwert: Auch wenn obige Formel darauf hindeuten könnte, dass Google Buzz ja viel mehr kann als andere soziale Netzwerke, ist dies nicht unbedingt der Fall. Laut herrschender Meinung hat Google Buzz keine signifikanten Vorteile gegenüber anderen sozialen Netzwerken. Außer

vielleicht, dass die Gmail-Kontakte direkt integriert sind, was aber nicht unbedingt ein Vorteil sein muss.

Risiken: In der Vergangenheit tauchten immer wieder datenschutzrechtliche Probleme bei Buzz auf. Darauf soll jedoch an dieser Stelle nicht detailliert eingegangen werden, da sich seither vieles geändert hat. Zum Beispiel wurden Kontaktdaten aus Gmail veröffentlicht, indem sie automatisch mit den Kontakten anderer Nutzer verknüpft wurden. Außerdem waren die Kontakte mit denen man am häufigsten über sein Konto kommuniziert, abrufbar. Bekanntestes Opfer ist wohl Andrew McLaughlin, Barack Obamas Beauftragter für Internetpolitik: Ende März 2010 war bekannt bekanntgeworden, mit wem er am häufigsten über sein Gmail-Konto korrespondiert hat (vgl. Lemm 2010, Pluta 2010b). Am 06. April 2010 reagierte Google mit einem Datenschutz-Reset auf die wachsende Kritik am Umgang mit privaten Informationen bei Buzz. Seitdem wurden alle Nutzer automatisch aufgefordert, ihre Privatsphäre-Einstellungen zu bestätigen oder gegebenenfalls anzupassen (vgl. N-TV 2010). Seitdem ist es zumindest ruhig geworden um Google Buzz. Wichtig ist jedoch, dass grundsätzlich alle persönlichen Daten, die man in Google Buzz preisgibt sowie auch die sozialen Kontakte, unmittelbar mit dem Google Konto verknüpft sind.

Risikoverminderung: Damit nicht auch noch persönliche bzw. soziale Informationen wie z.B. Fotos, Kontakte, Konversationen etc. mit dem Google-Konto verknüpft werden, sollte man Google Buzz deaktivieren (in den Gmail-Einstellungen möglich), zumal es viele, zumindest gleichwertige, soziale Netzwerke gibt.

4.2.3.6 Google Checkout

Google-Konto erforderlich: Ja

Beschreibung: Bei Google Checkout handelt es sich um ein elektronisches Bezahlverfahren.

Mehrwert: Google Checkout ist das bislang fehlende Glied in der Google-Kette von Suchen, Finden und Kaufen. Es gibt zwar genügend andere elektronische Bezahlverfahren, interessant wäre aber vielleicht, dass man sich nur noch einmal anmelden muss, nämlich mit dem Google-Konto. Viel günstiger als andere ist dieses Bezahlverfahren auf jeden Fall nicht. Die Kosten pro Transaktion betragen bei Google 2 Prozent vom Umsatz zzgl. 0,20 Euro. PayPal verlangt 1,9 Prozent vom Umsatz und 0,30 Euro Pauschale (vgl. Büttner 2010).

Risiken: Zum einen wird das Google-Konto fortan mit persönlichen Informationen verknüpft, die Google für die Nutzung von Checkout voraussetzt: Tatsächlicher Vor- und Nachname, Nummer der Kreditkarte (inkl. Ablaufdatum und Kartenprüfnummer) bzw. die Bankverbindung, die Adresse, die Telefonnummer und die E-Mail-Adresse. Sollte beim Anmelden bei Checkout noch kein Google-Konto existieren, wird es automatisch angelegt. Neben den gerade genannten Daten werden außerdem noch transaktionsbezogene Daten gespeichert: Der Transaktionsbetrag, eine Beschreibung der Ware oder der Dienstleistung (legt der Verkäufer fest), die Namen von Käufer und Verkäufer und die verwendete Zahlungsart. Ferner werden gesammelt: Informationen über die Interaktion mit dem Dienst sowie die IP-Adresse mit Zeitangaben zu den einzelnen Webanfragen und die Browseridentifikation (vgl. Google 2010k, Google 2010l, Google 2010m).

Risikoverminderung: Aufgrund der vielen persönlichen Informationen, die sich hier, ohne Opt-out, beim Google-Konto anhäufen, ist vom Gebrauch von Google Checkout dringendst abzuraten. Momentan ist ein wirklicher Mehrwert nämlich weder vorhanden, noch absehbar. Man kann nur hoffen, dass man als Käufer nicht irgendwann von diesem Bezahlverfahren abhängig wird. Noch ist dies nicht der Fall, jedenfalls nicht im herkömmlichen Internet. Im mobilen Internet hingegen versucht Google seine gute Ausgangsposition mit Android zu nutzen, um die Verbreitung von Checkout voranzutreiben. So ist Checkout z.B. das einzige zugelassene Zahlungsmittel für den Android Market (Lanzerath 2010).

4.2.3.7 Google Chrome

Google-Konto erforderlich: Nein

Beschreibung: Chrome ist Google's eigener Internet-Browser, der Google die Möglichkeit bietet, Daten von Internetnutzern zu erheben, auch wenn diese gar nicht auf Google's Webseiten surfen. Diese Möglichkeit ist wohl ein wichtiger Grund, weshalb Google mit Chrome bis direkt zur Einstiegsstelle ins Internet vordringt, obwohl man doch jahrelang behauptet hatte, man sei an diesem Geschäft nicht interessiert. Auch in Google's Anwendungspaket „Google Pack" wird fortan nicht mehr Firefox, sondern Google Chrome als Standardbrowser ausgeliefert (vgl. Brandt 2010: 19f). Diese Untersuchung bezieht sich ausschließlich auf Google Chrome als Internet-Browser, also aus Sicht eines konventionellen Internetnutzers. Dass Google Chrome vielmehr als nur ein herkömmlicher Webbrowser ist bzw. sein soll, zeigt Kapitel 4.2.4. Dort werden Google Chrome sowie das Betriebssystem Google Chrome OS als „Cloud-Clients" betrachtet, also als „Eingangstor in die Welt des Cloud Computing".

Mehrwert: Chrome ist ein Browser, der durchaus mit anderen Produkten wie dem Internet Explorer oder Firefox mithalten kann. Wesentliche Vorteile gegenüber den Anderen ergeben sich bei der Nutzung allerdings nicht und sind wohl nur im Detail zu finden (wie z.B. die direkte Suche über die URL-Leiste). Natürlich wirbt Google damit, schneller und nutzerfreundlicher als andere Browser zu sein, selbige werben aber mit den gleichen „Versprechungen".

Risiken: Wie schon angedeutet, sendet Chrome Nutzerdaten an Google. Dazu gehören in die Adressleiste eingegebene URLs oder Suchanfragen, und zwar von der Eingabe des ersten Zeichens des entsprechenden Suchbegriffs bzw. der URL (wegen der Auto-Suggest-Funktion), bis zum Absenden der Anfrage. Auch Nutzungsstatistiken (z.B. Informationen zu den Browser-Einstellungen, den Klicks auf Schaltflächen oder zur Speicherauslastung) werden an Google gesendet. Bei Aktivierung der Synchronisierungsfunktion (Opt-in) werden Browsereinstellungs-informationen (z. B. Lesezeichen) mit dem Google-Konto verknüpft und auf Google-Servern gespeichert (vgl. Google 2010n). Kritisiert wird auch die technische Möglichkeit, dass alle von Chrome erfassten Daten über die eindeutige Chrome-ID mit dem Google-Konto verknüpft werden könnten (vgl. Kraska 2008a). Allgemeine Risiken, die auch bei anderen Browsern bestehen, wie z.B. ein Tracking auf Basis von Cookies, sollen hier nicht weiter betrachtet werden.

Risikoverminderung: Wie beim Mehrwert schon angedeutet, gibt es im Grunde genommen keinen guten, objektiven Grund, Google Chrome zu verwenden. Als Alternativen bieten sich neben Firefox und Internet Explorer z.B. auch Safari oder Opera an. Möchte man Google Chrome aus subjektiven Gründen dennoch einsetzen, sollte man das Senden von bestimmten Daten an Google durch entsprechende Einstellungen unterbinden. Hinweise, wie das Übertragen

bestimmter Daten (z.B. Nutzerstatistiken) an Google deaktiviert werden kann, sind in der Anmerkung zum Datenschutz im Abschnitt „Informationen, die bei der Verwendung von Google Chrome an Google gesendet werden“ zu finden. Folglich gilt auch hier wieder das Opt-out-Prinzip (vgl. Google 2010n).

> *Für mich verbleibt die Frage, warum ich diesen Browser nutzen sollte: Schneller als Safari ist er nicht, der Unterschied zu einem ordentlich konfigurierten FF/Opera bei mir nur marginal. Also warum nutzen und Google schon wieder kostenlos unterstützen? Hier ist (Unique-ID die ausgelesen werden kann zusammen mit dem Blick in die Googlisierte Welt) auch meine Hauptkritik – die Punkte wie Suggest & Co. mögen noch dazu kommen, aber jedenfalls jetzt kann man sie ja deaktivieren.* (Kraska 2008a)

4.2.3.8 Google Code

Google-Konto erforderlich: Je nach Funktion

Beschreibung: Google Code ist ein Portal mit Open-Source-Software und Entwicklertools wie z.B. das Google Web Toolkit, einem Framework zur Entwicklung von Ajax-basierten Webanwendungen und eine Versionskontrolle (Subversion). In diesem Portal liegen (fast) alle Anwendungen und APIs rund um Google. Das Portal ist allerdings nicht deutschsprachig. Die App Engine ist die „Cloud-Plattform“ von Google und ermöglicht es Entwicklern, automatisch skalierbare Projekte auf den Servern von Google zu hosten und ist bei gewissen Beschränkungen bzgl. der Ressourcen kostenlos.

Mehrwert: Google Code ist eine nette Ergänzung zu weiteren Open-Source-Plattformen wie z.B. SourceForge. So begrüßte Jay Seirmarco, Chef von SourceForge, das Angebot von Google Code mit den Worten: "Was gut für die Open-Source-Gemeinschaft ist, ist auch gut für SourceForge." Dies bestätigte Greg Stein, technischer Leiter bei Google, mit dem Hinweis, dass beide Firmen an einer gemeinsamen Datenbank für Open-Source-Projektnamen arbeiten, um Verwirrungen und Duplikate zu vermeiden (Jäger 2006).

Risiken: Hier besteht m.E. kein Risiko, denn bei der Software auf dieser Plattform handelt es sich ausschließlich um Open-Source-Software. Lädt man beispielsweise ein Projekt auf Google Code hoch (z.B. weil man die Versionskontrolle nutzen will), so muss man zustimmen, dass es sich bei dem Projekt ausschließlich um Open-Source-Software handelt. Daher kann eine Betrachtung bzgl. des Datenschutzes und des Urheberrechts entfallen. Zu erwähnen wäre vielleicht noch, dass gehostete Projekte etc. natürlich mit dem Google-Konto verknüpft sind. Suchanfragen, z.B. bei der Suche nach Projekten, werden zumindest in der Webhistorie nicht erfasst.

Risikoverminderung: Entfällt

4.2.3.9 Google Desktop und Gadgets

Google-Konto erforderlich: Nein

Beschreibung: Google Desktop besteht im Wesentlichen aus einer Desktop-Suche, einer Websuche und den Google Gadgets. Bei der Desktop-Suche werden Dateien (z.B. Dokumente, E-Mails, Musik, Fotos, aber auch Chats (z.B. bei MSN und AOL Instant Messenger) und Webhistorien (z.B. beim Firefox und Internet Explorer) auf dem Computer indiziert, um eine

schnelle Suche nach ihnen zu ermöglichen. Bei der Websuche öffnet sich nur der Standardbrowser mit der normalen Suchmaschine und den entsprechenden Suchergebnissen. Google Gadgets sind Mini-Anwendungen von Google oder Drittanbietern, die auf dem Google Desktop angezeigt werden können (siehe Abbildung 8). Diese dienen z.B. zur Anzeige neuer E-Mails, Informationen zum Wetter, Fotos und personalisierter News.

Mehrwert: Die Websuche stellt keinen echten Mehrwert dar, nur dass hier ein etwas schnellerer Zugriff auf Suchergebnisse erfolgen kann. Die Desktop-Suche könnte interessanter sein als die normale Windows-Suche, da E-Mails z.B. aus Thunderbird (während Thunderbird gestartet ist, werden die E-Mails indiziert) und Chat-Verläufe integriert werden. Außerdem gibt es sehr viele, zum Teil auch interessante Gadgets wie z.B. eine integrierte Wikipedia-Suche.

Risiken: Der Desktop-Index und Dateikopien werden nur auf dem lokalen Computer gespeichert und nicht an Google übermittelt (vgl. Google 2010o). Bei der Websuche werden natürlich die gleichen Daten erhoben, die auch bei der normalen Websuche erhoben werden (siehe Abschnitt 4.2.3.30). Gadgets sind aus datenschutzrechtlicher Sicht relativ uninteressant, da eingegebene Daten anscheinend, im Gegensatz zu den Gadgets bei iGoogle, nur lokal gespeichert werden. Ansonsten müsste man sich ja mit seinem Google-Konto anmelden, um einen Bezug herzustellen, was hier jedoch nicht der Fall ist. Kommen die Gadgets von Drittanbietern, gilt es, deren Datenschutzbestimmungen zu beachten (vgl. Google 2010p). Außerdem weist Google beim Hinzufügen vieler solcher Gadgets darauf hin, dass diese nicht von Google getestet wurden und dass deshalb Sicherheitsrisiken bestehen.

Risikoverminderung: Man sollte immer die Sicherheitsrisiken und Datenschutzbestimmungen bei Gadgets von Drittanbietern beachten. Ansonsten sollte man aufpassen, dass Google Desktop nicht mit dem Google-Konto verknüpft wird, sofern dies überhaupt möglich ist. Ein entsprechendes Gadget, das ein Google-Konto voraussetzt, konnte (auf die Schnelle) nicht gefunden werden.

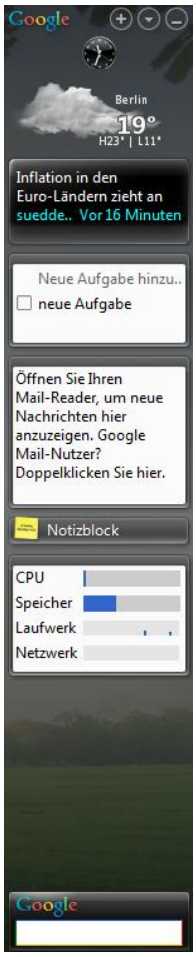


Abbildung 8: Google Desktop

4.2.3.10 Google Earth

Google-Konto erforderlich: Nein

Beschreibung: Google Earth ist ein herunterladbares Tool, das Satellitenbilder der Erdoberfläche in 3D liefert und auf Google Maps basiert. Außerdem kann man nach Orten von Interesse suchen und den integrierten Routenplaner nutzen. Von Google Earth gibt es auch kostenpflichtige Versionen, die weitere Funktionalitäten bieten, wie z.B. höhere Auflösungen beim Druck, GPS-Integration etc. Solche Versionen können z.B. für Unternehmen sehr interessant sein. Google Earth bietet zudem noch eine sehr abgespeckte Version von Street View. So kann man sich an einigen Orten Rundumansichten anschauen, die im Gegensatz zum echten Street View recht statisch wirken, denn man kann sich nicht dynamisch fortbewegen, sondern nur zur nächsten Rundumansicht springen. In Ballungsräumen wie z.B. New York ist eine solche statische Rundumansicht allerdings ca. alle fünf Meter verfügbar. Diese Aussagen bezogen sich auf Version 5; seit Version 6, die im November 2010 veröffentlicht wurde, ist Street View vollständig integriert (siehe Abbildung 9).

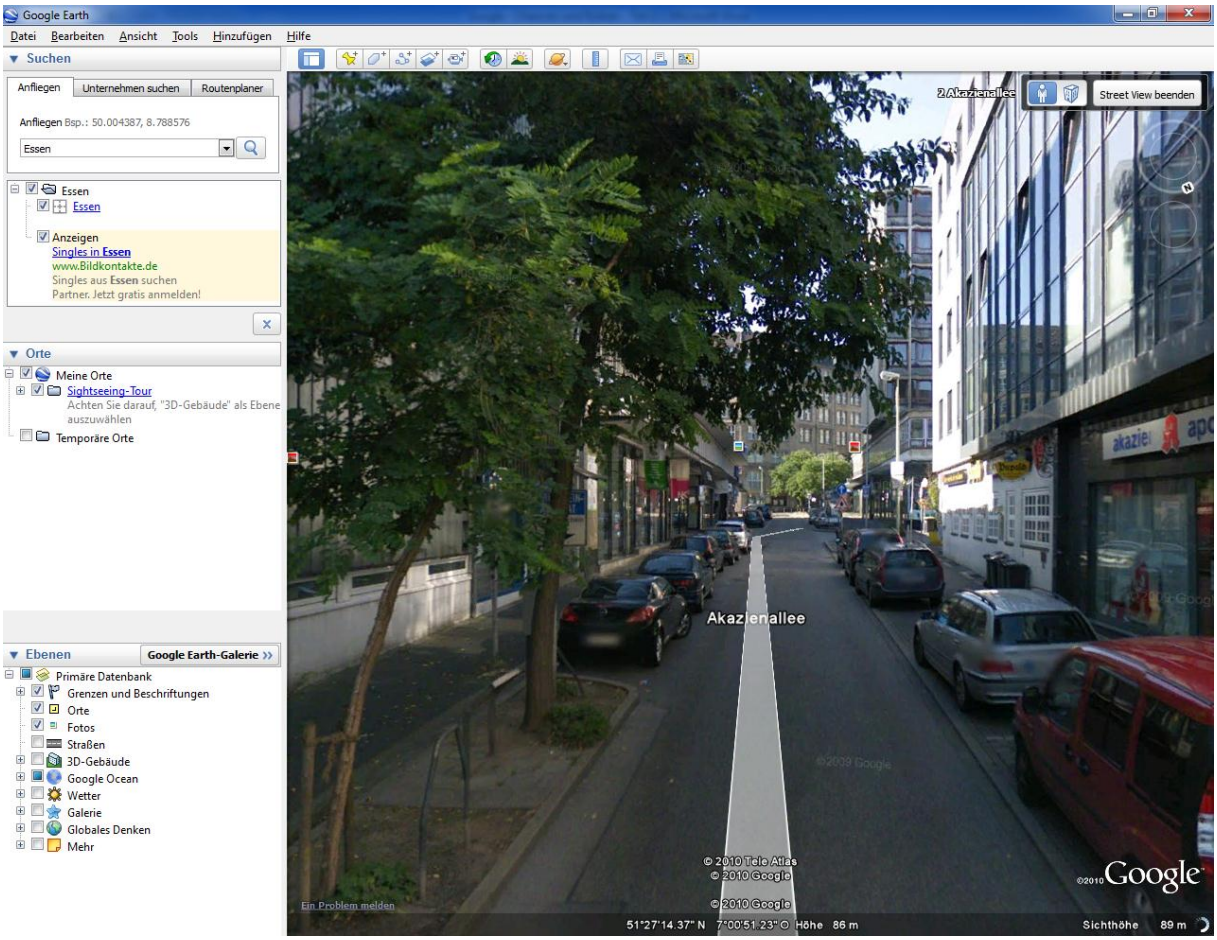


Abbildung 9: Integration von Street View in Google Earth 6

Mehrwert: Dieses Tool bietet m.E. für den Ottonormalverbraucher keinen echten Mehrwert. Es gibt viele andere Routenplaner und Karten. Alleine Google Maps, das komplett online verfügbar ist, ist m.E. deutlich einfacher zu bedienen und bietet mehr Funktionalitäten. Ausgenommen sind hier natürlich die Enterprise-Features der kostenpflichtigen Versionen von Google Earth oder die 3D-Ansichten der Erdoberfläche und dass man GPS-Daten aus einigen, wenigen GPS-Geräten importieren kann.

Risiken: Begonnen werden soll die Betrachtung der Risiken mit einem Satz, wie er auf der Google Earth Datenschutzseite zu finden ist: „Google Earth enthält nur Daten, die über kommerzielle und öffentliche Quellen verfügbar sind. Dieselben Informationen sind beispielsweise für jeden erhältlich, der ein Grundstück überfliegt oder daran vorbeifährt“ (Google 2010q). Es macht aber eben doch einen großen Unterschied, ob man z.B. nackte Menschen (die sich tatsächlich auf Google Earth auf ihren Balkonen oder Gärten wiederfanden, vgl. Stern Online 2010) weltweit auf Karten im Internet sehen kann, oder ob einzelne „Tiefflieger“, was in der Regel sehr unwahrscheinlich ist, diese Menschen sehen. Weitere Risiken sind in Kapitel 4.2.2 bzgl. der Debatte zum Datenschutz und zur Privatsphäre bei Street View zu finden. Auch dort macht es nämlich doch ein riesen Unterschied, ob jeder, der durch die Straßen fährt, die gleichen Fotos aufnehmen und die gleichen WLAN-Daten erfassen könnte, oder ob einer (Google) alle Daten erfasst und über das Internet verfügbar macht. Zudem erhebt Google Earth Nutzungsstatistiken (z.B. welche Funktionalitäten wie oft verwendet werden), diese Option kann jedoch deaktiviert werden (Opt-out).

Risikoverminderung: Wie schon angedeutet, gibt es viele Alternativen zu Google Earth. Selbst das hauseigene Google Maps ist hier für einfache Zwecke eine bessere Wahl und man muss sich kein Tool herunterladen und installieren. Verwendet man Google Earth dennoch, dann sollte man vorsichthalber die Option zum Übertragen der Nutzungsstatistiken deaktivieren, da nicht klar definiert ist, welche Daten genau übermittelt werden (vgl. Google 2010r).

4.2.3.11 Google Finanzen

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: Google Finanzen ist das Finanzportal von Google (vgl. Abbildung 10). Bis jetzt ist es in den USA, in Canada, in China und in Großbritannien verfügbar. Der Dienst bietet Übersichten, Detailinformationen und News zu Finanzmärkten. Wenn man mit dem Google-Konto angemeldet ist, kann man eigene Portfolios verwalten. Solche Portfolios erlauben u.a. die Zusammenstellung eigener Aktien in bestimmten Stückzahlen sowie auch eine Verwaltung von Transaktionen. Wenn man also z.B. 1000 Google-Aktien besitzt und sich weiter 500 dazu kauft, kann man alle relevanten Informationen im Portfolio hinterlegen.

Abbildung 10: Google Finanzen

Mehrwert: Der Dienst von Google hat offensichtlich keine signifikanten Vorteile gegenüber anderen Finanzportalen, außer vielleicht die dynamischen Auswertungsmöglichkeiten, die sehr umfangreich sind. So kann man sich z.B. Trends zu bestimmten Branchen anzeigen lassen oder eigene Kriterien bei der Auswertung mit einfließen lassen. Finanzen.net, das Finanzportal des Axel Springer Verlags, ist insgesamt allerdings deutlich umfangreicher und scheint ausgereifter. Außerdem gibt es von Google Finanzen keine deutschsprachige Version und vermutlich umfasst der Dienst deshalb die deutschen Finanzmärkte ziemlich unvollständig.

Risiken: Beim Durchsuchen von Finanzmärkten ergeben sich die gleichen Risiken wie bei anderen Google-Suchen auch. Wenn man eigene Portfolios mit Google Finanzen verwaltet, werden entsprechende Daten im Google-Konto gespeichert. Abbildung 11 zeigt den

Portfoliowert im Dashboard. Wie sensibel personenbezogene Finanzdaten sind, erkennt auch Google und vermerkt daher auf der Login-Seite folgendes:

> *Security Note: Since Google Finance Portfolios involves your personal financial information, we'll sometimes take extra care to protect you by asking you to verify your password even though you're already signed in.*

Risikoverminderung: Wenn man eigene Portfolios verwalten möchte, sollte man auf einen alternativen Dienst ausweichen, damit die eigenen Finanzdaten nicht mit dem Google-Konto verknüpft werden. Auch andere Dienste, wie das bereits genannte Portal Finanzen.net bieten diesbezüglich umfangreiche Möglichkeiten.

Abbildung 11: Das Finanzportfolio im Google Dashboard

4.2.3.12 Google Flu Trends

Google-Konto erforderlich: Nein

Beschreibung: Google Flu Trends ist ein Frühwarnsystem für Grippe-Wellen. Vorhersagen von weltweiten Grippe-Wellen werden anhand der Häufigkeit der Suchbegriffe, die bei der Google-Websuche eingegeben werden, getätigt.

Mehrwert: Dass die Eingabe von Begriffen rund um Grippen bei der Google-Websuche tatsächlich ein Indiz für drohende Grippewellen sein kann, zeigt auch, dass Google die Sieger der Schlager Grand Prix der letzten beiden Jahre durch sehr ähnliche Analysen korrekt vorausgesagt hat. Google behauptet ca. zwei Wochen schneller zu sein als die Gesundheitsbehörden mit ihren entsprechenden Veröffentlichungen (Zeuch 2009).

Risiken: Bei Flu Trends handelt es sich nur um ein Beispiel, wie Google Suchanfragen verwerten kann. Wie aussagekräftig so etwas hingegen ist, ist sehr umstritten. Grund dafür ist, dass letztlich nicht jeder, der z.B. „Grippe" eingibt, auch eine Grippe hat. Oder: Nicht jeder, der nach „Lena (Meyer-Landrut)" oder „Alexander Rybak" sucht, nimmt auch an der Abstimmung des Schlager Grand Prix Teil und stimmt dann noch für genau diesen Kandidaten. Auch wenn die Vorhersagen verblüffende Ergebnisse liefern, handelt es sich hier nur um nette Indizien, auf die man sich keineswegs verlassen sollte. Denn wie Google selbst sagt, handelt es sich lediglich um Schätzungen (vgl. Valdivia et al. 2010).

> *Im Gegensatz zu Google analysieren wir wissenschaftlich, ob wirklich eine Grippewelle naht oder nicht.* (Susanne Glasmachner vom Robert Koch-Institut nach Zeuch 2009)

Risikoverminderung: Entfällt, da lediglich ein lesender Zugriff auf die aktuellen Grippedaten erfolgt.

4.2.3.13 Google Groups

Google-Konto erforderlich: Ja, zumindest wenn man aktiv mitmacht

Beschreibung: Google Groups enthält ein Usenet-Archiv mit diversen Diskussionsgruppen, die seit 1981 existieren. Über eine Suche können so Gruppen gefunden werden, an denen man sich beteiligen kann. Neben dieser Suche im anbieterübergreifenden Usenet-Archiv bietet der Dienst selbst ein Usenet, ermöglichst also auch das Erstellen und Verwalten von Gruppen. Eine solche Gruppe besteht aus Online-Diskussionen und bietet Mailinglisten-Funktionalitäten. Teilnehmer einer Gruppe können so per Internet über bestimmte Themen diskutieren. Alle Inhalte einer Gruppe werden von Google gespeichert und für die Suche im Web verfügbar gemacht (vgl. Google 2011e).

Mehrwert: Gruppen können öffentlich sein oder mit eingeschränkten Zugriffsrechten konfiguriert werden. Das geht soweit, dass Gruppen privat sein können indem Mitglieder explizit eingeladen werden müssen. Alle anderen Benutzer haben keinen Zugriff auf diese Gruppe und die Inhalte erscheinen weder in den öffentlichen Google-Suchergebnissen noch im Verzeichnis. Insgesamt ergeben sich bis auf das anbieterübergreifende Usenet-Archiv aber wenige Vorteile gegenüber privaten oder öffentlichen Diskussionsforen. Wenn man allerdings mal eben schnell eine Online-Diskussionsgruppe gründen will, kann der Dienst schon von Vorteil sein. Diesbezüglich gibt es jedoch auch alternative Angebote.

Risiken: Inhalte sind entweder öffentlich zugänglich oder zumindest innerhalb der Gruppe sichtbar. Eigene Beiträge können nicht anonym, sondern nur nach einer Anmeldung beim Google-Konto verfasst werden. Dementsprechend laufen die eigenen Diskussionsbeiträge hier zusammen. Außerdem kann ein zusätzliches Profil um persönliche Informationen ergänzt werden. Außerdem sammelt Google diverse weitere Daten:

> *Google sammelt und verwaltet Informationen zu Ihrer Kontoaktivität, wie beispielsweise die Gruppen, denen Sie beitreten oder die Sie verwalten, Listen mit anderen Mitgliedern oder den zu einer Gruppe eingeladenen Personen, Nachrichten oder Themen, die Sie verfolgen, benutzerdefinierte Seiten, die Sie erstellen oder bearbeiten, Bewertungen, die Sie abgeben, sowie Ihre bevorzugten Einstellungen bei der Verwendung von Google Groups* (Google 2011f).

Risikoverminderung: Wie bei der Mehrwert-Betrachtung schon angedeutet, bieten sich sowohl für private als auch für öffentliche Diskussionsgruppen diverse Foren anderer Anbieter an und für die Suche im Usenet-Archiv benötigt man kein Google-Konto.

4.2.3.14 Google Health

Google-Konto erforderlich: Ja

Beschreibung: Google Health ist eine Gesundheitsplattform, auf der u.a. elektronische Patientenakten abgelegt werden können. Nutzer haben die Möglichkeit, Informationen über ihren allgemeinen Gesundheitszustand, Allergien, Laborergebnisse und aktuelle Medikationen bei Google Health abzulegen, um sie für mögliche Notfälle oder Arztbesuche verfügbar zu machen. Die Plattform nutzt diese Informationen, um ein Gesundheitsprofil des Nutzers zu erstellen und Hinweise über mögliche Unverträglichkeiten und Risiken zusammenzustellen. Im Zentrum der Bemühungen steht also die Verknüpfung verschiedener medizinischer Informationen mit dem

Ziel des informierten und mündigen Patienten. Es geht um personalisierte Medizin. Die notwendige Grundlage dafür ist die Verfügbarkeit des individuellen genetischen Codes eines jeden Patienten, der dann in der elektronischen Patientenakte abgelegt werden soll. Das sind immense Datenmengen, so benötigt ein genetischer Code ca. 750 MB Speicherplatz. Da ist es nicht verwunderlich, dass in den nächsten Jahren rund ein Drittel aller elektronisch erfassten Informationen medizinische Daten sein sollen. Es geht um die Nutzung der technischen Möglichkeiten für die prädikative Analytik durch das Zusammenführen und Auswerten von Unmengen an gesundheitlichen Daten. Der Dienst Google Health ist momentan nur in den USA verfügbar (vgl. SGZ 2008, Kaumanns/Siegenheim 2009: 313ff).

Mehrwert: Google und Anbieter ähnlicher Plattformen sorgen für eine Machtverschiebung und bessere Kontrolle der Patienten über Informationen und Entscheidungen bzgl. ihrer Gesundheit. Dies ist grundsätzlich zu begrüßen. „Google versucht im Fahrwasser der Veränderungen die Position eines Informationsvermittlers zu besetzen, die es vorher in dieser Form im Gesundheitswesen nicht gab." (Kaumanns/Siegenheim 2009: 324). Außerdem bringen die Analyse und die Auswertung immenser zusammenhängender Gesundheitsdaten ganz neue Erkenntnisse und Möglichkeiten für die Medizin.

Risiken: Das Google-Konto wird von nun an mit sensibelsten Gesundheitsdaten einzelner Personen verknüpft. Auch wenn Google versichert, dass die Daten bei ihnen mindestens so sicher seien wie beim bisherigen Gesundheitssystem auch, so unterliegen sie dort nicht den Gesundheitsdatenschutzgesetzen und zumindest Google als wirtschaftliches Unternehmen ist nun im Besitz dieser Daten.

> *Obwohl Microsoft wie auch Google versichern, dass die persönlichen Daten bei ihnen gut aufgehoben sind, erheben Kritiker starke Bedenken. Sie fürchten, dass interessierte Parteien wie Versicherungen und Arbeitgeber Wege finden werden, an sensible Gesundheitsdaten zu gelangen. Die Kritiker warnen zudem davor, dass die Suchmaschinenbetreiber nicht den Gesundheitsdatenschutzgesetzen unterliegen, geschädigte Personen somit kaum Regressmöglichkeiten hätten.* (Pieper 2008)

Risikoverminderung: Zu diesem Zeitpunkt ist eine mögliche Risikoverminderung nur schwer absehbar, da diese Thematik, zumindest in Deutschland, noch nicht wirklich angekommen ist. In der EU und in Deutschland gelten auch wieder andere Gesetze als in den USA. Hier muss man einfach mal abwarten, wie sich die Thematik in den USA entwickelt und ob es so etwas in Deutschland in dieser Form auch geben wird. Das Thema sollte hier nur kurz angerissen werden, es ist viel zu komplex und umfangreich, um an dieser Stelle ausführlich darauf einzugehen. Außerdem existieren ähnliche Plattformen, wie z.B. Microsoft's Health Vault. Hier hat der Wettbewerb um die Marktherrschaft gerade erst begonnen.

4.2.3.15 iGoogle

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: Bei iGoogle handelt es sich um eine personalisierte Google-Startseite, mit der die Suchmaschinenseite auf die eigenen Informationsbedürfnisse zugeschnitten werden kann, unabhängig vom Internetzugang. Neben der Websuche ist Gmail integriert und es sind eine Menge Gadgets (siehe Google Desktop) verfügbar, die der persönlichen Startseite angeheftet werden können. Eine Version für mobile Geräte ist ebenfalls verfügbar.

Mehrwert: Man erhält eine personalisierte Startseite mit allen benutzerspezifischen Informationen, auf die zentral und somit schnell zugegriffen werden kann, und zwar unabhängig vom Zugriffsort. Es gibt einige Alternativen von anderen Anbietern, wobei das Angebot der Gadgets in iGoogle vermutlich das umfangreichste ist. Ob iGoogle jetzt einen echten Mehrwert bietet, oder es doch nur Spielerei ist, sollte jeder für sich selbst entscheiden.

Risiken: Verwendet man iGoogle mit dem Google-Konto, so sind sämtliche Informationen auf der persönlichen Startseite unmittelbar mit dem Google-Konto verknüpft und werden auf Google's Servern gespeichert. Dazu gehören vor allem Lesezeichen und persönliche Inhalte der Gadgets, wie z.B. eigene Notizen oder Termine. Bei Gadgets von Drittanbietern müssen deren Datenschutzbestimmungen beachtet werden. Außerdem können natürlich alle Suchanfragen mit dem Google-Konto verknüpft werden.

Risikoverminderung: Man kann iGoogle auch ohne ein Google-Konto verwenden, dann jedoch nicht von jedem beliebigen Browser aus. Der personalisierte Desktop wird dann nämlich nicht mit dem Google-Konto verknüpft und auf Google-Servern gespeichert, sondern in einem Cookie. Wird dieses Cookie gelöscht, gehen allerdings alle Informationen verloren. Um dies zu verhindern, besteht wiederum die Möglichkeit, alle persönlichen Einstellungen und Daten als XML-Datei zu exportieren um sie anschließend wieder importieren zu können. Verwendet man dennoch ein Google-Konto bei iGoogle, sollte man darauf achten, welche Informationen man bei den Gadgets von iGoogle eingibt und die Nutzungs- und Datenschutzbestimmungen von Drittanbietern beachten.

4.2.3.16 Google Kalender

Google-Konto erforderlich: Ja

Beschreibung: Google Kalender ist ein Dienst zum Verwalten von Terminen. Dabei handelt es sich um eine Online-Variante von Produkten wie dem Mozilla Sunbird oder der Kalender-Funktionalität von Microsoft Outlook.

Mehrwert: Im Gegensatz zu den Offline-Produkten kann von jedem Internet-fähigen Endgerät auf einen zentralen Kalender zugegriffen werden. Im Einzelnen bietet der Google Kalender folgende Features (vgl. Google 2011g):

- Suche im Kalender
- Anzeige der deutschen Feiertage
- Freigabe von Terminen: Andere Personen können sich die eigenen Termine anschauen.
- Mobiler Kalender: Möglichkeit zur Synchronisation mit dem internen Kalender von verschiedenen mobilen Endgeräten. Zusätzlich gibt es eine für kleine Bildschirme optimierte Version des Online-Kalenders.
- Erinnerungsfunktionalität: Automatisch generierte Erinnerungen können per E-Mail oder per SMS versendet werden.
- Einladen von Personen: Bietet die Möglichkeit, andere Nutzer des Dienstes zu Terminen einzuladen. Die Einladung kann per E-Mail oder intern im Dienst übermittelt werden.
- Synchronisation mit Desktopanwendungen: Der Kalender bietet entsprechende Schnittstellen zu Apple iCal, Mozilla Sunbird und Microsoft Outlook, um Termine zu synchronisieren.

- Offline-Zugriff: Im Offline-Modus kann lesend auf den Kalender zugegriffen werden. Dafür wird allerdings Google Gears benötigt (siehe Kapitel 4.2.4: Cloud Computing).

Risiken: Alle Termine und ggf. die unterschiedlichen Teilnehmer, die zu einem Termin eingeladen wurden, sind fortan mit dem Google-Konto verknüpft. Welche anderen Personen die Termine sehen können, kann festgelegt werden und zwar sowohl terminübergreifend als auch auf einzelne Termine bezogen. Termine können privat und für andere Nutzer unzugänglich sein, für bestimmte, selbst ausgewählte Nutzer sichtbar sein oder für die breite Öffentlichkeit zugänglich sein. Öffentliche Termine sind in den Google-Suchergebnissen enthalten.

Risikoverminderung: Möchte man den Dienst verwenden, sollte man den Kalender generell so konfigurieren, dass dieser und somit auch die enthaltenen Termine nicht öffentlich zugänglich sind (Standardeinstellung). Beim Eintragen neuer Termine sind diese nun standardmäßig privat. Möchte man einen Termin ganz bewusst veröffentlichen, kann man dies in den Einstellungen des entsprechenden Termins machen.

4.2.3.17 Google Knol

Google-Konto erforderlich: Nein, nur wenn man aktiv mitmacht

Beschreibung: Knol (vom englischen Wort Knowledge abgeleitet) ist eine Wissensdatenbank. Damit ähnelt der Dienst Wikipedia, denn hier sollen Artikel zu verschiedenen Themen, möglichst abgeschlossen, behandelt werden. Dabei können mehrere Autoren Artikel zum gleichen Thema verfassen. Eine Bewertung durch andere Nutzer bestimmt die Relevanz und somit auch das Ranking in Suchergebnissen.

Mehrwert: Im Gegensatz zu Wikipedia ist Knol keine klassische Enzyklopädie. Dementsprechend kann die Behandlung eines Themas mehrere Artikel von mehreren Autoren und somit auch mehrere Meinungen umfassen, was von Vorteil sein kann. Bei Wikipedia hingegen gibt es einen Artikel zu einem Thema. Dieser wird in der Regel individuell erstellt, jedoch kollaborativ korrigiert, erweitert und aktualisiert. Aber auch bei Knol ist eine Beteiligung der Community möglich: Neben der Kommentierung von Artikeln können Nutzer dem Autor Verbesserungsvorschläge unterbreiten oder den Artikel sogar selber editieren, sofern sie berechtigt sind. Ein Artikel kann mehrere Eigentümer haben und auch vollständig zur Bearbeitung freigegeben werden. Bei einer Freigabe hat der Autor die Möglichkeit, den Artikel zu moderieren. Alles in allem ist Knol eine nette Ergänzung zu Wikipedia, auf keinen Fall jedoch eine Alternative. Neben der Integration von AdSense (wie beim Dienst Blogger.com) bietet Knol eine einfache Schnittstelle zu Google Analytics.

Risiken: Veröffentlichte Artikel oder auch abgegebene Kommentare, Änderungsvorschläge etc. werden im Google-Konto gespeichert. Vom Google-Profil werden lediglich die in Abbildung 12 zu sehenden Informationen angezeigt. Wenn in diesem Profil festgelegt wurde, dass der vollständige Name angezeigt werden soll, wird er auch hier bei Knol angezeigt. Außerdem ist in der Autorenstatistik ersichtlich, wann man sich angemeldet hat und wann man das letzte Mal aktiv war. Es besteht die Möglichkeit, sich als Autor verifizieren zu lassen. Dazu muss man beispielsweise die Telefon- oder die Kreditkartennummer angeben (vgl. Google 2011h).

Abbildung 12: Profil, das bei Knol angezeigt wird

Risikoverminderung: Man sollte keine sensiblen Inhalte veröffentlichen und das Google-Profil nicht unnötig mit persönlichen Daten anreichern, gesonderte Datenschutz-Optionen bestehen hier nicht. Ob man sich wirklich als Autor verifizieren lassen sollte, hängt vom sonstigen Gebrauch des Google-Kontos ab: Wenn es ausschließlich für Knol verwendet wird, wäre es vielleicht akzeptabel.

4.2.3.18 Google Mail

Google-Konto erforderlich: Ja

Beschreibung: Google Mail (kurz Gmail) ist der E-Mail-Dienst von Google. Ein Chat ist ebenfalls integriert.

Mehrwert: Unter etlichen E-Mail-Providern ist Gmail ein kostenloser Top-Dienst. Daher ist es auch wenig verwunderlich, dass Gmail schon bei diversen Tests Sieger geworden ist. Für Gmail spricht u.a.:

- Schlichte Aufmachung, also keine Portallösung a la GMX oder WEB.DE.
- Keine Popups und Werbebanner, dafür werden jedoch kurze Textanzeigen platziert
- 7 GB Speicherplatz
- Zuverlässiger Spam- und Virenschutz
- Google-Suchfunktion
- Automatische Backups (schon beim Schreiben einer Mail)
- Rechtschreibprüfung
- Import und Export von Mails und Adressen
- POP3/SMTP(S)/IMAP
- PDF-Dokumente sowie einige Dokumente aus Microsoft Office und Open Office können direkt als HTML-Dokument geöffnet werden, ohne zusätzliches Tools

Risiken: Die Inhalte der E-Mails werden von Software-Agenten durchsucht und analysiert, um inhaltlich passende Werbung zu platzieren. Dieses Durchsuchen der Daten durch einen Algorithmus stellt allerdings kein großes Problem dar. Ein vermutlich größeres Problem ist die Speicherung persönlicher und geschäftlicher E-Mails auf Google-Servern und die damit verbundene Verknüpfung mit dem Google-Konto. Auf Basis dieser Informationen könnte das Google-Konto ziemlich einfach einer Person zugeordnet werden inkl. deren Kommunikationsinhalte und Kontakte. Ca. 7 GB Speicherplatz stellt Google seinen Gmail-

Nutzern zur Verfügung, damit diese möglichst viele Informationen auf Google's Servern speichern können. Eines sollte man sich vielleicht auch noch bewusst sein: Nutzt man selbst kein Gmail und scheibt jemandem eine E-Mail an eine Gmail-Adresse, so wird diese E-Mail ebenfalls von Google gespeichert.

Risikoverminderung: Ggf. könnte man ähnlich hochwertige Alternativen suchen, auch wenn das sehr schwer werden könnte, zumindest wenn diese zugleich kostenlos sein sollen. Eine gute Möglichkeit wäre es auch, sich nur mit den nötigsten Daten anzumelden und dann nur einen E-Mail-Client wie Thunderbird oder Outlook zu verwenden. Man würde somit möglichst wenige Informationen mit dem Google-Konto verknüpfen, allerdings gehen die meisten Vorteile von Gmail dann verloren. Außerdem würden die E-Mails trotzdem dauerhaft auf Google-Servern gespeichert, zumindest bei der Verwendung von IMAP. Auf jeden Fall sollte man sich gut überlegen, ob man Gmail denn nun wirklich benötigt und wenn ja, dann sollte man das Konto mit möglichst wenig persönlichen Informationen anreichern und für persönliche sowie vertrauliche E-Mails lieber einen anderen Anbieter verwenden.

4.2.3.19 Google Maps

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: Geographische Karte, mit der man Adressen, Orte von Interesse, Geschäfte und andere Objekte suchen kann. Google Maps zeigt auch reale Aufnahmen der Erdoberfläche (Satellitenaufnahmen) an und enthält neben einem Routenplaner auch aktuelle Verkehrsinformationen. Des Weiteren können eigene Karten mit eigenen Objekten oder Routen erstellt werden. Dort können Texte, Fotos oder Videoaufnahmen hinzugefügt und die Ergebnisse veröffentlicht werden. Dazu ist allerdings ein Google-Konto notwendig. Außerdem ist Google Street View (siehe Kapitel 4.2.2) in Google Maps integriert.

Mehrwert: Die Kombination von Karte inkl. komfortabler Adresssuche à la Google, Routenplanung, Satellitenbildern, Street View und eigenen Karten ist einmalig. Herausgepickt sei an dieser Stelle mal die Routenplanung. Die Bedienbarkeit beispielsweise ist im Vergleich zu anderen Routenplanern genial. Per Drag & Drop kann man die einmal berechnete Route so modifizieren bzw. verlegen, dass alternative Strecken für einzelne Abschnitte oder die komplette Route entsprechend neu berechnet werden. Beim Ausdrucken einer Route kann der gedruckte Kartenausschnitt in der Druckvorschau beliebig angepasst werden, um z.B. lediglich die Zielumgebung detailliert darzustellen.

Risiken: Adressen inkl. Straßennamen und Hausnummern werden auf der Karte angezeigt. Man kann seinen eigenen Standort festlegen, der dann mit dem Google-Konto verknüpft und standardmäßig angezeigt wird. Dabei gelten die Google Mobile Datenschutzbestimmungen (siehe Kapitel 4.2.1). Außerdem werden alle Suchanfragen inkl. Routen in der Webhistorie gespeichert (siehe Abbildung 13). Erstellt man eigene Karten, sind diese standardmäßig öffentlich, sie sind also für alle freigegeben. Diese Karten werden dann in Suchergebnissen und Benutzerprofilen veröffentlicht. Wählt man die Option „nicht gelistet", so kann man nur selber und alle, die die entsprechende URL besitzen, auf die Karte zugreifen. Ein weiterer Aspekt wäre vielleicht, dass Unternehmen ihre Kunden so orten und beispielsweise nach soziodemographischen Kriterien bewerten können (vgl. Kraska 2008b). Die Risiken zu Street View sind in Kapitel 4.2.2 zu finden.

Abbildung 13: Google Maps in der Webhistorie

Risikoverminderung: Bei Suchen und Routenplanungen sollte man nicht mit seinem Google-Konto angemeldet sein, damit die eingegeben Informationen erst gar nicht mit dem Konto verknüpft werden und auf Google-Servern gespeichert werden können. Zudem sollte man keinen eigenen Standort festlegen, da sonst der potentielle Wohn- oder Arbeitsort mit dem Google-Konto verknüpft wird. Will man eigene Karten erstellen, sollte man beachten, dass auch alle angegeben Informationen fortan mit dem Google-Konto verknüpft sind. Will man dies dennoch tun, so sollte man immer die Option „nicht gelistet" wählen, außer natürlich, wenn diese Karten ausdrücklich öffentlich zugänglich sein sollen. Dennoch ist ein Fremdzugriff über die URL nicht ausgeschlossen.

4.2.3.20 Orkut

Google-Konto erforderlich: Ja

Beschreibung: Bei Orkut handelt es sich um ein im Januar 2004 erschienenes soziales Netzwerk. Somit ist es deutlich älter als Google Buzz, das im Februar 2010 veröffentlicht wurde. Über die Hälfte aller Zugriffe auf Orkut stammt aus Brasilien (Alexa 2011). Nichtsdestotrotz ist der Dienst auch in deutscher Sprache verfügbar.

Mehrwert: Vorteile anderer sozialer Netzwerke gegenüber sind wohl nur im Detail zu finden. So gibt es z.B. einen Button für diverse Webbrowser, mit dem man beliebige Webseiten, die man gerade besucht, schnell über Orkut freigeben kann. Wie bei Buzz auch, ist Google Talk zum Chatten integriert und es besteht eine direkte Zugriffsmöglichkeit auf Kontakte aus Gmail. Insgesamt spricht wenig für die Nutzung des Dienstes.

Risiken: Die Risiken beziehen sich in erster Linie auf allgemeine Datenschutzprobleme bei sozialen Netzwerken. Dazu kommt selbstverständlich, genau wie auch bei Google Buzz, die Verknüpfung mit dem Google-Konto (vgl. 4.2.3.5: Google Buzz).

Risikoverminderung: Da dieser Dienst keinen wahren Mehrwert hat, gibt es eigentlich keinen Grund ihn zu verwenden. Dazu kommt noch die fehlende Relevanz aufgrund der sehr geringen Verbreitung im deutschsprachigen Raum. Abbildung 14 zeigt dennoch die Wahlmöglichkeiten in den Einstellungen von Orkut.

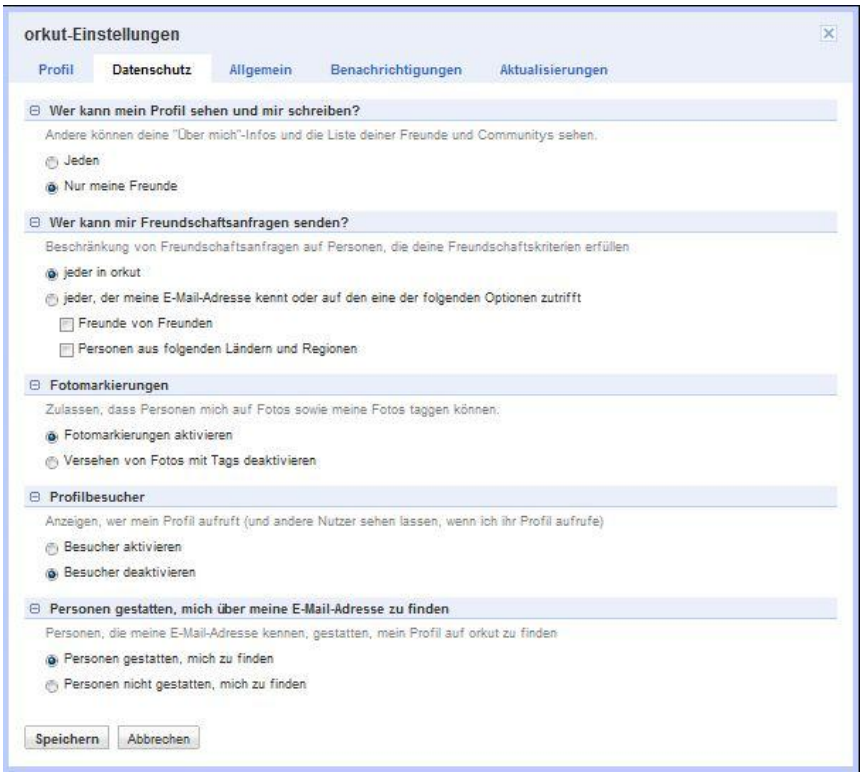


Abbildung 14: Datenschutzoptionen bei Orkut

4.2.3.21 Panoramio

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: Panoramio ist ein Dienst für das Sharing von Panoramaaufnahmen. Entsprechende Bilder können hochgeladen (Google-Konto vorausgesetzt) und mit einem Ort verknüpft werden (siehe Abbildung 15). Je nach Relevanz der Bilder bzw. Orte und der Metadaten werden die Aufnahmen in den Geo-Diensten von Google wie beispielsweise Google Earth aufgenommen. Wie eigene Tests zeigten, erscheinen ausschließlich Panoramaaufnahmen auf der Karte, andere Uploads werden dort ignoriert.

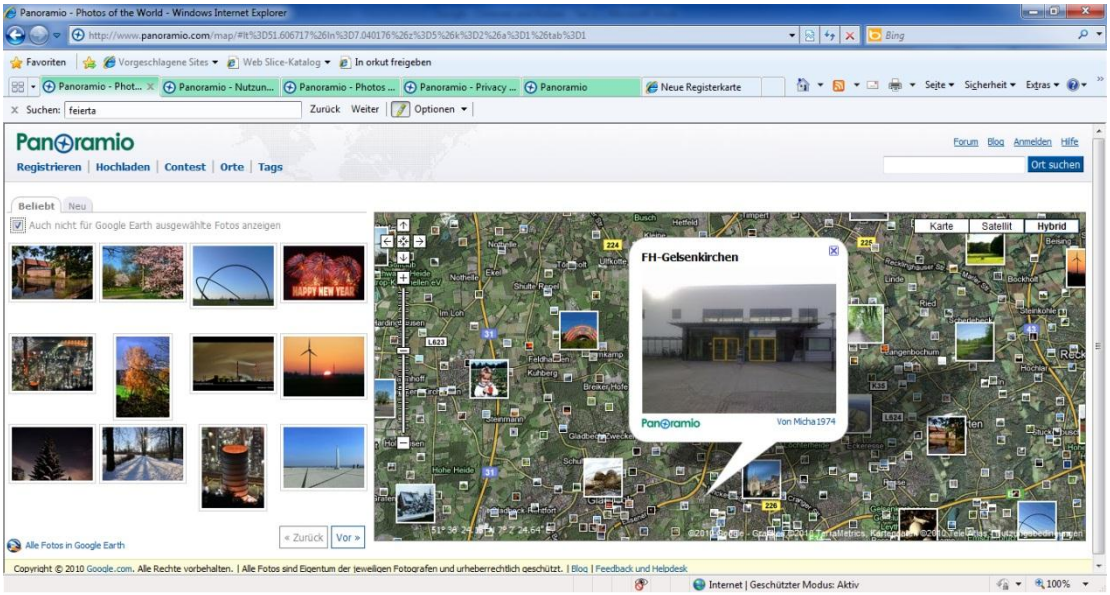


Abbildung 15: Der Google-Dienst Panoramio

Mehrwert: Dienste wie Panoramio, Locr und Woophy sind „wundervolle Instrumente für die Urlaubsrecherche und eignen sich dafür, anderen Menschen die schönsten Plätze der Welt näherzubringen“ (Dahlmann 2007). Für Panoramio spricht das hervorragende Geoinformationssystem von Google sowie auch die allgemeine Bedienbarkeit. Diesbezüglich können die anderen Dienste nicht mithalten. Außerdem gibt es neben Standard-Features wie Benachrichtigungen, Kommentierungen und Favoritenlisten einen Nutzer-Wettbewerb in den Kategorien „Landschaft“, „Erbe“, „Reisen“ und „außergewöhnliche Orte“ (siehe Abbildung 16).

Abbildung 16: Sieger eines Kontests bei Panoramia

Risiken: Bilder und Metadaten werden beim Upload im Google-Konto gespeichert. Wie auch bei anderen Diensten werden einige Nutzeraktivitäten aufgezeichnet. Dazu gehören z.B. der verwendete Speicherplatz, die Anzahl der Logins, angeguckte Inhalte und verfolgte Links (vgl. Google 2008). Man behält alle Rechte am eigenen Bild: „Niemand kann ohne Deine ausdrückliche Erlaubnis Kopien von Deinen Fotos machen oder sie verwenden“. Einer kommerziellen Verwendung sowie einer Bearbeitung der Aufnahmen kann man allerdings explizit zustimmen. Die Urheberrechte bleiben dabei unangetastet. Beim Nutzen des Dienstes ohne Anmeldung bestehen keine besonderen Risiken.

Risikoverminderung: Keine besonderen Verminderungsmaßnahmen vorhanden, aber dies ist zu verkraften, da es sich lediglich um Panoramafotos handelt.

4.2.3.22 Google Picasa / Picnic

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: Picasa ist eine Bildbearbeitungssoftware mit der u.a. Bilder in Alben organisiert und Beschreibungen hinzugefügt werden können. Außerdem bietet Picasa eine Personenerkennung, die Software kann also in allen indizierten Bildern nach Gesichtern suchen. Den gefundenen Personen kann man Namen zuweisen. Ist man mit dem Google-Konto angemeldet, kann man hierfür direkt Kontakte aus dem Google-Konto verwenden. Durch eine abgespeckte Google-Maps-Integration können Bilder mit beliebigen Orten verknüpft werden. Bei Alben besteht die Möglichkeit, diese mit dem Web zu synchronisieren. Auch ohne diese

Synchronisation können einzelne Alben oder Bilder einfach nur in die Picasa Webalben hochgeladen werden. Dabei stehen 1 GB Speicherplatz zur Verfügung. Im Gegensatz zu Picasa ist Picnik ist eine Online-Variante für die vollständige Bildbearbeitung und wurde im März 2010 von Google aufgekauft.

Mehrwert: Picasa und Picnik sind Softwarelösungen zur Organisation und Bearbeitung von Bildern. Mit Organisation ist nicht nur das Verwalten von Bildern in Alben gemeint, sondern auch das Verknüpfen mit Orten und Personen, das Veröffentlichen im Internet usw. Denn hier liegt der eigentliche Mehrwert: Picasa und Picnik verschmelzen die Offline-Bildbearbeitung und -organisation mit entsprechenden Onlinediensten.

Risiken: Bei der Nutzung der Picasa Webalben werden Bilder inkl. Metadaten (Orte, Personen, Beschreibungen usw.), Favoritenlisten und laut Datenschutzbestimmung „weiterer Daten" mit dem Google-Konto verknüpft. Nutzer, die sich Webalben anschauen, sehen dann neben den Fotos auch den Google-Nutzernamen des Eigentümers und verknüpfte Galerien. Werden die Alben in die öffentliche Suche mit eingeschlossen (Opt-in), so haben alle anderen Nutzer über die Suche in Picasa Webalben und die normale Google-Suche Zugriff auf sie. Wenn man die „Namens-Tag-Funktion" bzw. Gesichtserkennung nicht deaktiviert (Opt-out), analysiert Picasa automatisch alle indizierten Bilder, um passende Personen aus der bisher erfassten Datenbank für eine Verknüpfung vorzuschlagen. Dies geschieht, indem übereinstimmende Gesichter nach den dazugehörigen Personen gruppiert werden. Bei Picnik war es bisher so, dass alle Bilder nur für einen selber sichtbar waren, außer wenn man ausdrücklich andere Optionen wählt. Ob sich nach der Übernahme durch Google hier noch etwas ändert oder schon geändert hat, ist derzeit unklar (vgl. Google 2010s, Google 2010t).

Risikoverminderung: In der Offline-Version, also ohne Verschmelzung mit den Webalben und ohne Google-Konto, stellt Picasa keine besonderen Risiken dar. Synchronisiert man Alben und Bilder mit dem Web, sind anschließend sämtliche Informationen, auch die angesprochenen Metadaten, fortan mit dem Google-Konto verknüpft. Das Google-Konto wird also mit diesen ganzen persönlichen Daten angereichert. Daher sollte man Picasa Webalben nicht verwenden und sich auch sonst nicht mit dem Google-Konto anmelden, damit erst gar keine Daten mit diesem verknüpft werden können. Als Varianten zu Picasa Webalben stehen Flickr und Co bereit. Wie bei den Risiken schon angedeutet, wird Picnik hier nicht weiter betrachtet.

4.2.3.23 Google Profiles

Google-Konto erforderlich: Ja

Beschreibung: Mit Google Profiles können Personen eigene Profile, also beliebige Informationen über sich, ins Netz stellen. Dazu gehören persönliche Daten (vgl. Abbildung 17), Kontaktdaten (vgl. Abbildung 18) und Fotos. Nach diesen Profilen kann anhand des Namens gesucht werden. Zudem ist es über die URL www.google.com/profiles/*Kontoname* zugänglich. Das Profil, das für diese Ausarbeitung angelegt wurde, ist unter www.google.de/profiles/datenschutz2010 zu finden (siehe Abbildung 19). Ein Google-Profil ist außerdem Voraussetzung für die Verwendung von Google Buzz. Allerdings reicht es aus, wenn dieses Profil „leer" bleibt und nur irgendeinen, also nicht den echten Vor- und Nachnamen enthält (vgl. Google 2010u).

Abbildung 17: Persönliche Informationen in Google Profiles

Mehrwert: Ein echter Mehrwert besteht bei Google Profiles m.E. nicht. Es gibt viele andere Möglichkeiten, sich professionell im Web zu präsentieren. Allerdings wird man dann vielleicht nicht so schnell gefunden, was natürlich bzgl. der Privatsphäre kein Nachteil ist. Professionelle Alternativen sind allerdings selten vollständig kostenlos.

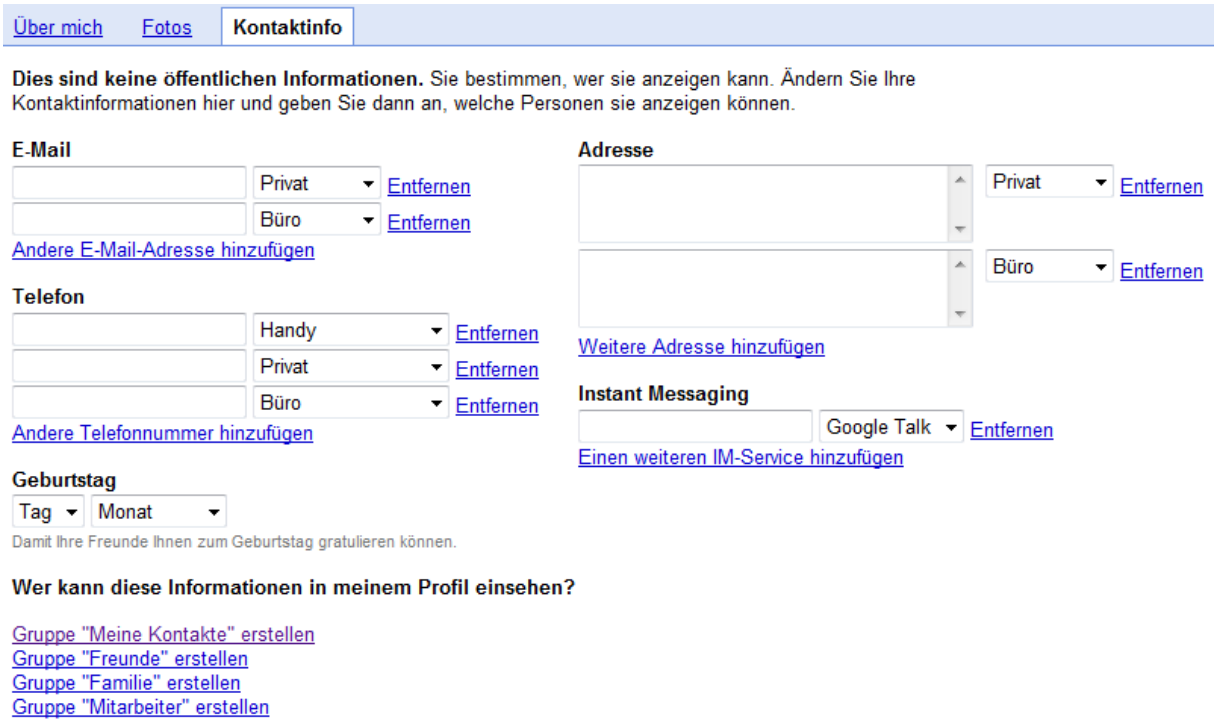


Abbildung 18: Kontaktinformationen in Google Profiles

Risiken: Das eigene Profil ist in anderen Google-Diensten sichtbar, z.B. in der Google Websuche, bei der nun dementsprechend auch nach Personen gesucht werden kann. Das Gefährliche ist,

dass hier das Google-Konto direkt mit einem ausführlichen Personenprofil verbunden wird. Damit Leute ihr Profil mit möglichst vielen Informationen anreichern, versucht Google diese mit der Überschrift „Bearbeiten Sie Ihr Profil - Je mehr Informationen Sie eingeben, desto leichter werden Sie von Ihren Freunden gefunden“ zu überzeugen. Wer die Kontaktinformationen sehen darf, kann eingestellt werden (vgl. Abbildung 10), öffentlich zugänglich sind sie jedenfalls nicht.

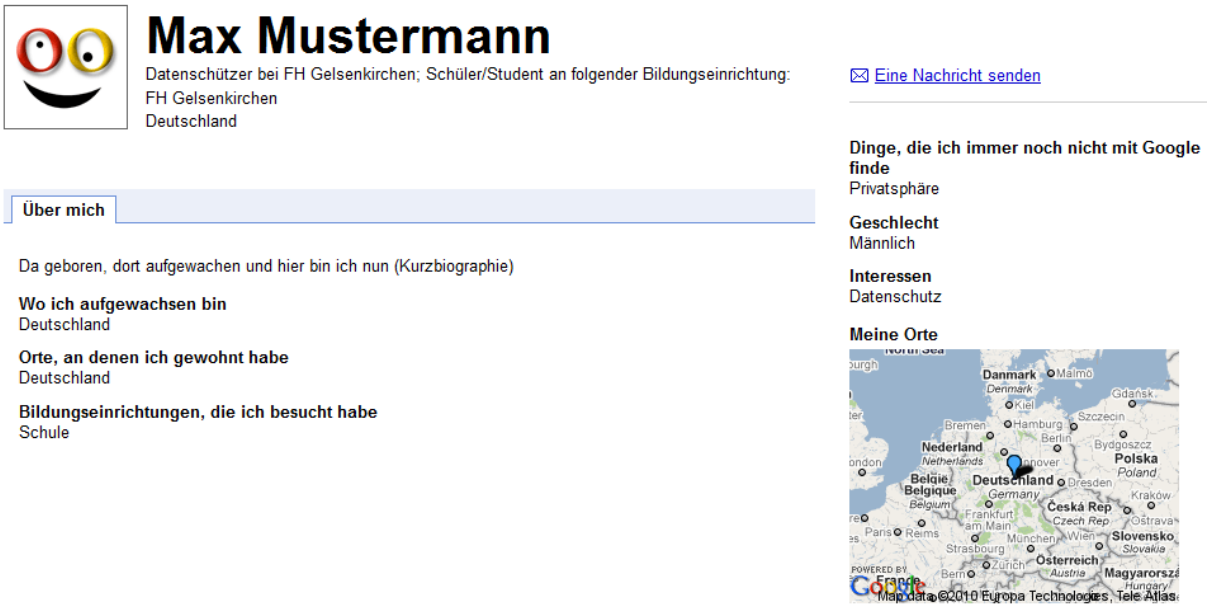


Abbildung 19: Das Google Profil

Risikoverminderung: Vom Verwenden eines eigenen Profils bei Google kann nur dringendst abgeraten werden, zumal kein echter Mehrwert besteht. Möchte man Google Buzz verwenden, muss man dem Profil keine zusätzlichen Daten hinzufügen. Es besteht außerdem die Möglichkeit, „nicht den vollen Namen anzuzeigen“. Dann ist das Profil nur noch über die URL (dort wird nur der Nachname ausgeblendet) und für Kontakte zugänglich und wird nicht mehr in die Suchfunktionalitäten von Google mit einbezogen. Unabhängig von der gewählten Option landen sämtliche Informationen auf Google-Servern, natürlich verknüpft mit dem Google-Konto.

4.2.3.24 Google Scholar

Google-Konto erforderlich: Nein

Beschreibung: Bei Google Scholar handelt es sich um eine wissenschaftliche Variante der Websuche von Google. Zu der wissenschaftlichen Literatur, die bei Scholar durchsucht wird, gehören Seminar-, Studien-, Abschluss- und Doktorarbeiten, aber auch Bücher, Zusammenfassungen und Artikel, die aus Quellen von akademischen Verlagen, Berufsverbänden, Magazinen für Vorabdrucke, Universitäten und anderen Bildungseinrichtungen stammen (vgl. Google 2010v).

Mehrwert: Die Vereinigung von wissenschaftlicher Suchmaschine und der unumstritten guten Suchfunktionalität (hier u.a. auch mit Filter für das Veröffentlichungsdatum und für Zitate) von Google ist einmalig und ein echter Mehrwert bei der Suche nach wissenschaftlicher Literatur.

Risiken: Den Risiken der Websuche sehr ähnlich (siehe Abschnitt 4.2.3.30).

Risikoverminderung: Siehe Websuche (Abschnitt 4.2.3.30).

4.2.3.25 Google Talk/Voice

Google-Konto erforderlich: Ja

Beschreibung: Google Talk vereint Instant Messaging, VoIP und Videokonferenzen. Von Google Talk gibt es zwei Varianten: Ein Plug-in für Gmail und iGoogle sowie eine installierbare Software für herkömmliche Betriebssysteme und Android. Google Voice ist ein webbasierter Telefonmanager (POTS), bei dem man in den USA Festnetznummern erhält und verwalten kann, getreu dem Motto "eine Nummer für alle deine Telefone, für immer".

Mehrwert: Bis auf die mögliche Integration von Google Talk in Gmail bzw. iGoogle (vor allem interessant wenn dort bereits Kontakte vorhanden sind) bestehen keine erheblichen Vorteile im Vergleich zu Skype und Co. Es besteht jedoch ein großer Nachteil: Im Gegensatz zu anderen Tools kann man nur mit Nutzern des Google Talk-Netzwerks kommunizieren und nicht mit Leuten, die Skype, ICQ, MSN oder Yahoo Messenger etc. verwenden.

Risiken: Google speichert Informationen wie z.B. wann man Google Talk verwendet, die Anzahl aller Kontakte, die Kontakte mit denen man kommuniziert und die Häufigkeit und das Volumen von Datentransfers. Deutlich dramatischer ist, dass die Inhalte aller Konversationen von Google aufgezeichnet werden. Diese Inhalte werden, wie bei Gmail, automatisch durchsucht, um kontextsensitive Werbung zu platzieren. Außerdem wird beim Versenden einer SMS über Google Talk die Telefonnummer des Empfängers, der Inhalt der SMS und die Kommunikationszeiten aufgezeichnet (vgl. Google 2010w). Ähnlich sieht es bei Google Voice aus, denn hier werden Telefongespräche nach einer Spracherkennung als Texte abgespeichert. Ob hier Opt-in oder Opt-out gilt, ist zu diesem Zeitpunkt unklar, da hier kontroverse Berichte vorlagen. In Deutschland ist Google Voice, wie bereits erwähnt, (noch) nicht verfügbar.

Risikoverminderung: Grundsätzlich sollte man alternative Tools zu Google Talk verwenden. Möchte man es dennoch nutzen, besteht die Möglichkeit, die Chat-Einstellungen so anzupassen, dass Chat-Konversationen zukünftig nicht mehr im Google-Konto abgespeichert werden. Um zu verhindern, dass der Chatpartner seinerseits eine spezielle Konversation im Google-Konto abspeichert, kann man einzelne Konversationen als vertraulich markieren. In Abbildung 20 sieht man auf der linken Seite das Chatfenster des einen Teilnehmers und auf der rechten Seite das seines Chatpartners. Markiert ein Teilnehmer den Chat als vertraulich, wird sein Gegenüber darüber informiert. Beide Seiten können die Vertraulichkeit jederzeit wieder abbrechen, auch wenn der Andere sie aktiviert hat. Leider ist es nicht möglich, die Einstellungen so anzupassen, dass Konversationen grundsätzlich vertraulich sind.

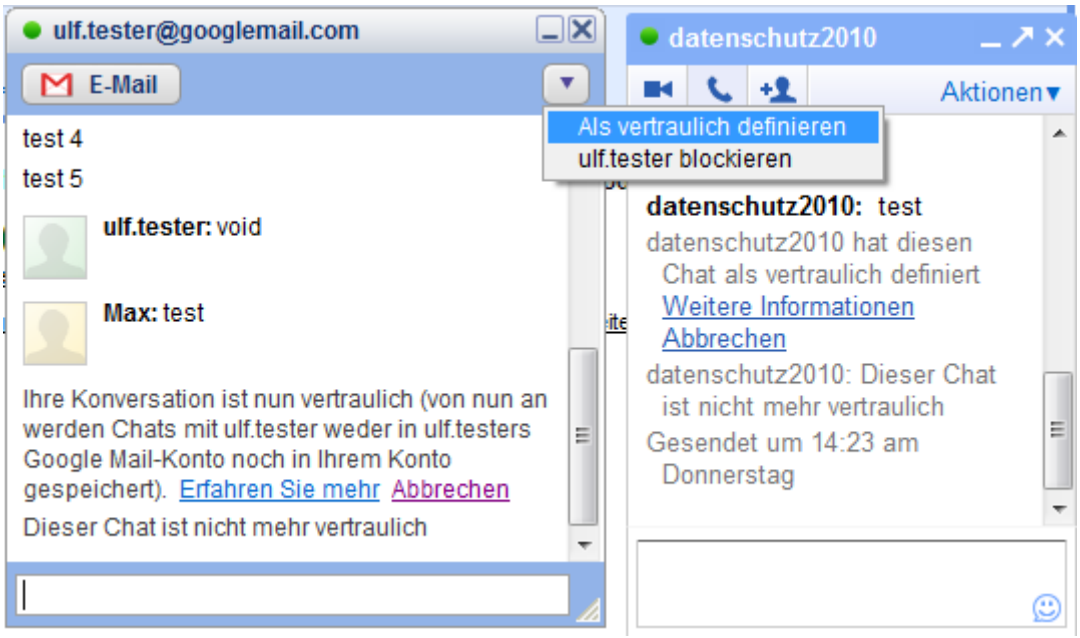


Abbildung 20: Vertraulichkeit bei Google Talk

4.2.3.26 Google Text & Tabellen

Google-Konto erforderlich: Ja

Beschreibung: Google Docs & Spreadsheets, zu Deutsch „Text & Tabellen“ ist ein Office-Dienst für Textverarbeitung, Tabellenkalkulation und Präsentationen, der vollständig online verfügbar ist. Dabei stehen einem 1 GB Speicherplatz für eigene Dokumente bereit. Mittlerweile kann man Textdokumente auch offline bearbeiten und sie dann automatisch mit der Online-Fassung synchronisieren lassen, sobald wieder eine Internetverbindung besteht. Für Unternehmen steht eine kostenpflichtige, werbefreie Version zur Verfügung.

Mehrwert: Bei diesem Dienst handelt es sich um ein komfortables Office-Paket in einer kostenlosen Onlinevariante. Unterstützt werden Dokumentformate von Open Office und Microsoft Office sowie PDF, HTML und weitere. Alle getätigten Eingaben werden unmittelbar im Dokument gespeichert, damit keine Daten verloren gehen. Als besondere Funktionalitäten gibt es den Google Docs Viewer für mobile Endgeräte, eine Texterkennung für hochgeladene Bilder und PDFs sowie die integrierte Google-Suche und -Übersetzung.

Risiken: Bei den Risiken spielen sowohl das Urheberrecht als auch der Datenschutz eine wichtige Rolle. Man gewährt Google eine Lizenz zur Vervielfältigung, Anpassung, Änderung, Übersetzung, Veröffentlichung, öffentlichen Aufführung, öffentlichen Anzeige und Distribution von Inhalten. Diese dient laut Nutzungsbedingungen allerdings nur dazu, den „Service gemäß den Datenschutzbestimmungen“ zu erbringen. Vermutlich handelt es sich hierbei um eine juristische Absicherung, tiefere Gründe sollen jedoch nicht betrachtet werden.

> *Sie behalten das Urheberrecht und alle anderen bereits vorhandenen Rechte an dem Inhalt, den Sie auf dem oder über den Service einreichen, freigeben, hochladen, einstellen oder anzeigen. Durch das Einreichen, Freigeben, Hochladen, Einstellen oder Anzeigen von Inhalten erteilen Sie Google eine weltweit gültige, kostenlose und nichtexklusive Lizenz zur Vervielfältigung, Anpassung, Änderung, Übersetzung, Veröffentlichung, öffentlichen Aufführung, öffentlichen Anzeige und Distribution von*

> *Inhalten, die Sie auf dem oder über den Service einreichen, freigeben, hochladen, einstellen oder anzeigen. Diese Lizenz dient ausschließlich dazu, Google in die Lage zu versetzen, Ihnen den Service gemäß den Datenschutzbestimmungen für Google Text & Tabellen zur Verfügung zu stellen.* (Google 2010x)

Alle erstellten und hochgeladenen Dokumente werden im Google-Konto „abgelegt". Standardmäßig ist die Dokumentoption „privat" eingestellt. Dokumente können jedoch veröffentlicht bzw. freigegeben werden, wobei man einstellen kann, wer die Dokumente sehen und bearbeiten darf. Außerdem werden Aktivitätsdaten in Bezug auf das Konto (z. B. Speichernutzung, Anzahl der Anmeldungen, ausgeführte Aktionen) sowie angezeigte oder angeklickte Daten (z. B. Elemente auf der Benutzeroberfläche und Links) gespeichert (vgl. Google 2010y). Eine Datenschutzpanne im Oktober 2009 sorgte dafür, dass eigene Dokumente von anderen Nutzern mitgelesen und bearbeitet werden konnten (vgl. Google 2009, RPO 2009).

Risikoverminderung: Allgemein sollte man keine Dokumente, die persönliche bzw. sensible Daten enthalten mit Google Text und Tabellen bearbeiten und aufpassen, wem man was zur Ansicht und Bearbeitung zur Verfügung stellt.

4.2.3.27 Google Toolbar

Google-Konto erforderlich: Je nach Funktion

Beschreibung: Die Toolbar von Google ist eine Erweiterung für Firefox und den Internet Explorer, um schnell auf Google-Dienste zugreifen zu können. Neben der Suche in diversen Google-Diensten (der gewünschte Dienst kann über ein Auswahlmenü selektiert werden, die Standardeinstellung ist die Websuche) stehen u.a. eine Übersetzungsfunktion und eine Rechtschreibprüfung für Webseiten zur Verfügung. Neuerdings ist auch das Weiterleiten von URLs über Gmail, Buzz, Twitter etc. sowie das Kommentieren von Webseiten über ein Sidewiki möglich. Dabei besteht natürlich auch Zugriff auf Kommentare anderer Nutzer. Für den Zugriff auf das Sidewiki und das Weiterleiten von URLs ist ein Google-Konto notwendig. Des Weiteren steht eine Auto-Fill-Funktion zur Verfügung, um das Ausfüllen von Formularen auf beliebigen Webseiten zu automatisieren. Google speichert dafür die Struktur der Formulare und die Inhalte, allerdings nur lokal auf dem Rechner. Dies ist allerdings nicht mehr der Fall, wenn man diese Daten ausdrücklich mit seinem Google-Konto synchronisiert, damit sie nicht nur lokal zur Verfügung stehen.

Mehrwert: Die Google Toolbar ermöglicht einen Schnellzugriff auf diverse Google-Dienste und enthält zusätzlich einige, mehr oder weniger nützliche Features.

Risiken: Genau wie bei Google Chrome werden alle in die Adressleiste des Browsers eingegebenen URLs und Suchbegriffe, von der Eingabe des ersten Zeichens bis zum Absenden der Anfrage, an Google übermittelt. In der Toolbar eingegebene Suchbegriffe werden in der Webhistorie gespeichert, sofern man mit dem Google-Konto angemeldet ist. Außerdem werden Nutzungsstatistiken an Google gesendet. Andere Daten werden wie auch bei der Suchmaschine erhoben. Jede Toolbar erhält eine eigene ID, um sie eindeutig zu identifizieren. Diese wird an Google übermittelt, jedoch nicht mit dem Google-Konto verknüpft (vgl. Google 2010z).

Risikoverminderung: Alle Funktionen, die automatisch URLs oder andere Informationen über besuchte Webseiten an Google senden oder Daten mit dem Google-Konto verknüpfen, können

in den Einstellungen deaktiviert werden (Opt-out). Darunter auch das Senden von Nutzungsstatistiken. Eine entsprechende Konfiguration sollte unmittelbar nach der Installation der Google Toolbar vorgenommen werden.

4.2.3.28 Google TV

Google-Konto erforderlich: Noch nicht absehbar, vermutlich ja, vielleicht aber auch nur je nach Funktionalität. Bei personalisierten Funktionalitäten wie Favoritenlisten etc. wird bei Google TV mit Sicherheit die Möglichkeit bestehen, diese auch mit dem Google-Konto zu synchronisieren bzw. Aufnahmen über das Internet zu programmieren.

Beschreibung: Mit Google TV will Google das Fernsehen mit dem Internet verschmelzen, dementsprechend soll das komplette Web auf den Fernsehgeräten verfügbar sein. Inzwischen sind die ersten Modelle mit Google TV in den USA verfügbar: Sony baut Fernseher und BlueRay-Player mit Google TV und Logitech entsprechende Set-Top-Boxen. Die Chips dafür liefert Intel. Die Software für Google TV basiert auf Android, so verwundert es auch wenig, dass alle (mittlerweile über 200.000) Android Apps, die keine Telefonfunktionalität voraussetzen, im Rahmen von Google TV ausgeführt werden können.

> *Das Prinzip ist dabei einfach: Google TV macht keinen Unterschied zwischen aktuell ausgestrahlten Fernsehsendungen, Internet-Streams oder im Netz verfügbaren Videos. Zentrales Element des Systems ist ein Suchfeld auf dem Fernsehbildschirm. Über dieses kann sich der Zuschauer anzeigen lassen, wann seine Lieblingsserie im TV zu sehen ist, bei welchem Streamingdienst er sie sich herunterladen kann oder ob sie vielleicht sogar auf der Serien-Website kostenlos gezeigt wird. Auch beim TV-Konsum selbst soll das Internet nun zum integralen Bestandteil werden. Statt zwischen Surfen und Fernsehen wählen zu müssen, sollen beide Funktionen verschmelzen. Optisch funktioniert das durch ein Bild-im-Bild-Verfahren, das auch bei Videorecordern oder DVD-Playern angewendet wird: In der unteren Ecke des Bildschirms wird ein kleines Fenster eingeblendet.* (Kuhn 2010)

Mehrwert: Die Kombination von Fernsehen mit der Google-Suchfunktionalität ist einfach nur genial: Videoclips, Bilder, Musik und Spiele; alles auf dem Fernseher. Das ist ein echter Mehrwert. Mit ähnlichen Technologien könnten wohl auch andere Anbieter dienen, mit der Qualität der Google-Suchfunktionalität hingegen nicht. Statt Werbeunterbrechungen könnte Google vielleicht die bisherige, unaufdringliche und wenig störende Werbung integrieren. So viel zu den Erwartungen aus dem Sommer 2010, mittlerweile wurden diese deutlich gedämpft. Denn eine echte Verschmelzung von Fernsehen und Internet gerät ins Stocken. Der Grund liegt darin, dass die großen TV-Anbieter in den USA nicht mitspielen. Mit Google TV kann man Programmübersichten aufrufen, die Aufzeichnung von Kabel- und Satellitenkanälen programmieren und die medialen Inhalte des Internets auf den Fernsehen holen und zwar nicht über einen Webbrowser, sondern deutlich praktischer. Und genau das bremsen die großen Sendeanstalten in den USA aus. ABC, CBS, NBC und Fox haben sich entschieden, ihre Netzangebote für Google zu blockieren. Wenn Nutzer von Google TV z.B. Medien von fox.com abrufen möchten, erscheint die Fehlermeldung „Dieser Inhalt ist nicht kompatibel mit ihrem Gerät“. Das führt u.a. dazu, dass man sich mit Google TV keine im Internet frei verfügbaren TV-Serien von Fox anschauen kann. Außerdem hat auch der Filmdienst Hulu Google TV ausgesperrt. Hulu bietet mit einer US-Internetadresse ein sehr breites Angebot an kostenlosen Serien und Kinofilmen.

> *Mit der Sperre der ‚Großen Vier' und Hulu bleiben Nutzern von Google TV fast nur Online-Videoportale wie YouTube, Vimeo und Co. Hinzu kommen kleinere Sender, die ihr Werbeangebot noch nicht für die Google-Kiste gesperrt haben. […] Inhalte kommen nun entweder aus dem Fernsehen – was nicht der Sinn war – oder über die beiden Inhaltepartner Netfix und Amazon on Demand. Der eine Dienst vermietet Filme gegen eine Monatspauschale, der andere verleiht sie gegen Einzelgebühren.* (Schwan 2010a)

Im Jahr 2011 plant Google mit seinem TV-Programm in Europa auf den Markt zu gehen. Es bleibt abzuwarten, wie Anbieter hierzulande reagieren. Auch diese möchten mit Sicherheit nicht, dass ihre Inhalte vorbei an ihren eigenen Webseiten und somit auch vorbei an ihren Werbeflächen der breiten Masse zur Verfügung gestellt werden. Vielleicht wären die Anbieter mit Werbepartnerschaften umzustimmen (Schwan 2010a).

Risiken: Es ist noch nicht absehbar, welche Risiken konkret bestehen werden. Irgendwelche Informationen (auch personenbezogene) wird man mit Sicherheit preisgeben können bzw. müssen.

Risikoverminderung: Konkrete Maßnahmen sind noch nicht absehbar. Allgemein gilt es natürlich, so wenige Informationen wie möglich mit dem Google-Konto verknüpfen.

4.2.3.29 Google Wave

Google-Konto erforderlich: Ja

Beschreibung: Google Wave ist ein internetbasiertes System zur Kommunikation und Kollaboration in Echtzeit. Im Gegensatz zu anderen Diensten im Einzelnen, verbindet Google Wave E-Mail, soziales Netzwerk, Instant Messenger, Chat, Wikis usw., alles auf einer Plattform. Außerdem können gemeinsame Dokumente, Bilder, Videos etc. geteilt und mit anderen bearbeitet werden. Dokumente per E-Mail-Anhang oder andere herkömmliche Methoden auszutauschen, würde damit der Vergangenheit angehören. Laut Google selbst ist Wave gar kein Dienst, sondern eine Architektur, für die Google die Quellcodes zu gegebener Zeit veröffentlicht. Damit sollen Anwender ihren eigenen „Wave-Server" betreiben können. Google sei am Ende schließlich nur einer vieler möglicher Provider für Wave (vgl. Kretschmann 2009). Google Wave ist nur mit Chrome, Firefox und Safari sowie iPhone und Android kompatibel. Möchte man es mit dem Internet Explorer verwenden, so benötigt man das „Google Chrome Frame Browser Plug-in". Obwohl Google Wave so vielversprechend begann, wurde die Entwicklung im August 2010 schon wieder eingestellt. Grund dafür war das fehlende Interesse seitens der Nutzer. Der Dienst steht aber vorerst noch weiter zur Verfügung (vgl. Weber 2010).

> *Der anfängliche Hype wurde durch die restriktive Vergabe von Einladungen noch angeheizt. Jeder wollte dabei sein. Wer aber erst mal drin war, der fragte sich schnell: "Und was jetzt?" Das Konversationskonzept von Wave war nicht leicht zu verstehen. Simultane Änderungen in der gleichen Konversation durch mehrere Benutzer an verschiedenen Stellen führten schnell zu unübersichtlichen Dokumenten, die eher einem klassischen Forenverlauf mit Fragen und Antworten glich denn einem Dokument.* (Weber 2010)

Mehrwert: Prinzipiell sind solche offenen, echtzeitbasierten „Kommunikationszentralen" aus Nutzersicht eigentlich sehr zu begrüßen:

> *Google Wave scheint wirklich die eierlegende Wollmilchsau und DIE Lösung für die Echtzeit-Kommunikation mit anderen Nutzern zu werden. […] Google Wave ist nicht einfach ein besserer eMail-Client, sondern eine ganz andere Herangehensweise an die Kommunikation.* (Wandiger 2009)

Risiken: Hier findet eine Datenkonzentration bei einem einzigen Provider statt, da statt mehrerer Dienste nur noch Google Wave genutzt werden könnte. Entsprechend bestehen auch die gleichen Risiken, die bei den einzelnen Diensten schon diskutiert wurden. Dazu kommt das Problem der Datenkonzentration, da alle Informationen bei Wave, also auch im Google-Konto zusammenlaufen. Auch das BSI warnte schon im Lagebericht des zweiten Quartals 2009:

> *Alle Google-Wave-Daten liegen auf Google-Servern. Damit gilt für Google Wave dieselbe Kritik, die durch Datenschützer und das BSI an Google Mail, Google Docs, Google Calendar und anderen Online-Diensten des Unternehmens geübt wurde: Der Nutzer verliert vollständig die Kontrolle über seine Daten. Daher ist eine Nutzung von Google Wave (ebenso wie eine Nutzung der anderen Google-Dienste) sowohl aus IT-sicherheitstechnischen Gründen als auch aus Sicht des Datenschutzes aktuell nicht zu empfehlen. Der offene Ansatz des Google Wave Federation Protocol ist zu begrüßen, kann aber die negative Gesamteinschätzung nicht ändern. Sollte zukünftig eine verteilte, gesicherte und kontrollierbare Datenhaltung mit Google Wave möglich sein, muss diese Bewertung neu vorgenommen werden.* (BSI 2009)

Risikoverminderung: Entfällt, da die Entwicklung eingestellt wurde.

4.2.3.30 Google Websuche

Google-Konto erforderlich: Nein

Beschreibung: Die Websuche ist die Suchmaschine, die Google bekannt gemacht hat.

Mehrwert: Die Google-Suche mit ihrem PageRank-Algorithmus ist zweifelslos die beste und qualitativ hochwertigste Suchmaschine im Internet. Microsoft hat mit Bing den Versuch gestartet, hier mitzuhalten. Auch wenn sich die Ergebnisse durchaus sehen lassen können, so ist Bing noch keine gleichwertige Alternative zur Google Websuche. Seit September 2010 bietet Google die sogenannte Instantsuche. Dabei werden die Suchergebnisse schon während der Eingabe des Suchbegriffs angezeigt und entsprechend aktualisiert. Laut Google kann der Nutzer durch dieses Feature pro Suche 2 bis 5 Sekunden einsparen.

Risiken: Google speichert, wie andere Suchmaschinen übrigens auch, Logdateien. Diese bestehen aus Anfrage (u.a. der Suchbegriff), IP-Adresse, Cookie(s) zur Identifikation, Zugriffszeitpunkten und Browser-Typ. IP-Adressen werden nach 9 Monaten anonymisiert und Cookie-IDs nach 18 Monaten gelöscht. Außerdem speichert Google neben den Suchanfragen alles, was in das Suchfeld eingegeben wird, auch wenn man die eigentliche Suchanfrage gar nicht absetzt. Ist die Webhistorie aktiviert, so werden Klicks auf Suchergebnisse, Anzeigen usw. mit dem Google-Konto verknüpft (vgl. Google 2010b).

Risikoverminderung: Damit sämtliche Angaben und Aktionen erst gar nicht in Verbindung mit dem Google-Konto gebracht werden können, sollte man bei der Websuche nicht mit diesem angemeldet sein, da die Funktionalitäten der Suchmaschine auch ohne Anmeldung nahezu die gleichen bleiben. Zwar ködert Google mit Suchergebnissen, die noch besser personalisiert

werden, wenn man angemeldet ist und die Webhistorie aktiviert hat, ob einem jedoch wirklich bessere Suchergebnisse geliefert werden, darf zumindest bezweifelt werden. Ist man nicht mit dem Google-Konto angemeldet, so kann man über die IP-Adresse und Cookies identifiziert werden. Hier hilft eigentlich nur das generelle Deaktivieren oder ein regelmäßiges Löschen der entsprechenden Cookies. Empfehlenswert ist es auf jeden Fall auch, einen Blick auf die Seite http://www.google.com/intl/de/privacy_ads.html zu werfen. Hier werden einem verschiedene Möglichkeiten geboten, Cookies, z.B. für interessensbasierte Werbung, dauerhaft zu deaktivieren:

> *Alle Nutzer können die Verwendung des DoubleClick-Cookies (für AdSense-Websites, die DoubleClick-Anzeigenschaltung und bestimmte Google-Services, die das DoubleClick-Cookie einsetzen) durch Klicken auf die oben angezeigte Schaltfläche jederzeit deaktivieren. Zudem bietet Google eine Reihe von Optionen zur dauerhaften Speicherung der Browser-Einstellungen mit dieser Deaktivierungseinstellung. Google gestattet außerdem Drittanbietern das Schalten von Anzeigen im Content-Werbenetzwerk von Google. Mithilfe eines Tools der Netzwerkwerbeinitiative (Network Advertising Initiative, NAI) können Sie den Erhalt von Cookies mehrerer Online-Werbevermarkter und Werbenetzwerke gleichzeitig deaktivieren. Google setzt Cookies für Google Analytics und Conversion-Tracking ein. Weitere Informationen hierzu erhalten Sie in den nachfolgenden häufig gestellten Fragen…*

Auf selbiger Seite sind einige Links zu weiteren Informationen vorhanden, so z.B. auch ein Link zu einer Auflistung der Interessen, die Google aus dem Surfverhalten abgeleitet hat; einschließlich der Möglichkeit, dies zu entfernen (siehe Abbildung 21).

Weitere Google-Suchen

Neben der Websuche und spezielleren Suchen wie Google Scholar gibt es weitere Inhalte, nach denen explizit gesucht kann. Dazu zählen Bilder, Videos, News, Produkte und Patente, von denen letztere drei noch ganz kurz erläutert werden sollen:

- Google News: Volltextsuche in Nachrichten mehrerer hundert entsprechender Quellen (Spiegel Online, Welt Online etc.), die zeitnah aktualisiert werden. Aktuelle Nachrichten werden in den Suchergebnissen bevorzugt.
- Google Produktsuche: Suchmaschine für kommerzielle Produkte mit der Möglichkeit des Preisvergleichs.
- Google Patentsuche: Bisher nur in den USA verfügbarer Suchdienst für Patente. Die Datenbank enthält 7 Millionen US-Patente seit dem Jahr 1790. Den Dienst kann man als Ableger von Google Books bezeichnen, denn die Bestände des US-Patentamts wurden und werden auf die gleiche Art und Weise erfasst (vgl. Dambeck 2006).

Abbildung 21: Von Google auf Basis von Cookies abgeleitete, persönliche Interessen

4.2.3.31 YouTube

Google-Konto erforderlich: Je nach Funktionalität

Beschreibung: YouTube ist ein Videoportal, bei dem Kurzfilme hochgeladen und angeschaut werden können. Für den Upload von Videos sowie für weitere Funktionalitäten wie das Verfassen von Bewertungen und das Verwalten von Playlists wird allerdings ein Konto benötigt. Jeder Nutzer hat einen eigenen Kanal (siehe Abbildung 23). Hier sind hochgeladene Videos, Favoriten, das Profil, Abonnements usw. sichtbar. Jeder Kanal kann von beliebigen Nutzern abonniert werden. Bei dem Konto muss es sich nicht um ein Google-Konto handeln, hier reicht ein YouTube-Konto aus. Dies ist allerdings von geringer Bedeutung ist, da es mit einem Google-Konto verknüpft werden muss (siehe Abbildung 22). Google's versuchte Begründung für die Notwendigkeit dieser Verknüpfung wirkt leicht lächerlich…

Abbildung 22: Verknüpfung des YouTube-Kontos mit dem Google-Konto

Mehrwert: Bei der Mehrwertbetrachtung muss man natürlich unterscheiden, ob man sich nur Videos anschaut oder ob man selber Inhalte zur Verfügung stellt. Man findet sehr viele, zum Teil auch interessante Videos auf YouTube. Immer mehr Unternehmen bzw. Institutionen schalten zudem eigene Kanäle um interessierten Nutzern aktuelle Informationen zur Verfügung zu stellen. Dementsprechend ist auch das zur Verfügung stellen von Inhalten für Unternehmen etc. ein echter Vorteil, um sich der Öffentlichkeit zu präsentieren. Ob es allerdings für den privaten Nutzer ein echter Vorteil ist, seine Videos zu veröffentlichen, darf zumindest bezweifelt werden. Der Zugriff auf eine Fülle von kostenlosen Videoclips zu den unterschiedlichsten Themengebieten ist jedenfalls ein Mehrwert.

Risiken: Da jeder Nutzer jedes Video online stellen und weltweit verfügbar machen kann, spielen hier die Privatsphäre und das Urheberrecht eine wichtige Rolle. Die Privatsphäre, da man jederzeit ein Video auf YouTube finden könnte, das einen selbst, den Namen oder ähnliches zeigen könnte, mit dessen Veröffentlichung man aus diversen Gründen nicht einverstanden ist. Ähnlich sieht es bei urheberrechtlich geschütztem Material aus: Jeder der in Besitz solcher Inhalte ist, kann sie hochladen und weltweit verfügbar machen. Jedenfalls kann erst einmal fast alles hochgeladen werden und bei Beschwerden werden die Inhalte dann von Google entfernt (Opt-out). Für bestimmte urheberrechtlich geschützte Inhalte gibt es auch automatisierte Filter, aber die Trefferquoten lassen doch sehr zu wünschen übrig. Wenn man z.B. auf einen Musiktitel stößt, der in Deutschland (wg. Urheberrechtsverletzungen) gesperrt ist, findet man ziemlich schnell den gleichen, nicht gesperrten Titel. Soviel zu Inhalten, die andere Nutzer auf YouTube veröffentlichen können. Über sich selbst kann man natürlich auch einige persönliche Informationen preisgeben. Dementsprechend kann man seinem Profil beispielsweise Informationen wie vollständiger Name, Standort und berufliche Daten hinzufügen. Videos, die man hochlädt oder sich anschaut sowie weitere Informationen werden alle mit dem Google-Konto verknüpft. Im eigenen Kanal werden standardmäßig Informationen veröffentlicht wie z.B. die letzten Aktivitäten (siehe Abbildung 23, http://www.youtube.com/user/2010datenschutz).

Risikoverminderung: Möchte man einfach nur Videos anschauen, sollte man vorsichtshalber auf eine Anmeldung verzichten. Dann wird auch nicht in der Webhistorie gespeichert, nach welchen Videos man gesucht und welche man sich angeschaut hat. Der eigene Kanal kann deaktiviert oder so angepasst werden, dass nur noch die gewünschten Informationen dort angezeigt werden (Opt-out). Standardmäßig finden andere Nutzer Statistiken und Daten zu den eigenen Videos. Auch diese Option kann deaktiviert werden. Möchte man einen eigenen Kanal veröffentlichen, sollte man dafür ein gesondertes Konto anlegen, das man dann strikt vom privaten Gebrauch von YouTube trennt. Lädt man Videos hoch, kann man auswählen, dass diese nicht gelistet und somit nur für Personen sichtbar sind, die über den generischen Videolink verfügen (Opt-in). Diese benötigen dann kein Konto, um auf das Video zugreifen zu können. Markiert man ein Video hingegen als privat, so haben bis zu 25 ausgewählte YouTube-Nutzer Zugriff auf das Video. Von den gerade genannten Optionen sollte man bei „Opt-out“ so viele wie möglich deaktivieren und bei „Opt-in“ so wenig wie nötig aktivieren.

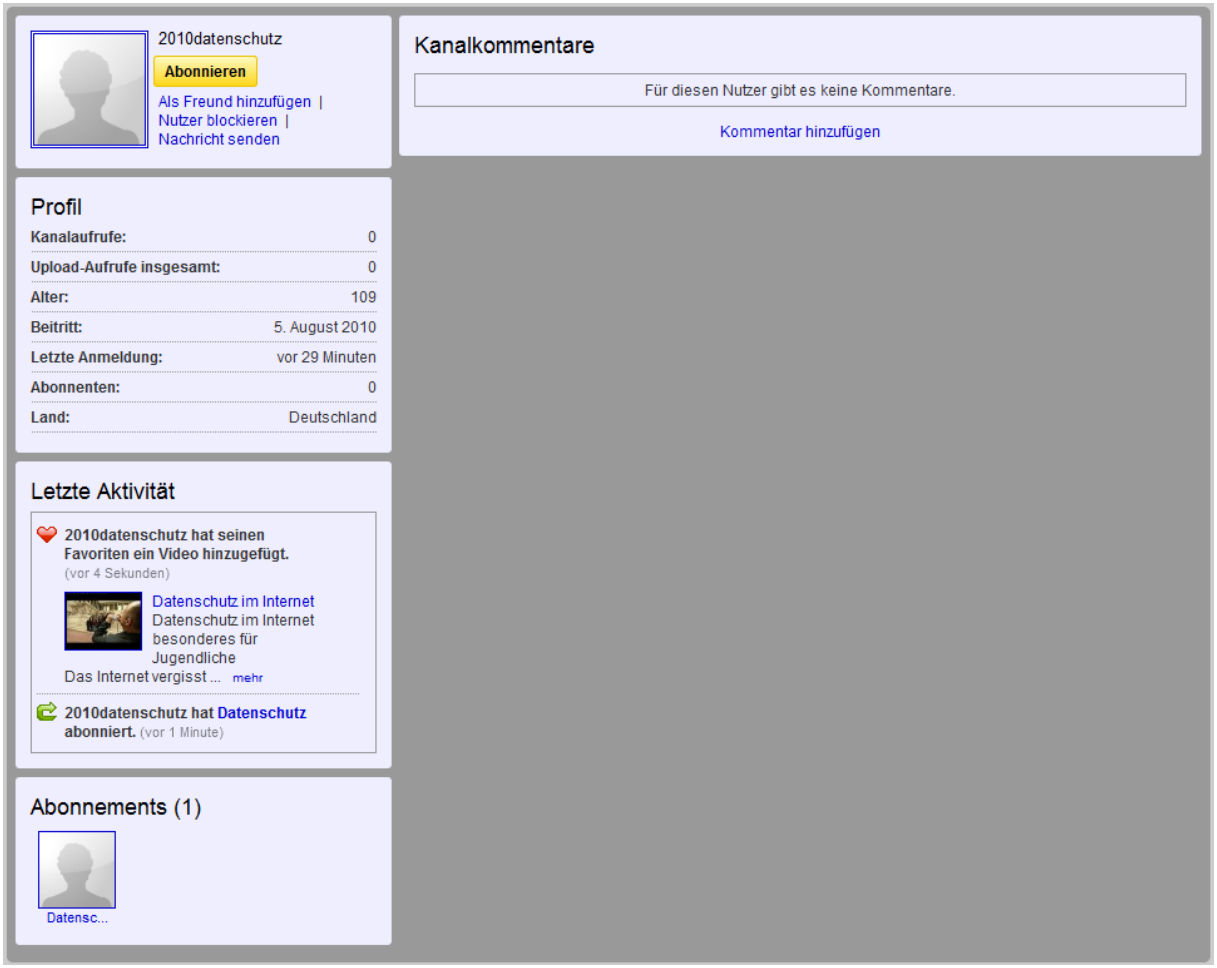


Abbildung 23: YouTube-Kanal

4.2.4 Cloud Computing

Cloud Computing basiert auf den Technologien Virtualisierung, serviceorientierte Architekturen (SOA) und Web Services. Insgesamt wird beim Cloud Computing zwischen einer Virtualisierung von Betriebssystemen, Plattformen, Speicher, Netzwerken und Anwendungen unterschieden. Es können ganze IT-Infrastrukturen virtualisiert und als Dienste realisiert und angeboten werden. Diese stehen zur Nutzung in einer serviceorientierten Architektur zur Verfügung. Auf die Dienste kann dann On-Demand zugegriffen werden. Eine Abrechnung kann dynamisch, auf Basis der in Anspruch genommenen Leistungen vorgenommen werden. Google hingegen verfolgt natürlich den Ansatz, die angebotenen Dienste durch Werbung zu finanzieren. Allerdings ist das nicht in allen Fällen möglich, denn virtualisierte Hardware und Laufzeitumgebungen bieten hierfür keine passenden Werbeflächen.

> *Cloud Computing erlaubt die Bereitstellung und Nutzung von IT-Infrastruktur, von Plattformen und von Anwendungen aller Art als im Web elektronisch verfügbare Dienste. Der Begriff Cloud soll dabei andeuten, dass die Dienste von einem Provider (bzw. Intranet eines größeren Unternehmens) erbracht werden. […] Cloud-Ressourcen sind in der Regel virtualisiert. Der Cloud-Nutzer hat dadurch stets eine wunschgemäße, beliebige Sicht auf seine Infrastruktur und es gibt in diesem Fall keine systembedingten Abhängigkeiten oder Zwangsbedingungen für seine Anwendungen* (Baun et al. 2010: 1f).

Cloud Computing verfolgt das Paradigma Everything as a Service (XaaS) mit seinen Hauptvertretern Infrustructure as a Service (Iaas), Platform as a Service (PaaS) und Software as a Service (SaaS). Bei IaaS wird den Benutzern eine abstrahierte Sicht auf Hardware angeboten, d.h. auf Rechner, Massenspeicher, Netzwerke etc. PaaS richtet sich mehr an Entwickler als an Endnutzer. In Entwicklungsumgebungen können Anwendungen entwickelt und in Ausführungsumgebungen ausgeführt und bereitgestellt werden. SaaS dient dazu, Software für deren Anwender zentral bereitzustellen. Anwendungsdaten werden dabei auf Servern, also in der Cloud gespeichert. Das SaaS-Angebot kann auf Basis eines Angebots in PaaS oder IaaS beim entsprechenden Provider entwickelt und betrieben werden. Es wird zwischen Anwendungsdiensten und Anwendungen unterschieden. Anwendungsdienste basieren im Wesentlichen auf einer einzigen einfachen Applikation, i.d.R. realisiert durch einen Web Service. Anwendungen dagegen können vollwertige komplexe Applikationen sein, die z.B. durch eine Orchestrierung einzelner Web Services realisiert werden (vgl. Baun et al. 2010: 28ff).

Anwendungen, die im Rahmen von SaaS bereitgestellt werden, können deutlich komplexer sein als herkömmliche Webanwendungen. Das Problem dabei ist, dass Browser ursprünglich nicht dafür ausgelegt waren, solch komplexe Anwendungen auszuführen, sie dienten nämlich nur dem Aufruf einfacher Webseiten. Deshalb hat Google drei Technologien entwickelt: Chrome, Native Client und Gears. Im Gegensatz zum Firefox, Internet Explorer etc. soll Google Chrome ein „Cloud Client“ sein. Ein zentrales Konzept bei diesem Browser ist die Aufteilung in nicht nur optisch, sondern auch prozesstechnisch getrennte Browser-Tabs: Dementsprechend funktioniert jede Registerkarte bzw. jeder Tab als eigener Prozess. Durch diese Trennung bleiben die anderen Registerkarten bei Absturz oder Funktionsstörung einer Registerkarte unbeeinträchtigt und die Nutzer können weiterarbeiten. Mit dem Native Client sollen Anwendungen im Rahmen von SaaS näher an den Prozessor des lokalen Rechners rücken, denn damit lässt sich nativer Code (Maschinencode) direkt im Browser ausführen. Dadurch lässt sich die Ausführung von Anwendungen enorm beschleunigen. Eine Bildbearbeitungssoftware in der Cloud könnte somit bei einer aufwändigen Bearbeitung eines Bildes theoretisch genauso schnell reagieren wie eine lokale Software. Im Endeffekt können Entwickler so die volle lokale Prozessorleistung nutzen und dennoch browser- und betriebssystemunabhängigen Code schreiben. Gears schließlich soll die Lücke zwischen internetbasierten und lokalen Anwendungen schließen. Ziel ist es, dass Anwendungen auch ohne ständigen Zugriff auf das Internet genutzt werden können, was insbesondere in Bezug auf die Ausfallsicherheit (bei Netzwerkstörungen) enorm wichtig ist.

Google Chrome ist allerdings irgendwo doch nur ein Webbrowser, der ein Betriebssystem benötigt. Wenn jedoch die Dienste (Software, Plattformen und IT-Infrastruktur) über das Internet bereitgestellt werden und auch die Daten dort gespeichert werden, rücken lokale Hardware wie z.B. Festplatten, Anwendungen und auch umfangreiche Betriebssysteme in den Hintergrund. Dementsprechend wird sowohl Hardware als auch das Betriebssystem im Sinne von Thin Clients immer „schmaler“, allerdings keineswegs überflüssig. Denn auch Google Chrome benötigt eine Laufzeitumgebung. Für diesen Zweck hat Google Chrome OS entwickelt. Dabei handelt es sich um eine Version des Chrome-Browsers, die auf einem Linux-Kernel basiert (vgl. Kaumanns/Siegenheim 2009: 307ff).

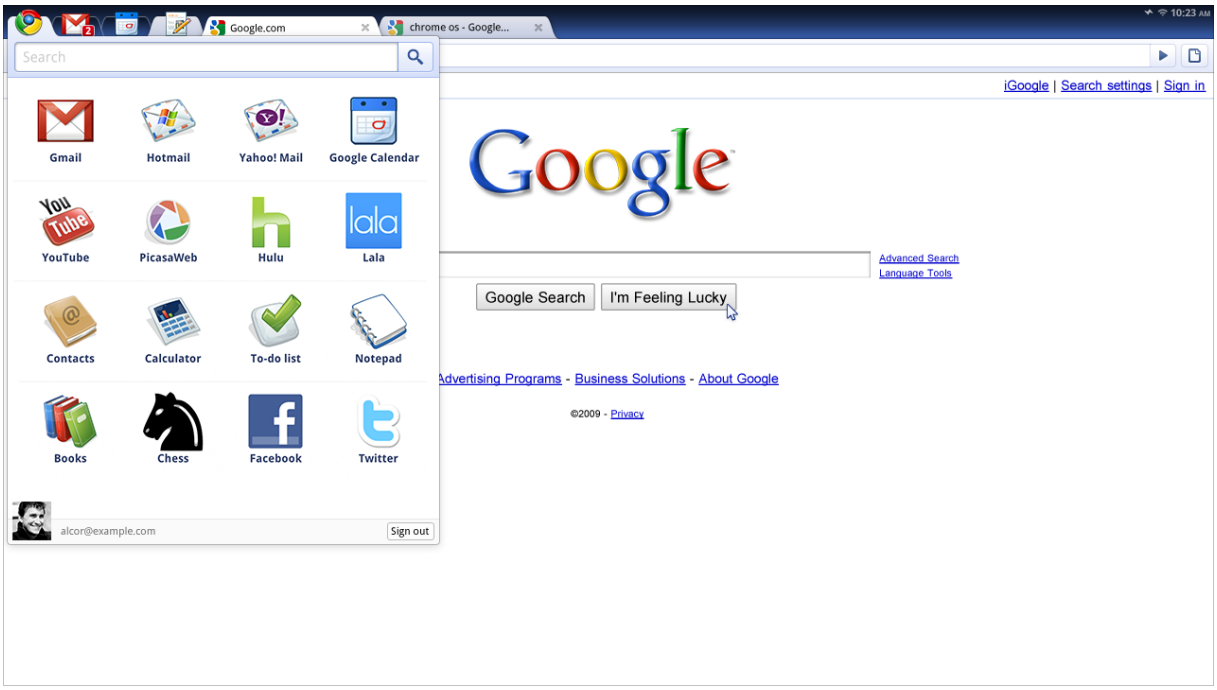


Abbildung 24: Die GUI von Google Chrome OS (Quelle: http://de.wikipedia.org/wiki/Chrome_OS)

Laut einer Google-Studie könnten 60 Prozent der weltweiten Arbeitsplatzrechner in Unternehmen besser und schneller funktionieren, wenn man Windows durch Chrome OS ersetzen würde, was sofort möglich wäre. Die Studie stützt sich darauf, dass ca. 60 Prozent der Windows-Rechner, die in den Firmen zum Einsatz kommen, nur für Aufgaben genutzt werden, die auch über Chrome OS realisiert werden könnten. Veröffentlicht hat die groß angelegte Studie der Vize-Präsident von Google's Entwicklungsbereich, Linus Upson (vgl. Hiner 2010). Im Dezember 2010 hat Google das Notebook CR-48 vorgestellt. Es ist das erste Notebook mit Chrome OS und wurde ersten privaten Testern in den USA ausgeliefert. Nun ist also das CR-48 Google's Schnittstelle zwischen Nutzer und Cloud. Als Schnittstellen hat es lediglich einen USB-Port, einen SD-Kartenslot, einen VGA-Ausgang sowie eine kombinierte Mikrofon/Audiobuchse. Zur Verbindung mit der Cloud verfügt es außerdem über einen WLAN- und einen UMTS-Anschluss (vgl. Thommes 2010).

> *Das CR-48 ist auf Googles Webdienste sowie die Cloud ausgelegt. Ohne Anmeldung bei Googlemail, Google-Docs oder anderen Google Diensten kommt man nicht weit, selbst das Drucken läuft über Cloud-Print. Einen Dateimanager gibt es nicht, Google sieht einen Zugriff auf das darunterliegende Linux-Dateisystem nicht vor. […] Dokumente werden ausschließlich im Web bearbeitet* (Thommes 2010).

Dass Chrome OS Windows einmal ersetzen wird darf jedoch bezweifelt werden, denn Unternehmen präferieren aus Datenschutzgründen natürlich eine Speicherung der Daten im eigenen Intranet. Dazu kommt, dass auch Microsoft beim Cloud Computing aktiv ist. So soll Windows 8 „das erste total virtualisierte Betriebssystem" werden. Es soll von lokaler Hardware unabhängig sein und somit z.B. auch einen Zugriff von einem Smartphone aus ermöglichen. Daten und Dokumente werden dann in der Cloud, im Falle von Windows 8 auf den Servern von Microsoft, gespeichert (Knobel 2010). Nun wurde Google Chrome als Cloud-Client betrachtet, im Folgenden sollen noch ein paar Cloud-Angebote und Werkzeuge von Google genannt werden (Baun et al. 2010: 29ff).

- Infrastructure as a Service: Google Big Table, Google File System
- Platform as a Service: Google App Engine
- Software as a Service: Google Docs, Google Maps API, OpenSocial

Auf jeden Fall bleibt festzuhalten, dass Cloud Computing ein sehr wichtiges Thema für Google ist, denn eine Bewegung hin zur Cloud bedeutet für Google mehr Daten bzw. Informationen und zugleich mehr Werbeflächen. Das sind wohl die Hauptgründe für die immensen Investitionen von Google in diese Technologie. Für den Nutzer heißt das wieder einmal: Kostenlose, durch kontextsensitive Werbung finanzierte Cloud-Angebote. Auf der anderen Seite birgt das Cloud Computing ein enormes Datenschutz-Risiko: Daten und Informationen, die normalerweise auf der lokalen Festplatte oder auf Wechseldatenträgern gespeichert werden, „wandern" nun in die Cloud und liegen auf den Servern von Google, natürlich verknüpft mit dem Google-Konto. Genau das ist auch der Grund, warum sich Unternehmen momentan noch vor dieser Technologie sträuben. Sie möchten nicht, dass ihre Daten die Unternehmensgrenzen verlassen und erst recht nicht, dass sie bei einem Werbeunternehmen lagern.

4.3 Chancen

Welche Möglichkeiten einem die Dienste und Produkte von Google bieten, wurde durch die entsprechenden Einzelbetrachtungen deutlich. Eine spezielle Empfehlung, welche Dienste denn diesbezüglich nun das meiste Potenzial haben, soll nicht ausgesprochen werden. Denn eigentlich muss man die Dienste selbst mal ausprobieren um zu sehen, ob ein individueller Mehrwert besteht oder eben nicht. So könnte der eine Dienst für den einen Nutzer gar von großer Bedeutung und für den anderen absolut überflüssig sein. Klar ist jedoch: Die Chancen im Sinne des Mehrwerts sind definitiv vorhanden. Das wurde ja auch in der Einleitung schon angedeutet. In diesem Sinne soll ein Überblick über die wichtigsten Eigenschaften vieler Dienste und Produkte von Google verschafft werden:

- kostenlos
- innovativ
- einmalig
- qualitativ hochwertig
- quelloffen
- intuitiv bedienbar
- unaufdringliche und wenig störend wirkende Werbung

Letztlich soll sich also jeder seine Google-Dienste selber frei aussuchen und dabei anhand des jeweiligen Mehrwerts und der Risiken inkl. möglicher Verminderungsmaßnahmen, entscheiden, ob man einen Dienst nutzen möchte, oder aber nicht. Bei den Verminderungsmaßnahmen handelt es sich vor allem um die Wahlmöglichkeiten bezüglich des Datenschutzes (Opt-out).

4.4 Risiken

> *Sie gehen eine Straße hinunter. Wir wissen ungefähr wer Sie sind, was für Sie wichtig ist, wer Ihre Freunde sind.* (Google CEO Eric Schmidt gegenüber Journalisten nach Diederichs 2010)

Nachdem die Risiken der verschiedenen Dienste im Einzelnen analysiert und bewertet wurden, geht es nun darum, diese im Gesamtkontext zu betrachten. Dabei soll kurz erläutert werden, warum es ein Problem darstellt, wenn viele personenbezogene Daten auf Google's Servern liegen und mit dem Google-Konto verknüpft sind. Es geht also darum, die Bedeutung von „Google weiß alles über Sie" näher zu betrachten, denn hierin sehen viele Nutzer anscheinend kein Problem. Das größte Problem ist wohl die Datenkonzentration bei nur einem Anbieter, nämlich Google. Diese Konzentration findet deshalb statt, weil Google die vielen unterschiedlichen Dienste anbietet, bei deren Nutzung oft ein Google-Konto notwendig ist. In diesem Konto laufen dann sämtliche, personenbezogene Daten zusammen. Aber auch wenn ein solches Konto nicht notwendig ist, können die erhobenen Daten auf anderem Wege verknüpft werden, z.B. per Cookies. Übrigens bestätigt Google grundsätzlich die Zusammenführung solcher, in verschiedenen Diensten erhobenen Daten (Kaumanns/Siegenheim 2010: 142). Im Blickpunkt steht der gläserne Mensch, denn seine Privatsphäre ist durch die Erhebung und Verknüpfung von verschiedenen personenbezogenen Daten durch einen einzigen Anbieter massiv gefährdet. Würde man viele bzw. alle Google-Dienste nutzen, dann wüsste Google (stets)

- wer man ist und wo man wohnt (*Buzz, Checkout, Gmail, Profiles* etc.)
- welche sozialen Kontakte man pflegt (*Buzz, Gmail, Orkut, Talk, Voice* etc.)
- wo man sich gerade aufhält (Ortung per GSM-Zelle, GPS oder WLAN bei Google's mobilen Diensten wie *Latitude, Navigation* oder *Near me now*; potentiell aber auch bei allen anderen Endgeräten, die WLAN-Signale empfangen)
- wo man hinwill (*Earth, Maps, Navigation* etc.)
- welche Termine man hat (*Kalender, Sync* etc.)
- welche Interessen man hat (diverse Suchdienste sowie weitere Dienste und Produkte wie *Analytics, Blogger.com, Buzz, Chrome, Gmail, Groups, iGoogle, Knol, Toolbar, YouTube* u.v.m.)
- wie die Bankverbindung von einem lautet (*Checkout*)
- wer die Partner bei eigenen Finanzgeschäften sind, was man kauft, wie viel man dafür ausgibt und wann diese Geschäfte abgewickelt werden (*Checkout*)
- welche und wie viele Aktien(-fonds) man besitzt und was man diesbezüglich für Transaktionen abwickelt (*Finanzen*)
- wie die eigene DNS aussieht und was für Krankheiten man hat oder hatte, einschließlich entsprechender Therapien (*Health*)
- wie man aussieht (*Buzz, Gmail, Picasa, Profiles* etc.)
- welche Daten man allgemein am eigenen Rechner verarbeitet (*Chrome OS* und weitere Cloud Computing-Angebote)
- usw.

„Google weiß alles" bedeutet in diesem Zusammenhang, dass ausführliche Persönlichkeitsprofile im Internet, bei einem gigantischen Konzern, lagern. Bleibt die Frage zu beantworten, was daran denn nun so schlimm sein soll, schließlich unterliegen sie bei Google, doch strengen

Datenschutzbestimmungen. Dabei handelt es sich sowohl um technische als auch organisatorische Maßnahmen zum Datenschutz. Dass Google der Schutz der Daten seiner Nutzer wirklich wichtig ist und die Daten bei Google vermutlich sogar besser geschützt sind als bei Konkurrenten, zeigt folgendes Beispiel: Im August 2005 verlangte das US-Justizministerium unter Strafandrohung von Google, AOL, Microsoft und Yahoo die Herausgabe der Suchanfragen zweier Monate und aller URLs in ihrem Verzeichnis, um die Durchsetzung eines Gesetzes gegen Internetpornographie zu unterstützen. Alle Unternehmen außer Google kamen diesen Forderungen umgehend nach. Google jedoch wehrte sich gerichtlich dagegen, weil es sich um einen Phishing-Feldzug ohne plausiblen Grund handele. Am Ende gelang es Google, die Zahl der übergebenen URLs auf 50.000 zu beschränken und es musste nicht die Suchbegriffe seiner Nutzer mitteilen (Brandt 2010: 127).

Trotzdem lagern die Daten auf Google's Servern und sind dort grundsätzlich weder vor gerichtlichen Zugriffen noch vor eigens verursachten Datenschutzpannen, wie sie es ja durchaus schon gegeben hat (siehe z.B. Google Buzz und Google Text & Tabellen in den Abschnitten 4.2.3.5 und 4.2.3.26), geschützt. Womöglich sind sie auch nicht ausreichend vor Hackern oder aber individuellen Fehlern bzw. Angriffen eigener Google-Mitarbeiter geschützt. Ein Beispiel für einen solchen individuell verursachten Fehler ist eine bekannte Datenpanne bei AOL aus dem Jahre 2006: Ein Mitarbeiter stellte die Suchdaten von mehr als 600.000 AOL-Nutzern versehentlich online. IP-Adressen wurden nicht genannt, dafür alle Suchanfragen mit Zeitstempel sowie die angeklickten Webseiten. Dabei konnte nachgewiesen werden, dass die Informationen aus den Suchprofilen in manchen Fällen durchaus ausreichen, um trotz Anonymisierung die Identität einzelner Personen zu enthüllen (Kaumanns/Siegenheim 2009: 144).

Dass viele der erfassten Daten gegen einen Nutzer verwendet werden könnten, wenn sie in die falschen Hände gelangen, ist eigentlich offensichtlich. Hier gibt es viele mögliche, vorstellbare Szenarien. Das könnten natürlich auch Nutzer zu spüren bekommen, die ja nichts zu verbergen haben. Die Wahrscheinlichkeit, dass dieses Risiko eintritt, ist wohlbemerkt sehr gering, dennoch besteht es und die Auswirkungen könnten verheerend sein. Deshalb muss man dieses Risiko vermindern, wenn man schon die Gelegenheit dazu hat, will man doch auf die Chancen nicht verzichten. Die Alternative wäre wohl die Aufgabe der Privatsphäre. Unterkapitel 4.4.1 widmet sich nochmal detaillierter der Datenschutzproblematik und den damit verbundenen Risiken für Nutzer. Unterkapitel 4.4.2 hingegen beschäftigt sich mit einer möglichen Verknüpfung von personenbezogenen Daten und einer dienstübergreifenden Korrelation.

> *Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun.* (Google CEO Eric Schmidt in einem CNBC-Interview nach Stöcker 2010)

Ein weiterer Angriffspunkt ist das Google-Konto. Angreifer könnten versuchen das Passwort zu knacken, wenn sie im Besitz der E-Mail-Adresse sind. Ein eher geringes Problem solange man sichere Passwörter wählt und selbiges gewährleistet schließlich ein entsprechender Prüfmechanismus, der dem Nutzer anzeigt, wie sicher sein Passwort ist. Die Ergebnisse waren hier allerdings erschreckend. Das Passwort „passwort" wurde folgerichtig als schwach eingestuft. Das Passwort „christoph" wurde hingegen als angemessen bewertet, unabhängig davon, ob ein „christoph" in der E-Mail-Adresse vorkommt oder nicht. Das Passwort „datenschutz" wurde sogar als stark eingestuft. Immerhin muss man sich nach drei Falscheingaben einer visuellen

Verifizierung unterziehen. Dabei muss man einen schlecht leserlichen Text, der als Grafik erscheint, eingeben.

Bei der Betrachtung der Risiken ist es auch wichtig, zu berücksichtigen, dass Google ein Wirtschaftsunternehmen ist. Die dazugehörige Branche lautet „Data Mining“ und in dieser werden halt Daten an Werbekunden oder andere Firmen verkauft. Es gibt allerdings keinerlei Hinweise, dass Google dies jemals getan hat und die Gründer versprechen, dass Google dies niemals tun wird. Dieses Versprechen können sie allerdings nur einhalten, solange sie das Sagen bei Google haben (vgl. Brandt 2010: 124).

Bei Google's meisten Diensten (und übrigens auch bei denen der Konkurrenz) ist es so: Erklärt man sich nicht mit den Nutzungs- und Datenschutzbestimmungen einverstanden, nutzt man diesen Dienst einfach nicht. Was das anbelangt nehmen einige Dienste von Google allerdings eine Sonderstellung ein, denn auch Nutzer, die keine Dienste und Produkte von Google nutzen, sind nicht sicher davor, dass Google Informationen über sie sammelt. Wer im Internet surft, der wird wohl kaum an Google Analytics vorbeikommen. Ohne dass es ihm (wohlbemerkt nicht unbedingt ein Google-Nutzer) gewahr wird, sammelt Google hier Daten über ihn. Ein weiteres Beispiel dafür, dass selbst Menschen betroffen sind, die vielleicht sogar nicht mal das Internet nutzen, ist Google Street View. Vielleicht taucht man selbst oder sein Eigentum ja auf irgendeinem Foto im Internet auf, ohne dass man davon etwas mitbekommt. Vielleicht werden aber auch die eigenen WLAN-Daten von Google erfasst. Hier wird es Unwissenden (und das sind enorm viele) sehr schwer gemacht, sich zur Wehr zu setzen. Sie können nur hoffen, dass Datenschützer und andere Politiker dies stellvertretend für sie tun. Das ist ja auch in den gerade genannten Fällen, zumindest in Deutschland, der Fall.

Ein interessanter Aspekt und eine weitere Gefahr für Unbeteiligte ist es auch, dass jeder Google-Nutzer Adressen, Telefonnummern etc. zu seinen Google-Kontakten abspeichern kann (vgl. Abbildung 25). Somit können andere Leute gekennzeichnete Informationen (man könnte diese Informationen theoretisch ja auch als Freitext speichern) über einen mit dem Google-Konto verknüpfen, ohne, dass man davon etwas mitbekommt. Infolgedessen wird man von Google-Nutzern und deren Affinität zu Datenschutz abhängig. Was nutzt es da noch, wenn man sich ein anonymes Konto angelegt hat, seine Kontakte dieses jedoch ggf. mit dem echten Namen und der echten Adresse verknüpfen?

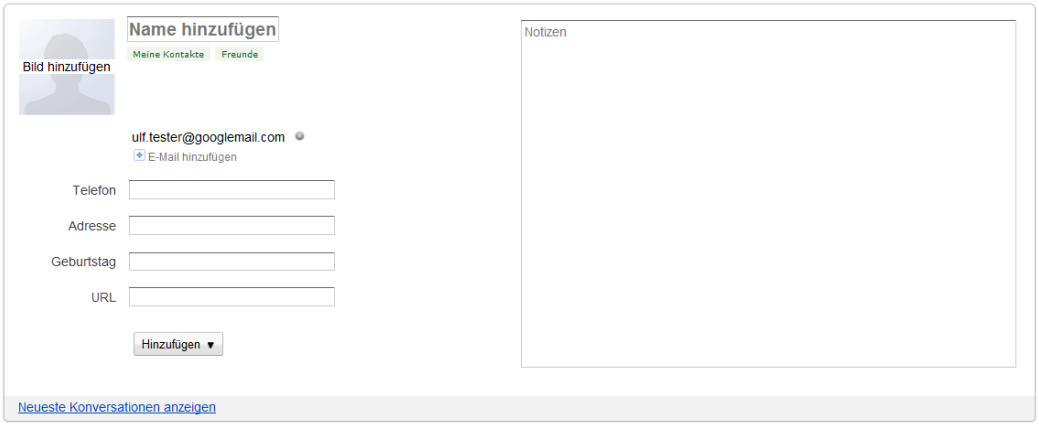


Abbildung 25: Kontakte bearbeiten

4.4.1 Datenschutz, informationelle Selbstbestimmung und allgemeine Risiken

4.4.1.1 Datenschutz

Die Datenschutzdebatte hatte ihren Ursprung in den 60er-Jahren in den USA und bezog sich auf das Recht auf Privatsphäre, das erstmals in „Right to Privacy" erwähnt wurde. Dabei handelt es sich um einen berühmten Aufsatz aus dem Jahr 1890: Samuel Warren und Louis Brandeis vertraten die These, dass „nicht erst die physische Beeinträchtigung von Rechtsgütern wie körperlicher Zwang, Entzug der Freiheit oder Eingriffe in das Eigentum rechtlich von Bedeutung sind, sondern bereits das Sammeln von Informationen". Im Wortlaut hieß es in dem Aufsatz: „Das Recht sichert jedem Individuum das Recht zu, grundsätzlich zu bestimmen, in welchem Ausmaß seine Gedanken, Gefühle und Empfindungen anderen mitgeteilt werden." Der Aufsatz war damals eine Reaktion auf indiskrete Veröffentlichungen in der Boulevardpresse, die gerade ihren Aufschwung nahm (Garstka 2003: 50f).

Erste datenschutzrechtliche Bestimmungen resultieren in Europa im Wesentlichen aus der Abwehr absolutistischer Vorgehensweisen, bei denen der Staat zur Erfüllung seiner Aufgaben personenbezogene Daten erhob. Diese Erhebung war aus Sicht der Betroffenen willkürlich. „Spätestens seit der französischen Revolution von 1789 hatte der inzwischen überwiegend republikanische Staat jedoch dabei die Menschenrechte zu beachten und sich auf seine Aufgaben zu beschränken. Diese Beschränkung wird als klassisches Freiheitsrecht angesehen" (Witt 2010: 25). Datenschutz soll wie folgt definiert werden (vgl. Witt 2010: 6f):

> **Datenschutz ist der Schutz des Einzelnen vor Beeinträchtigung bzw. unerwünschten Folgen, insbesondere durch zweckwidrigen Missbrauch, beim Umgang mit seinen personenbezogenen Daten.**

Bei personenbezogenen Daten wird zwischen unmittelbar personenbezogenen und personenbeziehbaren Daten unterschieden. Erstere sind Daten über persönliche oder sachliche Verhältnisse, die einer eindeutig bestimmten, natürlichen Person direkt zugeordnet werden können (Name, Ausweisnummer, biometrische Daten, Beruf, Arbeitszeiten, Versicherungsdaten, Kundenprofile etc.). Personenbeziehbare Daten sind solche, die durch Ausnutzung von Zusatzinformationen oder durch zeitlichen, personellen oder kostenintensiven Aufwand einer eindeutig bestimmbaren Person zugeordnet, also repersonalisiert werden können (z.B. IP-Adressen und Cookie-IDs).

4.4.1.2 Informationelle Selbstbestimmung

Grundlegend für das Verständnis, den Umfang und die Wirkung des Datenschutzes ist laut Christian C. Witt die grundrechtliche Verankerung des Datenschutzes als informationelles Selbstbestimmungsrecht.

> *Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe seiner persönlichen Daten zu bestimmen.*

So lautete der Leitsatz, mit dem das Bundesverfassungsgericht am 15. Dezember 1983 das Recht auf informationelle Selbstbestimmung als Bestandteil der verfassungsmäßigen Ordnung anerkannte (Garstka 2003: 48). Dieses Recht entstand 1983 im Rahmen des Volkszählungsurteils als das Bundesverfassungsgericht über die Rechtmäßigkeit des einstimmig von Bundestag und Bundesrat verabschiedeten Volkszählungsgesetzes zu entscheiden hatte. Bei dieser Volkszählung sollte in einer umfassenden Totalerhebung die Bevölkerungsstruktur der Bundesrepublik näher untersucht werden. Diese Erhebung wurde aus diversen Kritikpunkten untersagt, dazu zählen die in Abbildung 26 dargestellten. Das Recht auf informationelle Selbstbestimmung betrifft alle Phasen der Datenverarbeitung: Datenerhebung, Verarbeitung (Speicherung, Übermittlung, Veränderung und Löschung) sowie Nutzung. Es wirkt der Gefahr entgegen, dass „vor allem beim Aufbau integrierter Informationssysteme ein teilweise oder nahezu vollständiges Persönlichkeitsbild zusammengefügt werden könne, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren könne“ (Witt 2010: 47ff).

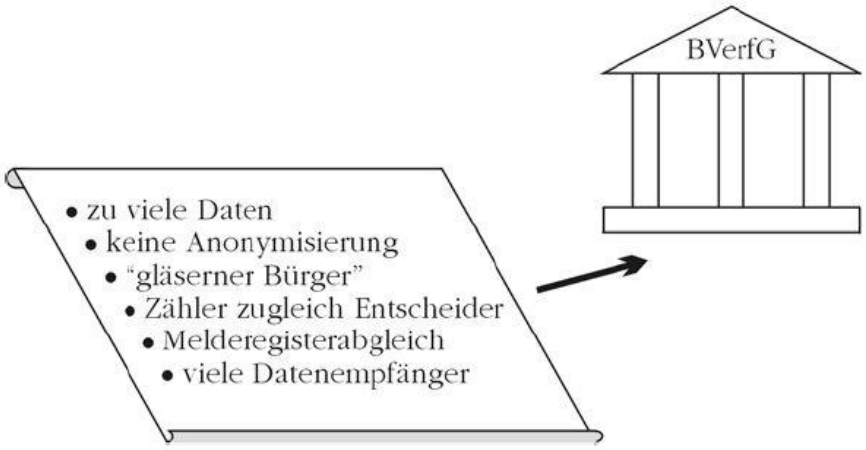


Abbildung 26: Kritikpunkte am Volkszählungsurteil (Witt 2010: 69)

Abschließend sollen noch zwei ausgewählte Zitate zur informationellen Selbstbestimmung nicht unerwähnt werden. Beide verdeutlichen noch einmal die Bedeutung des Datenschutzes:

> *Wenn Meinungsäußerungen, politische Einstellungen, Kommunikationsdaten und Bewegungsprofile erstellt werden, kann sich der Betroffene nicht sicher sein, was mit seinen Daten geschieht und ob diese eines Tages negative Auswirkungen für ihn haben können. Selbstbestimmung weicht dann zunehmend der Fremdbestimmung und die persönliche Freiheit des Einzelnen wird empfindlich eingeschränkt. Für die freiheitlich, demokratische Grundordnung sind Freiräume in denen sich Bürgerinnen und Bürger unbeobachtet fühlen unerlässlich um Meinungsvielfalt und Freiheit zu schützen.* (Bündnis 90/Die Grünen 2011)

> *Man begegnet immer wieder Pharisäern, die davon überzeugt sind, jeder dürfe über sie alles wissen, man habe nichts zu verbergen. Abgesehen davon, dass wohl jeder seine Geheimnisse hat, die er anderen nicht preisgeben möchte, wird dem Einzelnen dabei das wesentliche Risiko nicht bewusst. Das Wissen, dass Außenstehende jederzeit über Daten über das eigene Verhalten verfügen können, wirkt auf das eigene Verhalten zurück. Diese Umkehrung wurde vom Bundesverfassungsgericht eindrucksvoll beschrieben: Wer davon überzeugt ist, dass andere Stellen Daten über seine Verhaltensweisen speichern und weitergeben, wird sein eigenes Verhalten ändern, wird von seinen grundrechtlich verbrieften Freiheitsrechten nicht in dem Maße Gebrauch machen, wie ihm dies die Verfassung garantiert.* (Garstka 2003: 52)

4.4.1.3 Die Datenschutz-Risiken

In diesem Abschnitt sollen nun ein paar Risiken im Einzelnen vorgestellt werden. Dabei geht es vor allem darum, wie Daten bei fehlendem bzw. unzureichendem Schutz so missbraucht werden können, dass dies zu einer Beeinträchtigung des Betroffenen führt.

Verzerrtes Persönlichkeitsbild

Bei der elektronischen Erfassung von Informationen durch Suchmaschinen oder Webtrackern wie Google Analytics wird nicht zwischen wahren und falschen Informationen unterschieden. Es kann also durchaus passieren, dass Daten über Personen verarbeitet und ggf. veröffentlicht werden, die nicht der Wahrheit entsprechen. Dies führt unmittelbar zu verzerrten Persönlichkeitsbildern. Eine solche Verzerrung kann auch entstehen, wenn wichtige Details weggelassen werden (vgl. Bündnis90/Die Grünen 2011, Garstka 2003: 51).

Verfolgung von Personen

Wenn sich Informationen über mögliche Aufenthaltsorte von bestimmten Personen im Internet befinden und unbefugt auf diese zugegriffen wird, kann es passieren, dass diese Personen nirgendwo mehr sicher sind. Das ist besonders kritisch bei verfolgten Opfer häuslicher Gewalt oder wenn diese Personen z.B. durch Stalker belästigt werden. Sind Personen einmal aufgefunden, könnte ihnen ein körperlicher Schaden zugefügt werden (vgl. Bündnis 90/Die Grünen 2011, Witt 2010: 22). Neben einer solchen Verfolgung durch beliebige Personen(gruppen) spielt auch eine Verfolgung durch staatliche Behörden eine wichtige Rolle. Dazu zählen vor allem Strafverfolgungsbehörden aber auch Sicherheits- und Geheimdienste, die auf der Suche nach Spuren im Internet sind. Dabei suchen sie nach Informationen, um z.B. Straftäter zu überführen. Dabei kann es auch vorkommen, dass Unschuldigen Schaden zugefügt wird, wie die kleine Fallsammlung in Kapitel 4.4.1.4 zeigt. Eine wichtige Rolle spielen hier Rasterfahndungen, die in Deutschland erstmals in den 70er-Jahren bei der Fahndung nach RAF-Terroristen durchgeführt wurden:

> *Bei einer Rasterfahndung werden personenbezogene Daten aus unterschiedlichen Datenbeständen anhand eines vorgegebenen Rasters (etwa entsprechend dem konkret vorliegenden Täterprofil) miteinander verglichen und zusammengeführt. Sofern der maschinelle Datenabgleich nicht anhand des Namens, sondern etwa bestimmter Eigenschaften (z.B. Barzahler von Stromrechnungen oder Angehöriger einer Glaubensgemeinschaft) erfolgt, steht nicht mehr der konkrete Tatverdacht bezüglich einer Person zu Beginn des Datenabgleichs im Vordergrund: Sicherheitsbehörden hoffen, damit Personen ermitteln zu können, von denen möglicherweise eine konkrete Gefährdung der inneren bzw. äußeren Sicherheit ausgehen könnte (Gefahrenprävention).*
>
> *Da die Gefahr einer fehlerhaften Abbildung der Wirklichkeit im Rahmen des gewählten Datenmodells nicht ausgeschlossen werden kann und Betroffene nicht als Sache zu behandeln sind, resultierte daraus eine verstärkte Besinnung darauf, dass es beim Datenschutz um den Schutz von Persönlichkeitsrechten geht.* (Witt 2010: 26f)

Erhebliche Demütigung

Im vorherigen Abschnitt wurde bereits erwähnt, dass verfolgten Personen ein körperlicher Schaden zugefügt werden könnte. Darüber hinaus kann Personen ein geistiger Schaden zugefügt werden, indem sie gezielt mit Informationen, die ihre Person betreffen, gemobbt, gedemütigt und/oder entwürdigt werden (vgl. Witt 2010: 22).

Belästigung durch Werbung

Stalking und Mobbing (s.o.) sind zwar auch Formen der Belästigung, hier sind jedoch diverse Werbemaßnahmen gemeint, die als aufdringliche Belästigung aufgefasst werden können. Dazu zählen sowohl Anrufe, Briefe und E-Mails von Unternehmen, die etwas verkaufen möchten, aber auch beispielsweise Versuche, Personal an- bzw. abzuwerben. Spam ist ein bekanntes Beispiel für solche Belästigungen durch Werbung.

Identitätsdiebstahl

Beim Identitätsdiebstahl (englisch: Identity Theft) nehmen Personen die Identität anderer Personen an (oder versuchen dies), um sich hierdurch einen Vorteil zu verschaffen. Im Rahmen dieser Ausarbeitung soll grob zwischen vier Gründen für einen Identitätsdiebstahl unterschieden werden (vgl. http://www.idtheftcenter.org/):

- **Vertuschung krimineller Handlungen**: Straftaten werden unter falscher Identität begangen, um selber nicht für sie haften zu müssen.
- **Finanzielle Vorteile**: Ausnutzung einer anderen Identität, um Kredite zu erhalten oder Waren und Dienstleistungen in Anspruch zu nehmen, die nie bezahlt werden.
- **Klonen einer Identität**: Annehmen einer anderen Identität im Alltag. Die Gründe dafür können sehr diffus sein.
- **Medizinische Gründe**: Vortäuschen der falschen Identität, um gesundheitliche Leistungen, allem voran Arzneimittel in Anspruch zu nehmen.

Dabei fällt das Annehmen digitaler Identitäten besonders leicht, vor allem wenn Personenprofile im Internet zugänglich sind. Dass bereits der Name und das Geburtsdatum einer Person für einen Identitätsdiebstahl ausreichen können, zeigt das Fallbeispiel von Frau Groll (siehe Kapitel 4.4.1.4). Identitätsdiebstahl ist laut Polizei eines der am stärksten zunehmenden Delikte im Internet mit einem großen Schaden für die Wirtschaft. Durchschnittlich 400 Stunden müsse man rechnen, um den persönlich entstandenen Schaden wiedergutzumachen (vgl. Groll 2010).

4.4.1.4 Datenmissbrauch: Ausgewählte Fallbeispiele

Fernab der Theorie sollen die folgenden Beispiele zu Fällen von Datenmissbrauch die Risiken, die mit mangelndem Datenschutz verbunden sind, illustrieren. Es gibt nämlich erschreckenderweise viele Leute, für die sind diese Gefahren und die Bedenken von Datenschützern nur irgendwelche Paranoia. Die ersten beiden Beispiele entstammen einem Beitrag des Nachrichtenportals „Zeit Online“ von Tina Groll (Groll 2010), die selbst Opfer eines Identitätsdiebstalls wurde. Die weiteren Beispiele haben ihre Herkunft aus einer umfangreichen Sammlung von Fällen von Datenmissbrauch und -irrtum. Dort sind auch Verweise zu den ursprünglichen Quellen zu finden (Breyer 2008).

- Schulden soll Frau Groll gemacht und Waren bezogen haben, von Unternehmen, deren Namen sie zuvor noch nie gehört hatte. Die Sachen wurden an Adressen geliefert, die nicht ihr gehören. Laut Inkassounternehmen konnten Menschen, die dort wohnen zweifelsfrei bezeugen, dass auch Frau Groll dort gewohnt habe. Sogar Haftbefehle gegen sie lagen vor. „Es klingt lächerlich, aber: Ich habe Angst, den Briefkasten zu öffnen. Beinahe täglich flattern mir derzeit Mahnungen und Drohschreiben von Inkassounternehmen ins Haus. […] Es war kurz vor Weihnachten, als mein bisheriges

Leben endete und sich das erste Inkassounternehmen bei mir meldete. […] Jetzt soll ich widersprechen?! Warum? Das ist doch überhaupt nicht mein Business! Ich habe dazu weder Zeit noch Lust." Der Name und das Geburtsdatum von Frau Groll reichten aus, damit die Betrüger in „möglicherweise Hunderten Fällen" daraus eine fiktive E-Mail-Adresse bastelten und die Daten verwendeten, um Waren bei Versandhäusern auf Rechnung zu bestellen. Die Zahlungen blieben selbstverständlich aus. „Irgendwann, Monate später, kommen die geprellten Unternehmen dahinter, dass die Adressen nicht korrekt sein können. Meist haben die Firmen die ausstehenden Forderungen dann an Inkassounternehmen abgetreten, die so etwas recherchieren. Sie werden fündig, und zwar bei der realen Person." Woher kamen die Daten? Frau Groll hatte in ihrer letzten Bewerbungsphase ihre Unterlagen inkl. Lebenslauf etc. auf ihrer Webseite veröffentlicht. Außerdem hatte sie ähnliche Daten auch in einem sozialen Netzwerk hinterlegt.

> *Jeden Abend begleitet mich das gleiche ungute Gefühl, wenn ich den Briefkasten leere. An einen längeren Urlaub ist derzeit nicht zu denken. Denn wenn die meist sehr kurzen Fristen in den Mahnungen verstreichen, kündigen die Inkassounternehmen Pfändungen durch Gerichtsvollzieher an. Versäume ich eine dieser Fristen, riskiere ich, dass mein Gehalt oder Konto gepfändet werden. Meine Freizeit verbringe ich fast ausschließlich mit Schadensbegrenzung. Jeden Abend schreibe ich Briefe an Auskunfteien und Unternehmen, an Inkassofirmen und immerzu das Update für die Ermittlungsbehörden. 400 Arbeitsstunden scheinen eine eher optimistische Rechnung zu sein.*

- Ein Mann bekam eine Vorladung der Polizei wegen sexueller Belästigung von Minderjährigen im Netz. Nach zwei Wochen stellte sich heraus, dass ein Pädophiler mit seiner Identität am Werk war. Der Mann dazu: „Das waren die zwei schlimmsten Wochen in meines Lebens. […] Ich bin ein richtiger Datenschützer geworden."
- Ein 67 Jahre alter Mann aus Wiesbaden geriet unter Verdacht, sich Kinderpornographie beschafft zu haben, weil von seinem Bankkonto entsprechende Abbuchungen vorgenommen wurden. Schließlich standen zwei Kriminalbeamte samt Durchsuchungsbefehl in seinem Büro und beschlagnahmten PCs und externe Speichermedien. Seine Privatwohnung, das Geschäft und sein Auto sollten durchsucht werden. Es stellte sich heraus, dass Unbekannte seine Kreditkartendaten missbraucht hatten.
- Ein Inder veröffentlichte eine Karikatur eines historischen Staatsgründers auf der Webseite Orkut. Die indische Polizei wandte sich an Google und erhielt eine IP-Adresse. Bekannt wurde der Fall, weil die IP-Adresse einem falschen Kunden des indischen Internet-Providers zugeordnet wurde und der Verdächtige drei Wochen lang zu Unrecht in Haft saß. Interessanter ist im Rahmen dieser Ausarbeitung aber, dass Google die IP-Adresse wegen einer Karikatur herausgerückt hat bzw. herausrücken musste.
- Im Rahmen einer Fahndung nach Schläfern (Terrorverdächtige) wurden 32.000 Personen nach einer Rasterung in eine bundesweite Datei aufgenommen. Dabei gab es nicht auch nur ansatzweise konkrete Anhaltspunkte, dass es sich bei den Personen um Schläfer handelte oder diese in Kontakt zu solchen standen.
- Die Staatsanwaltschaft ließ die Wohnung eines G8-Gegners durchsuchen. Im Durchsuchungsbefehl wird dem Betroffenen vorgeworfen, an einem Brandanschlag auf ein Berliner Unternehmen beteiligt gewesen zu sein. Das Indiz für diese Annahme war,

dass der Beschuldigte im Internet nach dem entsprechenden Unternehmen recherchiert hatte (Eingabe des Namens in eine Suchmaschine). Allerdings hatte er nach einem anderen Unternehmen mit dem gleichen Namen recherchiert und zwar aus ganz anderen Gründen.

- Ein Mitarbeiter von AOL verkaufte für 28.000 US-Dollar eine Liste mit sensiblen Kundendaten (Anschriften, Kreditkartendaten etc.) von 92 Millionen amerikanischen AOL-Nutzern an einen Spammer.
- Nachdem ein Stalker auf einer Webseite beschrieben hatte, wie er sein Opfer „vernichten" wolle, fand er den Aufenthaltsort heraus und erschoss sein Opfer.

4.4.1.5 Die Grundprinzipien des Datenschutzes

Seit den anfänglichen Debatten um den Datenschutz haben sich Grundprinzipien entwickelt, die noch den Datenschutzstandard von heute prägen. Folgende Grundsätze sind einer entsprechenden UNO-Resolution angelehnt (Garstka 2003: 52):

- **Grundsatz der Rechtmäßigkeit und der Beachtung von Treu und Glauben**: Formen der Datenverarbeitung, die gegen die Menschenwürde verstoßen oder die unter Täuschung erhoben wurden sind auszuschließen.
- **Grundsatz der Richtigkeit**: Datenverarbeiter sind nicht nur verpflichtet, richtige Daten zu verarbeiten, sondern die Richtigkeit auch regelmäßig zu überprüfen.
- **Grundsatz der Zweckbindung**: Daten dürfen grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden; zweckwidrige Nutzung sowie zu lange Speicherung sind auszuschließen.
- **Grundsatz des Auskunftsrechts der Betroffenen**: Jeder soll wissen, wer welche Daten über ihn verarbeitet.
- **Grundsatz der Nichtdiskriminierung**: Besonders sensible Daten, die zu einer Diskriminierung von Betroffenen führen können, dürfen nicht oder nur unter sehr beschränkten Voraussetzungen verarbeitet werden.

Darüber hinaus gibt es weitere Prinzipien, die sich speziell in deutschen und europäischen Datenschutzgesetzen wiederfinden. Diese lassen sich teilweise aus den oben genannten Grundsätzen ableiten oder wirken ergänzend (vgl. Witt 2010: 76ff):

- **Prinzip der Transparenz**: Eine verantwortliche Stelle muss einige Vorschriften zur Nachvollziehbarkeit für Betroffene einhalten, damit diese überhaupt ihr informationelles Selbstbestimmungsrecht nutzen können. Dazu gehören neben dem schon erwähnten Auskunftsrecht seitens der Betroffenen auch Benachrichtigungs- und Informationspflichten der Stellen: Ist eine Datenverarbeitung (z.B. die Erfassung oder Übermittlung personenbezogener Informationen) nicht ausdrücklich im Gesetz vorgesehen, so ist der Betroffene bei der erstmaligen Speicherung seiner personenbezogenen Daten über die Art der gespeicherten Daten, die Zweckbestimmung und die Identität der verantwortlichen Stelle zu benachrichtigen. Informationspflichten bestehen für besondere Verfahren gegenüber der zuständigen Aufsichtsbehörde, sofern gespeicherte personenbezogene Daten unrechtmäßig Dritten zur Kenntnis gelangten (Datenschutzpannen).

- **Prinzip der Erforderlichkeit**: Das Prinzip der Erforderlichkeit beruht auf dem Verhältnismäßigkeitsprinzip. Eine Maßnahme, hier die Erhebung von personenbezogenen Daten, ist erforderlich, wenn es kein milderes Mittel gibt, mit dem sich der gewünschte Zweck ebenfalls erreichen ließe.
- **Prinzip der Datenvermeidung und -sparsamkeit**: Bei diesem Prinzip handelt es sich um eine konkrete Anforderung an die Gestaltung der zur automatisierten Verarbeitung eingesetzten IT-Systeme. Ein IT-System entspricht dem Prinzip der Datensparsamkeit, wenn es mit möglichst wenig personenbezogenen Daten funktioniert. Ein Personenbezug sollte also nur dann vorgesehen sein, wenn dieses zur Aufgabenbewältigung unbedingt erforderlich ist. Pseudonymisierung und Anonymisierung sind gängige Mittel um den Anforderungen dieses Prinzips zu genügen.
- **Verbot mit Erlaubnisvorbehalt**: Das Verbot mit Erlaubnisvorbehalt lässt sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung ableiten. Die Erhebung, die Verarbeitung oder die Nutzung personenbezogener Daten ist verboten. Dieses Verbot kann nur außer Kraft gesetzt werden, wenn eine ausdrückliche Erlaubnis vorliegt. Dabei kann es sich um eine Einwilligung des Betroffenen oder eine gesetzliche Grundlage handeln.

Allgemeine Kritikpunkte bei Google sind, dass bei einigen Diensten die Einwilligung des Nutzers in die Erhebung persönlicher Daten zum Teil vollständig fehlt (z.B. bei Google Analytics) oder unzureichend realisiert ist. Hinzu kommt, dass bei vielen Diensten datenschutzrechtliche Grundprinzipien wie Zweckbindung, Erforderlichkeit, Datenvermeidung und -sparsamkeit sowie das Transparenzgebot nicht eingehalten werden. Es wird nämlich nicht ausführlich definiert, welche Daten genau für welche Zwecke erhoben werden. Daher ist auch schwer ersichtlich, ob erhobene Daten wirklich erforderlich sind. Personenbezogene Daten zu erheben, um einen Dienst erbringen zu können oder die Systemsicherheit zu gewährleisten sei viel zu allgemein gehalten. Das Dashboard ist mehr oder weniger die Verwirklichung des Auskunftsrechts und des damit verbundenen Rechts zur Löschung personenbezogener Daten. Allerdings ist die Realisierung unvollständig, da keine Kontrolle über alle erfassten Daten mit Personenbezug besteht. Eine ausführliche Analyse der Zwecke und Gründe für die Erhebung von personenbezogenen Daten ist unter der gleichen Quelle zu finden, wie das folgende Zitat:

> *Generell ist festzustellen, dass die Suchmaschinenbetreiber keinen umfassenden Überblick geben, für welche festgelegten, eindeutigen und rechtmäßigen Zwecke sie personenbezogene Daten verarbeiten. Erstens sind einige Zwecke wie „Verbesserung der Dienste" oder „personalisierte Werbung" zu allgemein definiert und bieten daher keinen angemessenen Beurteilungsrahmen für die Rechtmäßigkeit der Zwecke. Da zahlreiche Suchmaschinenbetreiber viele verschiedene Verarbeitungszwecke anführen, ist zweitens nicht klar, in welchem Umfang Daten für einen anderen Zweck weiterverarbeitet werden, der mit der ursprünglichen Zweckbestimmung nicht vereinbar ist.* (Artikel-29-Datenschutzgruppe 2008: 18)

4.4.2 Dienstübergreifende Verknüpfung von Daten

In der Einleitung wurde bereits angedeutet, dass sich die Datenerfassung, speziell bei Google, aufgrund der vielen unterschiedlichen Dienste auf einen sehr großen Bereich ausdehnt. Wie umfangreich diese Palette an Diensten und Produkten ist und welche Daten im Einzelnen erfasst

werden, wurde in Kapitel 4.2 deutlich. Am Anfang von Kapitel 4.4 war die Rede von ausführlichen Persönlichkeitsprofilen von Google-Nutzern, da sehr viele personenbezogene Informationen dienstübergreifend im Google-Konto zusammenlaufen oder aber auch auf Basis von IP-Adressen, Cookies oder einer Browser-ID zusammengeführt werden können. Solche Informationen werden in diversen Protokolldateien gespeichert. Protokolldateien sind neben den Informationen, die in einem eventuellen Konto zusammenlaufen, die wichtigsten personenbezogenen Daten, die allgemein von Suchmaschinenbetreibern verarbeitet werden (sofern diese nicht anonymisiert sind). Es gibt Protokolle über

- Anfragen: Inhalt der Suchanfragen, Zeitstempel, Benutzerspezifische Einstellungen und Daten, die sich auf den Computer des Nutzers beziehen.
- Daten über die angebotenen Inhalte: Auf angebotene Inhalte wie Links und Werbeanzeigen kann über die Anfrage geschlossen werden.
- Daten über die anschließende Benutzernavigation (Mausklicks).
- Operative Daten: Daten, die sich auf Benutzerdaten beziehen
- Daten über registrierte Benutzer.
- Daten von anderen Diensten.
- Daten anderen Ursprungs wie z.B. Werbeanzeigen auf Webseiten Dritter.

Die Daten werden mit der Quelle als Schlüssel aufgezeichnet, also z.B. mit der Cookie-ID. Eine dienstübergreifende Verknüpfung von personenbezogenen Daten heißt also mehr als nur ein Zusammenlaufen der entsprechenden Daten im Google-Konto. Es geht um die Korrelation unterschiedlicher Protokolldateien und -inhalte über die Quelle, also IP-Adresse, Cookie-ID oder ggf. auch Browser-ID. Auf diese Art und Weise funktioniert z.B. auch interessensbasierte Werbung, nämlich indem die angebotenen Inhalte aber auch die Benutzernavigation per Cookie-ID korreliert werden (vgl. Artikel-29-Datenschutzgruppe 2008: 6ff).

> *Die Suchhistorie einer Person gibt Aufschluss über die Interessen, Beziehungen und Absichten dieser Person. Diese Daten können nachfolgend sowohl für kommerzielle Zwecke als auch – aufgrund von Anfragen und Phishing-Operationen und/oder Data Mining – von Strafverfolgungsbehörden oder nationalen Sicherheitsdienten verwendet werden.* (Artikel-29-Datenschutzgruppe 2008: 8)

Darüber hinaus gibt es bei Google ja noch die Webhistorie (siehe Kapitel 4.1.1), die beim Anlegen eines Google-Kontos standardmäßig aktiviert ist. Dabei werden die Suchhistorie und weitere Informationen direkt im Google-Konto gespeichert. Somit wird die Suchhistorie unmittelbar mit dem Benutzerkonto verknüpft. Nach Auffassung der Arbeitsgruppe ist das dienst- und plattformübergreifende Korrelieren von personenbezogenen Daten für authentifizierte Benutzer nur mit Einwilligung und nach angemessener Unterrichtung der Benutzer rechtmäßig. Allgemein sollten sich Dienstanbieter klar zum Umfang der dienstübergreifenden Korrelation von Daten äußern und Korrelationen allgemein nur mit Einwilligung des Nutzers vornehmen (Artikel-29-Datenschutzgruppe: 2008: 24). Bei Google heißt es in den Datenschutzbestimmungen unter dem Punkt „Informationen, die Sie uns zur Verfügung stellen“ lediglich:

> *Wenn Sie ein Google-Konto erstellen, fragen wir Sie nach personenbezogenen Daten. Zum Zwecke einer besseren Servicequalität werden möglicherweise die über Ihr Konto bereitgestellten Informationen mit Informationen aus anderen Google-Services oder Services von Drittanbietern kombiniert. Bei*

> *bestimmten Services geben wir Ihnen zudem die Möglichkeit, die Zusammenführung solcher Informationen zu deaktivieren. Nutzen Sie das Google Dashboard, um mehr darüber zu erfahren, welche Informationen in Verbindung mit Ihrem Konto gespeichert sind.* (Google 2010p)

Wird die Quell-ID in Protokolldaten im Rahmen einer Anonymisierung irreversibel durch eine andere, offensichtlich nicht personenbeziehbare ID ersetzt, ist eine Identifizierung durch Korrelation der erhobenen Daten dennoch möglich. Bernhard C. Witt spricht in diesem Zusammenhang auch von einem Kontextproblem, denn „erst durch den Kontext werden Daten zu Informationen" (Witt 2010: 28ff). Man kann dann auch von einer Repersonalisierung durch Korrelation sprechen. Eine solche ist in Abbildung 27 visualisiert. Daher fordert die Artikel-29-Datenschutzgruppe, dass die verwendeten Methoden zur Anonymisierung sorgfältig geprüft und gründlich durchgeführt werden um eine indirekte Identifizierung von Nutzern auszuschließen, z.B. indem Teile der Suchhistorie beseitigt werden (Artikel-29-Datenschutzgruppe: 2008: 23).

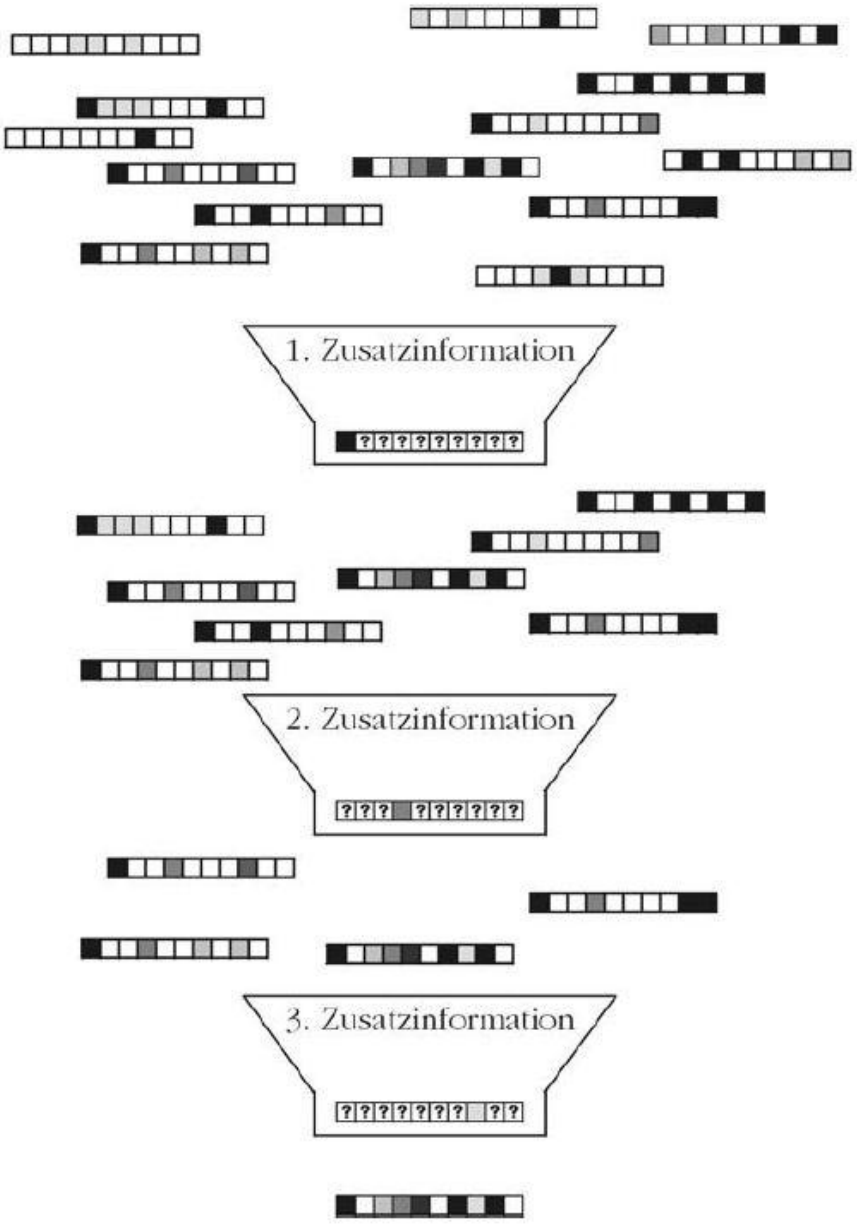


Abbildung 27: Repersonalisierung durch Korrelation (Witt 2010: 29)

Bei der Repersonalisierung durch Korrelation ergibt sich noch ein weiteres Problem: Gespeicherte Daten können einem Bedeutungswandel unterliegen. Das betrifft die in Abbildung 27 dargestellten „Zusatzinformationen“ in Form von Identitätsmerkmalen. Über ein Merkmal Adresse können z.B. Datensätze korreliert werden. Bei einem Umzug der betreffenden Person könnte dieses Merkmal zu fehlerhaften Korrelationen führen, wenn nun eine andere Person unter der Adresse ihren Wohnsitz hat. Identitätsmerkmale können also von Zeit zu Zeit oder von (datenerhebender) Stelle zu Stelle eine unterschiedliche Bedeutung haben. Dabei könnte man auch verschiedene Dienste als unterschiedliche Stellen betrachten (vgl. Witt 2010: 28). Das Problem verschärft sich, wenn wichtige Informationen fehlen bzw. ausgelassen werden und daraus falsche Persönlichkeitsbilder entstehen (siehe Abbildung 28).

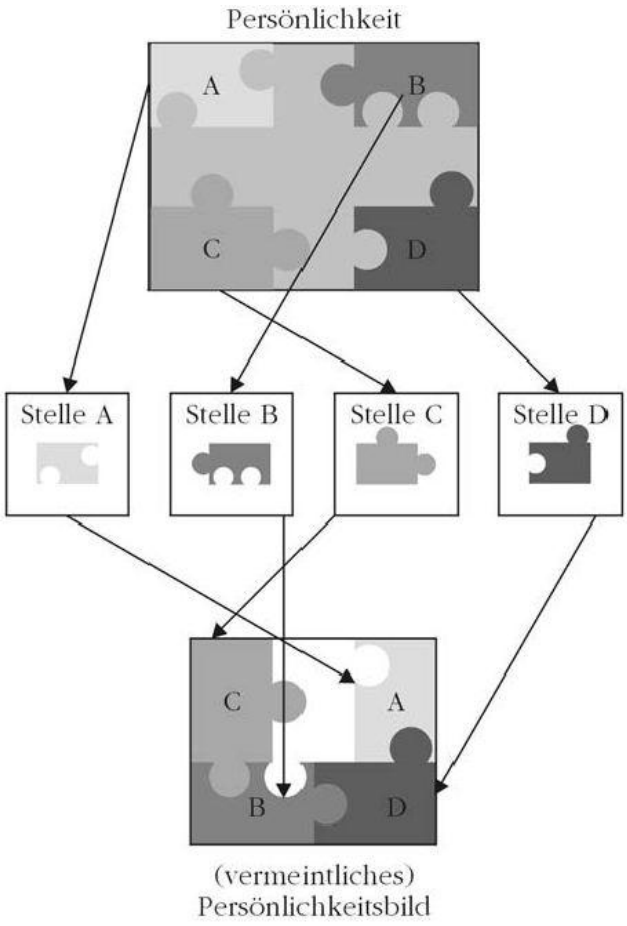


Abbildung 28: Fehlerhaftes Persönlichkeitsbild durch das Fehlen von Informationen (Witt 2010: 51)

4.5 Das Opt-out-Problem und Risikoverminderung

Wie bereits in der Einleitung erwähnt, berücksichtigt Google laut seinen Datenschutzprinzipien den Umstand, dass jeder Nutzer eine eigene Einstellung zum Datenschutz hat und bietet ihm daher detaillierte Wahlmöglichkeiten bzgl. der persönlichen Daten, die an Google übermittelt und dort gespeichert werden. Dass dem wirklich so ist, konnte bei der Betrachtung der Maßnahmen zur Risikoverminderung bei den einzelnen Diensten festgestellt werden. Da Google auf Daten angewiesen ist, werden die Optionen zum besseren Datenschutz auch weiterhin standardmäßig deaktiviert sein. Opt-in wäre für Google nämlich fatal, denn welcher Nutzer würde die Einstellungen freiwillig so anpassen, dass der entsprechende Dienst mehr persönliche Daten an

Google sendet? Die Antwort lautet wohl: Niemand. An dieser Stelle sollten sich vielleicht mal die Nutzer, die pauschal argumentieren, dass sie ja nichts zu verbergen hätten, hinterfragen, ob sie entsprechende Einstellungen auch von sich aus aktivieren würden, und wenn nein, warum nicht. Solche Nutzer sind natürlich willkommene Datenlieferanten für Google. Das funktioniert wohlbemerkt aber nur bei Opt-out.

Daher müssen sich die Nutzer von Google's Diensten bewusst sein, erstens, dass Datenschutz wichtig ist, zweitens dass bei Google diesbezüglich Wahlmöglichkeiten bestehen, um eigene Daten besser zu schützen und dennoch entsprechende Dienste nutzen zu können und drittens, dass jeder diese Wahlmöglichkeiten auch nutzen sollte. Nutzer müssen ein Gefühl dafür entwickeln, viel kritischer an neue Dienste heranzugehen und wissen, wo man entsprechende Opt-out-Anpassungen vornehmen kann oder wo weitere Informationen diesbezüglich zu finden sind. So gibt es in fast allen Diensten in den Einstellungen eine Kategorie „Datenschutz". Bei den Datenschutzbestimmungen zum Dienst ist zudem oft auch ein Abschnitt „Ihre Wahl" zu finden, in dem die Wahlmöglichkeiten aufgelistet sind.

Neben den Wahlmöglichkeiten gibt es natürlich noch weitere, allgemeine Maßnahmen, um Risiken zu minimieren. Das Google-Konto authentifiziert den Benutzer. Daten können einem Nutzer nur eindeutig zugeschrieben werden, wenn dieser mit dem Google-Konto angemeldet ist. Standardmäßig ist man selbstverständlich immer eingeloggt, wenn man sich einmal registriert bzw. angemeldet hat. Dabei spielt es keine Rolle, ob der Zugangspunkt zum Internet nun ein Webbrowser oder das Android-Handy ist. Im Web ist bei der Registrierung und Anmeldung die Option „Eingeloggt bleiben" vorselektiert. Egal welchen Dienst man nun nutzt, Informationen, die Google erfasst, könnten immer mit dem Google-Konto verknüpft werden. Ähnlich sieht es bei Android aus. War die Anmeldung an das Google-Konto früher noch eine Voraussetzung für die Nutzung von Android, hat man nun beim ersten Start die Möglichkeit diesen Vorgang zu überspringen. Dementsprechend sollte man nur dann mit dem Konto angemeldet sein, wenn dies zwingend erforderlich ist und sich lieber mal öfter ab- und wieder anmelden. Eine weitere Maßnahme wäre es z.B. auch, sich einen zusätzlichen Browser zu installieren, bei dem alle gespeicherten Daten (allem voran Cookies) nach dem Beenden gelöscht werden. Dieser könnte dann für Google's Dienste verwendet werden, getreu dem Motto: Sicher ist sicher. Selbiges wurde auch für die Tests, die im Rahmen dieser Ausarbeitung durchgeführt wurden, gemacht.

Eine weitere gute Maßnahme zur Risikoverminderung ist es, das Google-Konto mit so wenig persönlichen Informationen anzureichern wie nur irgendwie möglich. Warum den echten Namen beim Anlegen eines Kontos angeben? Warum z.B. bei Google Checkout auch noch seine überprüfte Adresse und seine Konto- bzw. Kreditkartendaten mitteilen? Warum z.B. bei Google Maps seinen eigenen Standort festlegen? Warum ein (öffentliches) Profil verwenden und dieses mit persönlichen Informationen anreichern? Warum eigene Kontaktdaten bei der Nutzung von Gmail angeben? Warum soziale Kontakte mit dem Google-Konto verknüpfen, wenn es doch andere, mindestens gleichwertige, soziale Netzwerke gibt? Warum Google Talk verwenden, wenn es genügend bessere Instant Messanger gibt? Das führt unmittelbar dazu, doch allgemein alternative Dienste zu verwenden, wenn diese (nahezu) gleichwertig sind.

Es gibt aber auch viele weitere, allgemeinere Schutzmaßnahmen, wie z.B. dass man sein WLAN schützt, damit Google (oder andere) nicht „ausversehen" Daten mitschneiden oder dass man sich nur an vertrauenswürdigen Stellen mit seinem Google-Konto anmeldet und nicht in irgendeinem

Internet-Café. Dann könnten nämlich womöglich die Anmeldeinformationen mitgelesen werden und fortan hätten unautorisierte Personen Zugriff auf das Google-Konto und die damit verknüpften Informationen.

4.5.1 Browser-Add-ons

Um zu verhindern, dass Google und andere während des Browsens im Internet verschiedene persönliche Daten sammelen, wurden diverse Add-ons bzw. Plug-ins für Browser entwickelt. Speziell in den Communitys von Open-Source-Browsern, allem voran Mozilla Firefox, sind mehrere Tools bzw. Add-ons entstanden, die explizit der Sammelwut von Google aber auch der allgemeinen Erhebung von Daten entgegenwirken. Im Folgenden sollen einige davon vorgestellt werden. Aber auch von Google gibt es offizielle Add-ons, wie das in Kapitel 4.2.3.1 erwähnte „Google Analytics Opt-out Browser Add-on". Eine Übersicht über viele Datenschutz-Add-ons für den Firefox sind hier zu finden: https://addons.mozilla.org/de/firefox/extensions/privacy-security/

- **Kill-ID** (Google Chrome) – das Tool kann folgende Optionen deaktivieren bzw. Datenübermittlungen unterbinden (Kolokythas 2008):
  - Browseridentifikation
  - Vorschläge zur Auto-Vervollständigung
  - Vorschläge für Navigationsfehler
  - Nutzungsstatistiken und Absturzberichte
  - Google Update
- **GoogleSharing** (Firefox) – hierbei handelt es sich um ein interessantes Projekt, welches das Motto „Teilen für mehr Privatsphäre" vertritt. Die Webseite zum Projekt lautet: http://www.googlesharing.net/.

  Bei dem Vorhaben, hinter dem unter anderem der bekannte IT-Sicherheitsforscher Moxie Marlinspike steckt, wird versucht, Google-Dienste nutzbar zu machen, ohne dass der Nutzer dafür seine (IP-)Identität preisgeben muss, berichtet Technology Review in seiner Online-Ausgabe.

  Die Grundidee: Wenn sich Gruppen von Nutzern zusammentun, wird es möglich, deren Google-Nutzung zu verwürfeln. Dazu hat GoogleSharing ein kostenloses Zusatzprogramm für den Browser Firefox entwickelt, das jede Anfrage an Google.com umleitet. Dem Anfragenden A wird die Eingabe des Anfragenden B zugeordnet, dem Anfragenden B die von C – und so weiter. Außerdem wird dafür gesorgt, dass Google den Anfragenden nicht über ein Cookie identifizieren kann – es wird stets ein neuer Datenkrümel angefordert. (Schwan 2010b).

- **Plug-in zum Deaktivieren des Cookies für Anzeigenvorgaben** (diverse Browser) – Offizielles Plug-in für Google zum dauerhaften Deaktivieren des DoubleClick-Cookies. Zu finden ist das Plug-in hier: http://www.google.com/ads/preferences/html/intl/de/plugin/.
- **TrackMeNot** (Firefox) – Das Add-on sorgt dafür, dass ein Hintergrundprozess periodisch willkürlich gewürfelte Suchanfragen an bekannte Suchmaschinen wie z.B. AOL, Yahoo, Google und Bing sendet. Somit gehen eigene Eingaben in den

Suchmaschinen in dem Wirrwarr der automatisch gesendeten Suchanfragen unter (http://cs.nyu.edu/trackmenot/).

- **BetterPrivacy** (Firefox) – Schützt den Nutzer vor sogenannten Langzeit-Cookies, die nicht wie normale Cookies entfernt werden können. Dazu zählen vor allem Flash- und „DOM Storage"-Cookies (http://netticat.ath.cx/BetterPrivacy/BetterPrivacy.htm).
- **Ghostery** (Firefox) – Informiert den Nutzer wenn Webtracker wie Google Analytics im Hintergrund z.B. per Web Bugs Informationen aufzeichnen. Außerdem bietet das Add-on Informationen zum Webtracker sowie dem dazugehörigen Unternehmen und bietet verschiedene Möglichkeiten, solche Datenerfassungen zu steuern.

  Ghostery sees the invisible web - tags, web bugs, pixels and beacons. Ghostery tracks the trackers and gives you a roll-call of the ad networks, behavioral data providers, web publishers, and other companies interested in your activity (http://www.ghostery.com/).

- **Adblock Plus** (Firefox) – In erster Linie handelt es sich bei dem Add-on um einen dynamischen Blockierer von Werbeinhalten. Per Filterlisten, die beliebig ergänzt werden können, werden bestimmte Inhalte wie z.B. Flash und Java blockiert. Somit bietet es auch Features, um der Datensammelei entgegenzuwirken. Detaillierter soll das Add-on in diesem Rahmen allerdings nicht betrachtet werden. Über 100 Millionen Downloads der mehrsprachigen Firefox-Erweiterung und hervorragende Bewertungen der Community sprechen jedoch für sich (http://adblockplus.org/de/).
- **CustomizeGoogle** (Firefox) – Das Add-on bietet mehrere Optionen, um Google-Dienste anzupassen bzw. zu verbessern, auch was die Datensicherheit angeht, dazu gehören die folgenden (http://www.customizegoogle.com/):
  - Automatisches Umschalten auf eine verschlüsselte TLS-Verbindung, sobald Gmail oder Google Kalender verwendet wird
  - Blockierung des Google-Analytic-Cookies
  - Anonymisierung von User-IDs, die von Google zugewiesenen wurden
  - Deaktivierung des Trackings von Mausklicks im Browser
  - u.v.m.

5 Widerstand, Abhängigkeiten und Konkurrenz

In diesem Kapitel soll ermittelt werden, was die in Kapitel 3 dargestellte, wirtschaftliche Macht von Google schmälern oder gar zerstören könnte. Zu den Beteiligten gehören diesbezüglich im großen Ganzen drei Gruppen: Erstens verschiedene Interessensgruppen bzw. Institutionen, die sich Google's Strategien und Methoden aus unterschiedlichen Gründen widersetzen, zweitens die Nutzer und Kunden, von denen Google absolut abhängig ist und drittens natürlich die Konkurrenten, die auf den gleichen Märkten wie Google agieren. Alle drei beteiligten Gruppen sollen nun der Reihe nach etwas näher betrachtet werden.

5.1 Politische Institutionen

Bei den politischen Institutionen, die die Interessen eines Gemeinwesens vertreten, spielen vor allem die Datenschutz-, die Verbraucherschutz- und die Wettbewerbsbehörden eine wesentliche Rolle, was den öffentlichen Widerstand gegen Google's Unternehmenspolitik anbelangt. Der Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Der Datenschutz will den so genannten gläsernen Menschen verhindern (vgl. Wikipedia 2010a). Als Folge der Datensammelei von Google sehen sich der Bundesdatenschutzbeauftragte Peter Schaar, aber auch die Landesdatenschutzbeauftragten, ständig mit Google konfrontiert. Viele Dienste von Google werden kritisch untersucht und datenschutzrechtlich diskutiert, da sie bzgl. der Datenerhebung nicht mit den Prinzipien der Transparenz, der Erforderlichkeit, der Datenvermeidung und -sparsamkeit, des Verbots mit Erlaubnisvorbehalt sowie mit dem Grundsatz der Zweckbindung in Einklang zu bringen sind (siehe Kapitel 4.4.1.5).

Auch der Verbraucherschutz, der für allgemeine Maßnahmen zum Schutz für Verbraucher von Dienstleistungen einsteht, spielt hier eine Rolle. So ist auch Ilse Aigner, momentane Verbraucherschutzministerin der Bundesrepublik Deutschland, auf diesem Gebiet tätig und setzt sich stellvertretend für das deutsche Volk gegen Google und andere Internet-Dienstleister wie z.B. Facebook zur Wehr. Dann geht es meist um den Schutz der personenbezogenen Daten von Verbrauchern, daher leistete sie z.B. gegen Google Analaytics und nun gegen Street View Widerstand. Bei Google's Dominanz in der Internetökonomie verwundert es wenig, dass sich auch immer öfter die Wettbewerbsbehörden einschalten, um auf Google's Märkten regulierend einzuwirken (vgl. Kaumanns/Siegenheim 2009: 395ff). Dazu gehören z.B. die Federal Trade Commission in den USA, das Bundeskartellamt in Deutschland und die Generaldirektion Wettbewerb der Europäischen Kommission. So startete die EU-Kommission z.B. Ende November 2010 ein Kartellverfahren, weil sich mehrere Konkurrenten darüber beschwert hatten, dass sie in den Ergebnissen der Google-Suche weit nach unten verbannt wurden. Außerdem gingen die Wettbewerbshüter Vorwürfen nach, wonach Google bei Werbeverträgen Bedingungen auferlegt haben soll, dass Werbepartner keine konkurrierende Werbung auf ihren Seiten schalten dürfen (http://www.tagesschau.de/wirtschaft/google350.html).

An einigen Stellen wird staatlichen Behörden allgemein auch vorgeworfen, sie setzten sich nicht genug für den Datenschutz ein, da sie selbst an den von Google erfassten Daten interessiert seien, um über mehr Beweismittel für eventuelle Kriminalfälle zu verfügen. Übrigens sind

politische Institutionen nicht die einzigen Kritiker. Auch freie Medien bzw. Autoren betrachten Google's Dienste und allgemein die Unternehmenspolitik sehr kritisch. Neben zahlreichen Artikeln in Zeitschriften und Zeitungen gibt es z.B. auch ein Buch von Gerald Reischl, das sich sehr kritisch mit Google und seiner „Sammelwut" auseinandersetzt: „Die Google-Falle. Die unkontrollierte Weltmacht im Internet". Im Gegensatz zu den politischen Institutionen geht es hier allerdings mehr um Aufklärung und Berichterstattung als um aktiven Widerstand im Rahmen der Gesetze.

5.2 Die Abhängigkeit von Nutzern und Werbetreibenden

Unmittelbar verbunden mit dem Widerstand der politischen Institutionen und Co ist auch das wohl kritischste Gut von Google, nämlich das Vertrauen seiner Nutzer. Dieses Vertrauen in Google und seine Dienste könnte durch die öffentliche, medienwirksame Kritik von Datenschützern, Politikern und Journalisten verloren gehen. Ein gutes Beispiel ist die aktuelle Debatte um Google Street View. Durch die vielen kritischen Berichte in den Medien werden die Nutzer mit Google's Umgang bzgl. personenbezogener Daten unmittelbar konfrontiert und es kommt allgemeine Skepsis auf. Ein immenser Vertrauensverlust wäre aber auch die unmittelbare Folge weiterer Fälle von Datenschutzpannen oder wohlgemerkt erster Fälle von Datenmissbrauch. Die Folge eines Vertrauensverlustes seitens der Nutzer könnte das Ende der Erhebung von Unmengen an Daten, speziell personenbezogener Informationen, bedeuten. Wie abhängig Google von diesen Daten ist, wurde in Kapitel 2 geschildert.

Genau wie für die Nutzer, würde sich ein möglicher Imageschaden auch auf das Vertrauen der Geschäftskunden, also der Werbetreibenden, auswirken. Aber auch der Wettbewerb spielt bei den Werbetreibenden eine entscheidende Rolle: Natürlich kann ein Monopol bei der Online-Werbung nicht im Interesse des eigentlichen, zahlenden Kunden sein, da Google in dieser Position die Preise diktieren kann. Deshalb suchen immer mehr Werbetreibende Alternativen zu Google (Kaumanns/Siegenheim 2009: 341).

5.3 Konkurrenz

Laut Ralf Kaumanns und Veit Siegenheim wird die heutige Welt des Internets von Google, Microsoft, Yahoo, AOL, eBay und Amazon weitestgehend dominiert. Facebook wird dort, neben anderen, zu einem Unternehmen gezählt, dass dabei ist, sich in diese Reihe einzugliedern. Alle genannten Konkurrenten stünden sich mehr oder weniger in dem einen oder anderen Segment in einem Wettbewerb gegenüber. Google jedoch würde sich irgendwie mit allen Wettbewerbern anlegen und dabei kein Segment verschonen (Kaumanns/Siegenheim 2009: 337). Im Weiteren sollen die Wechselwirkungen zwischen Google und Microsoft, Yahoo, Facebook sowie Amazon etwas näher betrachtet werden. Das dazugehörige Buch der beiden Autoren wurde bereits im Jahr 2009 veröffentlicht und inzwischen kann man wohl ohne Zweifel behaupten, Facebook habe die Eingliederung in diese Reihe vollzogen. AOL wurde von den beiden Autoren vor allem wegen der Fusion mit Time Warner, einem gigantischem internationalen Medienunternehmen mit zahlreichen Geschäftsfeldern, erwähnt. Im Dezember 2009 trennte sich Time Warner wieder von AOL. Daher fällt AOL aus dieser Reihe raus. eBay wurde eher wegen der Konkurrenz von PayPal zu dem Zahlungsdienst Google Checkout und eBay's Marktplatz als Konkurrent zu

Google Base erwähnt. Google Base ist die Datenbank hinter der Google Produktsuche, in der auch Warenangebote aller Art inseriert werden können. Da es sich hier um nur zwei konkurrierende Dienste handelt, soll auch eBay nicht näher betrachtet werden. Neben diesen Größen der Internetökonomie konkurriert Google natürlich auf den einzelnen Märkten mit vielen weiteren Unternehmen, wie z.B. Medien-, Telekommunikations- und Mobilfunkunternehmen. Konkurrenz ist also durchaus vorhanden und anders als es früher den Anschein hatte, wird Google mittlerweile von dieser Konkurrenz ernstgenommen:

> *Google trifft zudem in vielen der neuen Segmente nicht auf Firmen, die Google und dessen Fähigkeiten unterschätzen. Beispielsweise gehen die meisten der Akteure im Telekommunikations- und Mobilfunkmarkt nicht so naiv mit Google um, wie es viele Internet- und Medienunternehmen vor ein paar Jahren taten. Die Zeiten als Google noch unterschätzt wurde und man im Mountain View daraus einen strategischen Vorteil ziehen konnte, sind endgültig vorbei.* (Kaumanns/Siegenheim 2009: 397)

5.3.1 Yahoo und Microsoft

Yahoo verfolgte, im Gegensatz zu Google, immer das Portalkonzept: Alles was für den Nutzer interessant oder nützlich sein könnte, wurde zentral in einem Portal angeboten. Dementsprechend konkurriert Yahoo bei ziemlich vielen Diensten mit Google, aber auch bei der Werbevermarktung. Allerdings wurden bei Yahoo keine echten Schwerpunkte gesetzt und so wurde sehr wenig wirklich vernünftig gemacht und Yahoo blieb relativ erfolglos. „Die meisten Angebote sind Me-Tools. Man surft nicht zu Yahoo, um sie dort zu nutzen, man nutzt sie bei Yahoo, weil man sie dort eben auch findet“ (Kaumanns/Siegenheim 2009: 355). In Bezug auf die Reichweite hingegen ist Yahoo immer noch ein Riese, was an den großen Nutzerzahlen (siehe Kapitel 3) deutlich zu erkennen ist. Was fehlt ist eine klare Positionierung und eine bessere Umwandlung der vielen Nutzer in bares Geld, denn „die erfolgreiche Werbevermarktung ist seit Jahren die größte Dauerbaustelle im Konzern“ (Kaumanns/Siegenheim 2009: 357).

Bei Microsoft hatte man den Eindruck, dass sie oft nur reagieren statt auch mal zu agieren. So wurden neue Trends im Internet regelmäßig unterschätzt und wenn sich solche neuen Trends entwickelten, speziell bei Google, war es oft schon zu spät. Dieser Rückstand und die gemachten Fehler werden versucht, durch viel Geld wieder wett zu machen. Das ist auch daran zu erkennen, dass Microsoft momentan massiv seine Rechenzentren ausbaut. Microsoft konkurriert auf vielen Märkten mit Google: Cloud Computing, Suche, Werbung, Geoinformationen, Digitalisierung von Büchern, Gesundheitsdienste, Bürosoftware, Mailing und Instant Messaging sowie weiteren Online-Diensten. Allerdings beträgt der Anteil des Internetgeschäfts keine entscheidende Rolle bei der Erwirtschaftung von Gewinnen bei Microsoft. Das Kerngeschäft sind Betriebssysteme, Server, Büroanwendungen und Unternehmenssoftware. Allerdings drängt Google mit Android, Chrome, Chrome OS, Text & Tabellen etc. massiv in diese Märkte vor. Es bleibt abzuwarten, wie sich der Wettbewerb im Weiteren entwickelt. Jedenfalls bleibt dieser Konkurrenzkampf spannend und ist vollkommen offen, denn Microsoft hat aus begangenen Fehlern gelernt und verfügt über eine enorme Finanzkraft.

Im Jahr 2008 bestätigten sich Gerüchte, dass Microsoft an einer Übernahme von Yahoo interessiert sei. 47,5 Milliarden Dollar wurden geboten. Das Angebot stieß bei Yahoo allerdings

auf Ablehnung, denn man wollte unabhängig bleiben. Die größte Chance der angestrebten Fusion wäre die Kopplung von Online- und Offline-Anwendungen gewesen, denn man hätte die vielen Yahoo-Dienste unmittelbar in Windows integrieren können. Mittlerweile wurden zumindest strategische Partnerschaften zwischen Microsoft und Yahoo geschlossen, z.B. bei der Suche und der Werbevermarktung. Auch Google wollte wenig später eine Allianz mit Yahoo bei der Vermarktung von Werbung eingehen, einschließlich 800 Millionen Dollar jährliche Garantiezahlungen an Yahoo. Aufgrund angekündigter Kartellverfahren wurden die Gespräche allerdings eingestellt (vgl. Kaumanns/Siegenheim 354ff).

> *Eine derartige Verschmelzung von Online- und Offline-Anwendungen (gemeint ist eine Fusion von Microsoft und Yahoo) wäre sicherlich der größte Albtraum von Google – dem hätte man in Mountain View so ohne weiteres nichts Wirksames entgegenzuwirken* (Kaumanns/Siegenheim 2009: 360)

5.3.2 Facebook

Facebook ist das größte und bekannteste soziale Netzwerk der Welt und ist dabei, seinen Einfluss auf das Internet auszudehnen. Allein zwischen Februar und Juli 2010 stieg die Nutzerzahl von 400 auf 500 Millionen Nutzer. Im August 2008 waren es noch 100 Millionen (Wikipedia 2010b). Dieser Erfolg ist atemberaubend. Um das noch einmal zu verdeutlichen, zeigen die Abbildungen 29 und 30 den aktuellen Trend bezüglich der Anzahl an Google- und Facebook-Besuchern im direkten Vergleich. Laut Facebook-Chef Mark Zuckerberg hätten die meisten vorherigen Webanwendungen noch nicht die wahren Identitäten der Nutzer verwendet. Diesbezüglich sei das Internet momentan an einem wichtigen Wendepunkt. Sobald ein Nutzer sich bei Facebook einloggt, sollen sich neue Webseiten, die er besucht, entsprechend seinem Facebook-Profil verändern. Somit sollen alle möglichen Websites personalisiert werden, einschließlich der dort platzierten Werbung. Auf einer Nachrichtenseite würden so beispielsweise Nachrichten, die seinen Interessen oder denen seiner Kontakte entsprechen, angezeigt. Andere Webseiten sollen die Facebook-Profile dafür einsehen und verwenden können. Wenn die Nutzer die Neuerungen annehmen, könne Facebook wichtige Informationen über sie gewinnen und diese wären bei der Werbevermarktung sehr nützlich. Das wäre fatal für Google, denn Nutzer könnten nun über Facebook zu personalisierten Webseiten weitergeleitet werden und nicht mehr über die Google-Suche. Der Einstiegspunkt zum Surfen auf verschiedenen Webseiten könnte so für viele Nutzer fortan Facebook und nicht mehr die klassische Suchmaschine sein (vgl. BBV 2010a).

> *Wenn ich Google wäre, dann würde ich Angst bekommen, weil Facebook mit mehr Informationen (über die Internetnutzer) dastehen könnte, als sie.* (Alain Chuard, Produktmanager der Wildfire Marketing Group nach BBV 2010a)

Auch wenn Facebook eigentlich „nur“ als soziales Netzwerk und in der Werbevermarktung mit Google konkurriert, so handelt es sich um zwei grundsätzlich unterschiedliche Philosophien, was die Personalisierung angeht. So personalisiert Google zum Großteil auf Basis von Algorithmen und enormer Datenmengen, bezogen auf unterschiedliche Nutzer. Facebook hingegen verfolgt vielmehr die Vision der Personalisierung auf Basis sozialer Beziehungen zwischen Nutzern. Nutzer zeigen in sozialen Netzwerken nämlich ein anderes Verhalten bzgl. ihrer Anonymität. Im Gegensatz zum sonstigen Internet geben sie hier gerne Informationen über sich preis: Tatsächlicher Name und Kontakte, Gedanken, Gefühle, Gewohnheiten, Neuigkeiten usw. Diese

Informationen stehen Google in dieser Summe nicht zur Verfügung und es kann sich diese Informationen auch nicht aus anderen Daten ableiten. Im Jahr 2010 kaufte Microsoft einen 1,6-prozentigen Anteil an Facebook für rund 240 Millionen Dollar. Im Gegenzug dazu wurde Microsoft's Suchtechnologie eingebunden und Microsoft erhielt das Vermarktungsrecht für einen Teil der amerikanischen Webseite von Facebook. Auch Google bot mit, wurde aber augenscheinlich nur benutzt, um den Preis in die Höhe zu treiben, denn laut Aussage von Facebook war Microsoft von Anfang an der bevorzugte Partner. Ein Rückschlag für Google, denn Facebook zieht immer mehr Aufmerksamkeit auf sich und somit auch viele personenbezogene Daten und zwar vorbei an Google. Des Weiteren hat Facebook Konzepte wie Facebook Apps mit (laut Facebook selbst) weit über 50.000 Zusatz-Anwendungen und Facebook Connect, einer Schnittstelle um die bei Facebook gespeicherten Profildaten anderen Webseiten zur Verfügung zu stellen. Momentan entwickelt sich Facebook vom sozialen Netzwerk zu einer ganzen Plattform verschiedener Dienste und Möglichkeiten, alles auf Basis dieses sozialen Netzwerks. Vermutlich werden die Werbemodelle von Facebook eine große Konkurrenz zu Google's Werbemodellen, z.B. beim lokalen Anzeigemarkt. Die Resultate der versuchten Gegenwehr zu Facebook (und anderen) mit Google-Diensten wie Buzz, Orkut und Wave brachten nicht den gewünschten Erfolg. Somit ist und bleibt Facebook ein ernsthafter Wettbewerber für Google, vor allem, wenn sich aus den vielen Nutzern in Zukunft, speziell durch Werbung, Kapital schlagen lässt (vgl. Kaumanns/Siegenheim 2009: 376ff).

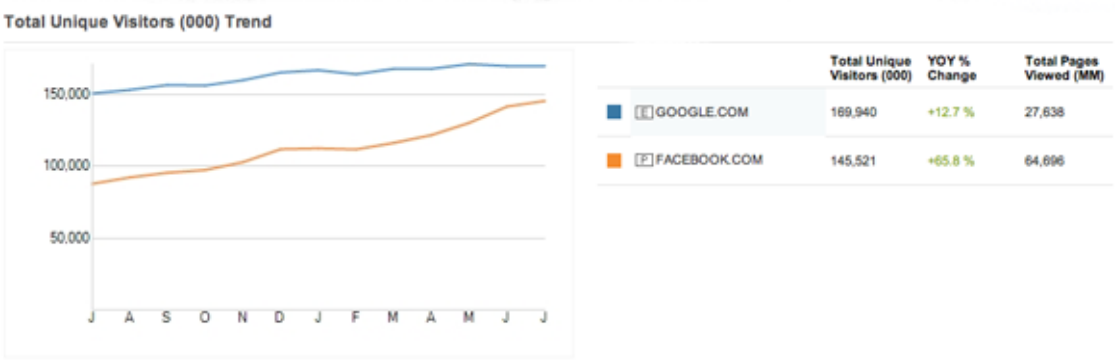


Abbildung 29: Wöchentliche Besucher auf google.com und facebook.com von Juli 2009 bis Juli 2010 (Tsotsis 2010)

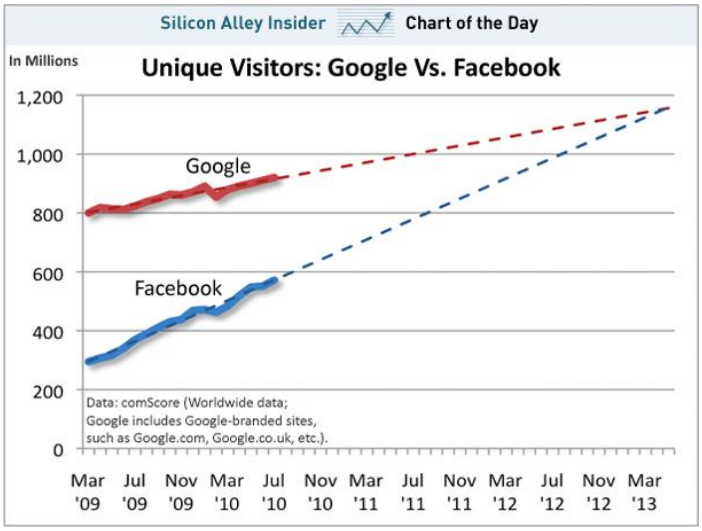


Abbildung 30: Monatliche Google- und Facebook-Besucher von März 2009 bis März 2013 (Angelova/Yarow 2010)

5.3.3 Amazon

Amazon ist sowohl beim Cloud Computing (siehe Kapitel 4.2.4) als auch bei der Distribution digitaler Güter ein ernstzunehmender Konkurrent für Google. Beim Cloud Computing ist Amazon nach Kaumanns und Siegenheim der momentane und vorerst auch zukünftige Marktführer. Dieser Markt sei ein (theoretisch) gigantischer Wachstumsmarkt. Laut Amazon nutzen über eine halbe Million Entwickler die Cloud Computing Angebote von Amazon (Stand 2009). Die Preise beider Unternehmen sind recht ähnlich und stehen unter einem starken Wettbewerbsdruck. Das Einsteigerangebot bei Google ist kostenlos, stößt jedoch auf erhebliche Skepsis in der Entwicklergemeinde, da die Anwendungen sehr eng mit proprietären Technologien von Google einhergehen. Man befürchtet eine Abhängigkeit von Google, sodass ein Wechsel zu einem anderen Anbieter kompliziert und teuer werden könnte. Die Angebote von Amazon hingegen seien offener und flexibler vor allem bzgl. Programmiersprachen, Technologien, Datenbanken etc. Google setze hier sehr enge Grenzen und Vorgaben. Dafür muss man die Software bei Amazon z.B. selber hosten. Bei IT-Infrastrukturen und Plattformen im Sinne von IaaS und PaaS verzeichnet Amazon also deutliche Vorteile. Bei vollständigen Applikationen in der Cloud (SaaS) hingegen hat wohl Google die Nase vorn, genau wie auch bei den Cloud Clients mit Chrome, Chrome OS, Gears und dem Native Client. Nähere Informationen zu diesen Produkten bzw. Technologien sind in Kapitel.4.2.4 zu finden.

Bei der Distribution digitaler Güter, wie z.B. E-Books, kommt Amazon seine Marktposition bei der Distribution physischer Güter zu Gute. Daher ist Amazon beim Vertrieb von E-Books in den USA sehr erfolgreich. Außerdem liegt die Distribution digitaler Güter bei Amazon, im Gegensatz zu Google, direkt am Kerngeschäft. Als Konkurrent in Sachen Zahlungsanbieter stieg Amazon 2009 mit „Simple Pay“ für Privatkunden und „Checkout by Amazon“ für professionelle Online-Händler in den Wettbewerb ein. Dies soll Teil einer übergeordneten Strategie sein, in der Amazon seine Webtechnologien und Dienstleistungen anderen Unternehmen zur Verfügung stellen will. Gerade in Bezug auf das Cloud Computing ist dies ein wichtiges Element. Hinzu kommt, dass Amazon den größten Onlineshop der Welt hat und dadurch sehr viele Kundendaten, die im direkten Zusammenhang mit gekauften oder angeschauten aber nicht gekauften Produkten stehen (vgl. Kaumanns/Siegenheim 2009: 347ff).

5.3.4 Der Konkurrenzkampf mit dem Datenschutz

Wie bereits zuvor erwähnt, speichert Google die IP-Adressen zu erfassten Daten 9 Monate und die Cookie-IDs 18 Monate, bevor sie anonymisiert bzw. gelöscht werden. Neun Monate seien laut Google das maximal machbare Entgegenkommen, um immer noch gute Suchergebnisse sowie eine gute Stabilität und Sicherheit des Netzwerks zu gewährleisten. Was solche Fristen anbelangt hat sich ein ganz neuer Konkurrenzkampf im Internet eröffnet: Microsoft legte vor und bot am 8. Dezember 2008 an, die Speicherfrist für die Nutzdaten auf die von der EU geforderten sechs Monate zu reduzieren, falls die anderen dasselbe tun. Yahoo gab am 17. Dezember des gleichen Jahres sogar bekannt, die Frist, abgesehen von begrenzten Ausnahmen, auf drei Monate zu reduzieren. Bei der medienwirksamen Austragung des Kampfes steht Google schließlich als der Böse da, der auf seine neun Monate beharrt, weil Google wie kein anderer auf diese Daten angewiesen ist. In diesem Konkurrenzkampf geht es scheinbar um Datenschutz vs. Qualität und letztlich entscheidet der Nutzer, was ihm wichtiger ist (vgl. Brandt 2010: 127ff).

6 Fazit & Ausblick

Zusammenfassend kann man sagen, dass Google's Dienste dem Nutzer enorme Möglichkeiten (Chancen) bieten, aber auch eine große Gefahr (Risiken) bergen, nämlich die Aufgabe der Privatsphäre und des Grundrechts auf informationelle Selbstbestimmung. Letzteres soll den Einzelnen vor unerwünschten Folgen, insbesondere durch zweckwidrigen Missbrauch, beim Umgang mit seinen personenbezogenen Daten schützen. Google selbst bietet viele Möglichkeiten, um dieses Risiko zu vermindern. Dabei handelt es sich um die Wahlmöglichkeiten bezüglich des Datenschutzes in den einzelnen Diensten. Dementsprechend kann man nach einigen Dienst-Konfigurationen relativ unbeschwert in den Genuss vieler Google-Dienste und -Produkte kommen. Diesbezüglich mangelt es leider noch an einer Aufklärung und Sensibilisierung der Nutzer, denn die meisten von ihnen nehmen diese Wahlmöglichkeiten nicht wahr. Das liegt aber auch daran, dass die Gefahren bei der Nutzung von Google-Diensten nicht gerade offensichtlich sind und „im Hintergrund lauern". Das führt zu einer Unterschätzung des Risikos. Die Eintrittswahrscheinlichkeiten der einzelnen Risiken sind schwer absehbar und schlecht einschätzbar, da sie von vielen Faktoren abhängen. Daher ist Vorsicht geboten, bevor es vielleicht irgendwann zu spät sein könnte. Man sollte es also gar nicht erst soweit kommen lassen.

Nutzer sollten wissen, dass der Schutz ihrer personenbezogenen Daten generell wichtig ist, dass sie bei der Nutzung von Google's Diensten tendenziell sehr viele persönliche Informationen preisgeben und dass die Möglichkeit besteht, nicht in einen Zwiespalt zu geraten. Dieser lautet: Entweder Google-Dienste nutzen oder Privatsphäre und informationelle Selbstbestimmung aufrecht zu erhalten. Wenn Nutzer sich dessen bewusst sind, dann fehlt eigentlich nur noch ein Leitfaden bzw. Nachschlagewerk, in dem verzeichnet ist, wo besondere Gefahren lauern und welcher Dienst wie und wo konfiguriert werden muss, aber auch welcher Dienst lieber nicht genutzt werden sollte. Auch die weiteren Maßnahmen zur Risikoverminderung beim Umgang mit dem Google-Konto sollten berücksichtigt werden, genau wie beispielsweise auch die Add-ons für Webbrowser, um ein Tracking des eigenen Verhaltens im Internet zu verhindern.

Ich selbst bin mir ziemlich sicher, dass Google jetzt, nachdem ich die Dienste und Produkte getestet habe, nicht mehr über mich weiß, als vorher auch. Denn außer IP-Adressen und Cookie-IDs, die in Verbindung mit weiteren Informationen zu meiner Identität führen könnten, wurden keine personenbezogenen Daten preisgegeben. Daten, die auf dieser Basis erhoben wurden, sind mit Sicherheit in den Protokolldateien von Google erfasst. Außerdem wurden natürlich viele Informationen mit dem Google-Konto, das für Testzwecke angelegt wurde, verknüpft (siehe Anhang A). Dabei handelte es sich aber weder um persönliche noch um andere sensible Daten. Das Google-Konto ist also nicht unmittelbar mit meiner wahren Identität verbunden (außer vielleicht jetzt durch diese Ausarbeitung), könnte aber vielleicht mit IP-Adressen und Cookie-IDs verknüpft worden sein. Basis für diese Sparsamkeit bei der Preisgabe der eigenen Daten waren eine gewisse Grundeinstellung zum Datenschutz und sehr viel Recherche. Die ausführlichen Tests und das Recherchieren waren zwingend erforderlich, da ein entsprechender Leitfaden bisher fehlte. Allerdings stellt diese Ausarbeitung keinen vollständigen Leitfaden dar, sondern lediglich einen ersten Ansatz. Ein solcher Leitfaden wäre natürlich umfangreicher, da im Rahmen dieser Ausarbeitung nicht alle Dienste und die genauen Zusammenhänge sowie weitere Aspekte berücksichtigt werden konnten. Außerdem müsste ein Leitfaden stets aktuell gehalten werden, denn bei Google ändert sich (fast) täglich irgendetwas. Seien es neue Dienste, neue Nutzungs-

und Datenschutzbestimmungen etc. Dementsprechend ist es unmöglich, eine Ausarbeitung über Google und seine Dienste zu verfassen, die zum Zeitpunkt der Abgabe bzw. Veröffentlichung immer noch aktuell ist. In der Thematik ist so viel Bewegung, dass sich inzwischen mit Sicherheit irgendwelche inhaltliche Änderungen ergeben haben. Dies sollte berücksichtigt werden.

Dass Google die Daten seiner Nutzer braucht, um Geld zu verdienen, wurde im Laufe dieser Ausarbeitung deutlich. Eine interessante Frage wäre, was aus Google wird, wenn nun wirklich alle seine Nutzer aufgeklärt und sensibilisiert sind. Angenommen, alle Nutzer würden die Opt-out-Wahlmöglichkeiten nutzen. Wäre dann nicht das Geschäftsmodell von Google gefährdet? Müsste Google dann für die Nutzung seiner Dienste Geld nehmen? Würden Innovation und Qualität darunter leiden? Könnte Google persönliche Daten dann heimlich erheben? Oder würde Google vielleicht nur die Wahlmöglichkeiten streichen, um die Datenschützer und andere Kritiker so hart kämpfen mussten und einen „Krieg" in neuer Dimension entfachen? Bis dahin ist es allerdings noch ein weiter Weg.

Es soll noch einmal deutlich gemacht werden, dass es in dieser Ausarbeitung nicht darum ging, einzig und allein Google an den Pranger zu stellen und als „das Böse" der Internetökonomie zu outen. Allerdings sind die Gefahren bei Google besonders groß, da Google auf die personenbezogenen Daten wie kein anderer angewiesen ist und sich mit seinen vielen Diensten und Nutzern im Internet und auch in der Realwelt sehr breit macht und enorm viele Daten sammelt. Auch wenn die Daten bei Google augenscheinlich sicher aufgehoben sind, sollte man sich immer fragen, wie sicher sie dort, bei einem Wirtschaftsunternehmen, wirklich sind und was, wenn auf einmal jeder bzw. die falschen Leute Zugriff auf sie hätten. Dass Google in den Medien so viel Aufmerksamkeit auf sich zieht und Kritik erntet ist wohl auch die Bürde eines Marktführers, der massenweise personenbezogene Daten sammelt und sich zugleich selbst darauf verpflichtet, nichts Böses zu tun. „Don't be evil" lautet nämlich Google's Motto in seiner Unternehmensphilosophie. Man könnte dies aber auch als eine Art Drohung an den Nutzer interpretieren: „Tue nichts Böses, denn wir werden es erfahren!".

Ein weiteres Thema, wenn es darum geht, sich der Datensammelei im Internet allgemein zur Wehr zu setzen, ist Datenschutz durch Technikgestaltung. Dabei sollen entsprechende Schutzmechanismen in der Technik verankert werden und der Datenschutz auf dieser Ebene sichergestellt werden. Die Technik soll es also ermöglichen, automatisch auf Gefährdungen zu reagieren. Diesbezüglich hat Stefan Willenbrock im Jahr 2009 eine Bachelorarbeit verfasst, die mit dem Wissenschaftspreis des Landesbeauftragten für Datenschutz des Landes Rheinland-Pfalz ausgezeichnet worden ist. Ein Verweis auf die Arbeit ist im Literaturverzeichnis zu finden (Willenbrock 2009). Prof. Dr. Roßnagel zeigte bei der Preisrede die Notwendigkeit des Zusammenwirkens von Technik und Recht auf. Er ist der Meinung, dass informationelle Selbstbestimmung momentan nur der ausüben könne, der kein Nutzer des Internets ist. Er verlangt eine Überarbeitung des Datenschutzes, denn das jetzige Datenschutzkonzept würde grundlegend in jedem seiner Bestandteile in Frage gestellt und zwar dadurch, dass Ubiquitous Computing (die allgegenwertige IT) den Betroffenen nicht aufgedrängt wird, sondern von diesen gewollt ist. „Sie werden dann als Konsequenz auch damit einverstanden sein müssen, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten" (Roßnagel 2009).

Was aus Google in der Zukunft wird, ist vollkommen offen und bleibt spannend. Google's Dominanz ist groß, ebenso groß sind die Abhängigkeiten von den Nutzern und den Geschäftskunden. Kritiker und Gegner gibt es mehr als genug, darunter auch politische. Die Konkurrenz ist ernst zu nehmen, auch wenn es in der Vergangenheit oft nicht danach aussah. Außerdem ist die Internetökonomie von Trends gekennzeichnet. Seit einigen Jahren sind soziale Netzwerke der Trend bei den Nutzern. Soziale Netzwerke sind momentan bei der Personalisierung im Internet richtungsweisend. Große soziale Netzwerke, allem voran Facebook, blühen seit einiger Zeit unaufhörlich auf und Investitionen schlagen sich gerade erst in Gewinne nieder, so wie es bei Google vor zehn Jahren der Fall war.

Literaturverzeichnis

Alexa, 2010: Site Info of orkut.com. http://www.alexa.com/siteinfo/Orkut.com# (Zugriff am 11. Januar 2011).

AlpaxX GmbH & Co. KG, 2010: *Google auch 2010 wertvollste Marke der Welt.* http://www.topnews.de/google-auch-2010-wertvollste-marke-der-welt-386670 (Zugriff am 28. August 2010).

Angelova, K. / Yarow, J., 2010: *How Long Until Facebook Passes Google In Traffic?* http://www.businessinsider.com/chart-of-the-day-google-facebook-unique-visitors-2010-8 (Zugriff am 8. September 2010).

Artikel-29-Datenschutzgruppe 2008: *Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen.* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_de.pdf (Zugriff am 11. Januar 2011).

Baun, C. / Kunze, M. / Nimis, J. / Tai, S., 2010: *Cloud Computing - Web-basierte dynamische IT-Services.* Hrsg.: Günther, O. / Karl, W. / Lienhart, R. / Zeppenfeld, K. Bd.: Informatik im Fokus. Berlin: Springer Verlag.

Biermann, K., 2009: *Datenschutz auf Google-Art.* http://www.zeit.de/digital/datenschutz/2009-11/google-dashboard-datenschutz?page=2 (Zugriff am 17. August 2010).

Bogatin, D., 2006: *Google CEO's new paradigm: 'cloud computing and advertising go hand-in-hand'.* http://www.zdnet.com/blog/micro-markets/google-ceos-new-paradigm-cloud-computing-and-advertising-go-hand-in-hand/369 (Zugriff am 17. August 2010).

Bonstein, J. / Rosenbach, M. / Schmundt, H., 2008: *Data Mining You to Death - Does Google Know Too Much?* http://www.spiegel.de/international/germany/0,1518,587546,00.html (Zugriff am 17. August 2010).

Brandt, R.-L., 2010: *Googles kleines Weißbuch - Die Managementstrategien der wertvollsten Marke der Welt.* München: FinanzBuch Verlag GmbH.

Braun, H., 2010: *Ein bisschen Datenschutz für Google Analytics.* http://www.heise.de/netze/meldung/Ein-bisschen-Datenschutz-fuer-Google-Analytics-Update-1007307.html (Zugriff am 17. August 2010).

Breyer, P., 2008: *Fälle von Datenmissbrauch und -irrtümern.* http://www.daten-speicherung.de/index.php/faelle-von-datenmissbrauch-und-irrtuemern/ (Zugriff am 11. Januar 2011).

Brownlow, Mark, 2010: *Email and webmail statistics.* http://www.email-marketing-reports.com/metrics/email-statistics.htm (Zugriff am 28. August 2010).

Bundesamt für Sicherheit in der Informationstechnik, 2009: *Lagebericht 2. Quartal 2009.* https://www.bsi.bund.de/cae/servlet/contentblob/621516/publicationFile/38045/Quartalslagebericht_2_2009_pdf.pdf (Zugriff am 17. August 2010).

Bündnis 90/Die Grünen 2011*: Daten schützen - Unterwegs im Netz: Suchmaschinen.* https://www.datenschutz-ist-buergerrecht.de/was-geschieht-mit-deinen-daten/unterwegs-im-netz/suchmaschinen (Zugriff am 11. Januar 2011).

Büttner, K., 2010: *Bezahlsystem Google Checkout geht an den Start.* http://www.online-marketing-praxis.de/wissen/checkout.php (Zugriff am 17. August 2010).

Cloes, R. / Schappert, C., 2009: *Das Für und Wider der urheberrechtlichen Diskussion im Zusammenhang mit dem „Heidelberger Appell" - Google Buchsuche und Open Access.* http://www.bundestag.de/dokumente/analysen/2009/heidelbergerappell.pdf (Zugriff am 17. August 2010).

CloudTweats, 2010: *Google Data Center in 1997 and Now… 2010 – Data Domination?* http://www.cloudtweaks.com/2010/02/google-data-center-in-1997-and-now-2010-data-domination/ (Zugriff am 28. August 2010).

CNN, 2010: *Global 500 - Our annual ranking of the world's largest corporations.* http://money.cnn.com/magazines/fortune/global500/2010/full_list/index.html (Zugriff am 28. August 2010).

Dahlmann, D., 2007: *Onlinefotoalben im VergleichLocr, Woophy und Panoramio: Fotos mit Geodaten.* http://www.focus.de/digital/foto/tid-6943/digitalbilder_aid_67820.html (Zugriff am 11. Januar 2011).

Dambeck, H., 2006: *Sieben Millionen Erfindungen - Google startet Patentsuche.* http://www.spiegel.de/netzwelt/tech/0,1518,454592,00.html (Zugriff am 11. Januar 2011).

Dean, J. / Ghemawat, S., 2009: *MapReduce: Simplified Data Processing on Large Clusters.* http://static.googleusercontent.com/external_content/untrusted_dlcp/labs.google.com/en//papers/mapreduce-osdi04.pdf (Zugriff am 1. September 2010).

Debatin, S., 2010: *Google Goggles - Google Suche mal ganz anders!* http://knol.google.com/k/stefan-debatin/google-goggles/1srjjkdqab52y/2 (Zugriff am 17. August 2010).

Diederichs, F., 2010: *Im Griff des Daten-Kranken: Google will über Menschen alles wissen - und am liebsten nach Belieben steuern.* Bocholter-Borkener Volksblatt vom 21. August 2010.

Dirscherl, H.-C., 2010: *Tolle Gratis-Navi-App - Google Maps Navigation im Test.* http://www.pcwelt.de/start/mobility_handy_pda/navigation/tests/2345045/google-maps-navigation-im-test/ (Zugriff am 17. August 2010).

Dreuw, J., 2010: *Street-View-Start - Google schließt Pannen nicht aus.* http://www.focus.de/digital/internet/google/street-view-start-google-schliesst-pannen-nicht-aus_aid_572261.html (Zugriff am 11. Januar 2011).

Fischer, S., 2010: *Aigner feiert Vier-Wochen-Erfolg gegen Google.* http://www.spiegel.de/politik/deutschland/0,1518,712754,00.html (Zugriff am 11. Januar 2011)

Fenselau, C., 2010: *Datenschützer: Google weist Schwarzsurfern den Weg.* http://computer.t-online.de/google-wlan-daten-laden-schwarzsurfer-ein/id_41424588/ (Zugriff am 17. August 2010).

Fernsehen in Dresden, 2010: *Mit Street View quer durch Dresden - Google stellt die 20 größten Städte online.* http://www.dresden-fernsehen.de/default.aspx?ID=6090&showNews=887060 (Zugriff am 11. Januar 2011).

Garstka, H., 2003: *Informationelle Selbstbestimmung und Datenschutz - Das Recht auf Privatsphäre.* Erschienen in: Schulzki-Haddouti, C., 2003: *Bürgerrechte im Netz.* Wiesbaden: VS Verlag.

Google Inc., 2008: *Panoramio Privacy Notice.* http://www.panoramio.com/privacy/ (Zugriff am 11. Januar 2011).

Google Inc., 2009: *On yesterday's email.* http://googledocs.blogspot.com/2009/03/on-yesterdays-email.html (Zugriff am 17. August 2010).

Google Inc., 2010a: *Google Werbeprogramme.* http://www.google.de/intl/de/ads/ (Zugriff am 17. August 2010).

Google Inc., 2010b: *Google-Konten: Ist das alles?* http://www.google.com/support/accounts/bin/answer.py?hl=de&answer=162743 (Zugriff am 17. August 2010).

Google Inc., 2010c: *Info zum Webprotokoll: Grundlagen.* http://www.google.com/support/accounts/bin/answer.py?hl=de&answer=54068 (Zugriff am 7. September 2010).

Google Inc., 2010d: *Google-Konten - Informationen zum Dashboard.* http://www.google.com/support/accounts/bin/answer.py?hl=de&answer=162744 (Zugriff am 17. August 2010).

Google Inc., 2010e: *Google Sync für Ihr Handy.* http://www.google.de/mobile/sync/ (Zugriff am 17. August 2010).

Google Inc., 2010f: *Google Maps Navigation (Beta).* http://www.google.de/intl/de/mobile/navigation/ (Zugriff am 17. August 2010).

Google Inc., 2010g: *Google Mobile-Datenschutzbestimmungen.* http://www.google.de/mobile/privacy.html (Zugriff am 17. August 2010).

Google Inc., 2010h: *WiFi data collection: An update.* http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html (Zugriff am 17. August 2010).

Google Inc., 2010i: *Google Analytics: Funktionen für Unternehmen stehen auf der erstklassigen Plattform von Google bereit.* http://www.google.com/intl/de/analytics/features.html (Zugriff am 17. August 2010).

Google Inc., 2010j: *Über die Google Buchsuche.* http://books.google.de/googlebooks/about.html (Zugriff am 17. August 2010).

Google Inc., 2010k: *Google Checkout Datenschutzbestimmungen.* http://checkout.google.com/files/privacy.html?hl=de (Zugriff am 17. August 2010).

Google Inc., 2010l: *Google Checkout: Datenschutzrichtlinien.* https://checkout.google.com/support/bin/answer.py?hl=de&answer=39332 (Zugriff am 17. August 2010).

Google Inc., 2010m: *Google Checkout: Konto und Überprüfung.* https://checkout.google.com/support/bin/answer.py?hl=de&answer=105406 (Zugriff am 17. August 2010).

Google Inc., 2010n: *Google Chrome - Anmerkung zum Datenschutz.* http://www.google.com/chrome/intl/de/privacy.html (Zugriff am 7. September 2010).

Google Inc., 2010o: *Google Desktop - Häufig gestellte Fragen zum Datenschutz.* http://desktop.google.de/de/privacyfaq.html (Zugriff am 17. August 2010).

Google Inc., 2010p *Datenschutz-Center: Datenschutzbestimmungen.* http://www.google.com/intl/de/privacypolicy.html (Zugriff am 11. Januar 2011).

Google Inc., 2010q: *Google Earth - Datenschutz: Art der verfügbaren Daten.* http://earth.google.de/support/bin/answer.py?hl=de&answer=21413 (Zugriff am 17. August 2010).

Google Inc., 2010r: *Google Earth - Datenschutz: Informationen über Nutzungsstatistiken.* http://earth.google.de/support/bin/answer.py?hl=de&answer=40936 (Zugriff am 17. August 2010).

Google Inc., 2010s: *Picasa: Anmerkung zum Datenschutz.* http://picasa.google.com/intl/de/privacy.html (Zugriff am 17. August 2010).

Google Inc., 2010t: *Picnik: Datenschutzbestimmungen.* http://www.picnik.com/info/privacypolicy2 (Zugriff am 17. August 2010).

Google Inc., 2010u *Google-Konten: Profile.* http://www.google.com/support/accounts/bin/topic.py?topic=14962 (Zugriff am 17. August 2010).

Google Inc., 2010v: *Über Google Scholar.* http://scholar.google.de/intl/de/scholar/about.html (Zugriff am 17. August 2010).

Google Inc., 2010w: *Google Talk - Anmerkung zum Datenschutz.* http://www.google.com/talk/intl/de/privacy.html (Zugriff am 17. August 2010).

Google Inc., 2010x: *Google Text & Tabellen - Zusätzliche Nutzungsbedingungen.* http://www.google.com/google-d-s/intl/de/addlterms.html (Zugriff am 17. August 2010).

Google Inc., 2010y: *Google Text & Tabellen - Datenschutzbestimmungen.* http://www.google.com/google-d-s/intl/de/privacy.html (Zugriff am 17. August 2010).

Google Inc., 2010z: *Installieren oder deinstallieren: Google Toolbar - Anmerkung zum Datenschutz.* http://www.google.com/support/toolbar/bin/answer.py?hl=de&answer=81841&rd=2 (Zugriff am 17. August 2010).

Google Inc., 2011a: *Google Base-Hilfe - Grundlagen.* http://base.google.de/support/bin/topic.py?hl=de&topic=2904 (Zugriff am 11. Januar 2011).

Google Inc., 2011b: *Google Base-Hilfe - Überblick über den Feed-Prozess.* http://base.google.com/support/bin/answer.py?hl=de_DE&answer=59537 (Zugriff am 11. Januar 2011).

Google Inc., 2011c: *Blogger-Funktionen.* http://www.blogger.com/features (Zugriff am 11. Januar 2011).

Google Inc., 2011d: *Anmerkung zum Datenschutz in Blogger.* http://www.blogger.com/privacy (Zugriff am 11. Januar 2011).

Google Inc., 2011e: *Google Groups - Nutzungsbedingungen.* http://groups.google.com/intl/de/googlegroups/terms_of_service3.html (Zugriff am 11. Januar 2011).

Google Inc., 2011f: *Google Groups - Anmerkung zum Datenschutz.* *http://groups.google.com/intl/de/googlegroups/privacy3.html* (Zugriff am 11. Januar 2011).

Google Inc., 2011g: *Weitere Informationen über Google Kalender.* http://www.google.com/intl/de/googlecalendar/about.html (Zugriff am 11. Januar 2011).

Google Inc., 2011h: *Knol - Datenschutzbestimmungen.* http://knol.google.com/k/datenschutzbestimmungen# (Zugriff am 11. Januar 2011).

Groll, T., 2010: *Datenmissbrauch - Meine Identität gehört mir!* http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung (Zugriff am 11. Januar 2011).

Hiner, J., 2010: *Google exec: 60% of businesses could dump Windows for Chrome OS.* http://www.zdnet.com/blog/btl/google-exec-60-of-businesses-could-dump-windows-for-chrome-os/42141 (Zugriff am 7. Januar 2011).

Hesselbach, M., 2009: *Android - Revolutioniert Google die Handywelt?* http://knol.google.com/k/android (Zugriff am 17. August 2010).

Hoffman, J.-E. / Myllymaki, J., 2010: *Finding places "Near me now" is easier and faster than ever on Google.com.* http://googlemobile.blogspot.com/2010/01/finding-places-near-me-now-is-easier.html (Zugriff am 17. August 2010).

Ihlenfeld, J., 2009: *Videotour durch ein Google-Rechenzentrum.* http://www.golem.de/0904/66376.html (Zugriff am 28. August 2010).

Intac, 20010: *A Comparison of Dedicated Servers By Company.* http://www.intac.net/a-comparison-of-dedicated-servers-by-company_2010-04-13/ (Zugriff am 28. August 2010).

Jäger, M., 2006: *Google Code als Alternative zu Sourceforge.net.* http://www.tecchannel.de/kommunikation/news/52915/google_code_als_alternative_zu_sourceforgenet/ (Zugriff am 17. August 2010).

Kappes, C., 2010: *Gedanken zu Google Street View.* http://carta.info/23941/gedanken-zu-google-street-view/ (Zugriff am 17. August 2010).

Kaumanns, R. / Siegenheim, V., 2009: *Die Google Ökonomie - Wie der Gigant das Internet beherrschen will.* Düsseldorf: Books on Demand GmbH.

Kaumanns, R. / Siegenheim, V., 2008: *Von der Suchmaschine zum Werbekonzern - Googles Ambitionen für ein crossmediales Werbenetzwerk.* http://www.accenture.com/NR/rdonlyres/A8EB26F4-BF55-45D1-B234-1C1EEE78A6AA/0/Accenture_Google_Von_der_Suchmaschine_zum_Werbekonzern.pdf (Zugriff am 17. August 2010).

Knobel, R., 2010: *Windows 8 - genial oder gefährlich?* http://www.tagesanzeiger.ch/digital/computer/Windows-8--genial-oder-gefaehrlich/story/13847398 (Zugriff am 29. Dezember 2010).

Kolokythas, P., 2008: *Kill-ID für Chrome - Anti-Schnüffeltool in neuer Version.* http://www.pcwelt.de/news/Kill-ID-fuer-Chrome-Anti-Schnueffeltool-in-neuer-Version-252363.html (Zugriff am 20. Januar 2011).

Kraska, S., 2008a: *Google-Chrome - die Intention liegt auf der Hand.* http://www.datenschutzbeauftragter-online.de/google-chrome-die-intention-liegt-auf-der-hand/ (Zugriff am 17. August 2010).

Kraska, S., 2008b: *Google Maps als Kundenauswahl?* http://www.datenschutzbeauftragter-online.de/google-maps-als-kundenauswahl/ (Zugriff am 17. August 2010).

Kraska, S., 2010: *Datenschutz-Artikel hier zu Google-Analytics.* http://www.datenschutzbeauftragter-online.de/datenschutz-artikel-hier-zu-google-analytics/ (Zugriff am 17. August 2010).

Kretschmann, T., 2009: *Google wehrt sich gegen BSI-Kritik an Wave.* http://www.tomshardware.de/Wave-Google-BSI-Datenschutz,news-243460.html (Zugriff am 17. August 2010).

Kuhn, J., 2010: *Google TV: Wie Google Glotze und Netz verschmelzen will.* http://www.sueddeutsche.de/digital/google-tv-wie-google-glotze-und-netz-verschmelzen-will-1.945808 (Zugriff am 17. August 2010).

Kuhr, D., 2010: *Bilder-Dienst Street View: Bürger sagen Google den Kampf an.* http://www.sueddeutsche.de/digital/netzneutralitaet-buerger-wehren-sich-gegen-google-street-view-1.988416 (Zugriff am 17. August 2010).

Labs, L., 2010: *Google: 200.000 Androiden pro Tag.* http://www.heise.de/newsticker/meldung/Google-200-000-Androiden-pro-Tag-1051145.html (Zugriff am 17. August 2010).

Lanzerath, C., 2010: *Google Android - so spioniert das Handy-Betriebssystem: Big Google is watching you.* http://www.chip.de/artikel/Google-Android-so-spioniert-das-Handy-Betriebssystem_41132429.html (Zugriff am 17. August 2010).

Lemm, K., 2010: *Soziale Netzwerke: GMail + Twitter + Facebook = Google Buzz.* http://www.stern.de/digital/online/soziale-netzwerke-gmail-twitter-facebook-google-buzz-1542283.html (Zugriff am 17. August 2010).

M., Valdivia A. / López-Alcalde J. / Vicente M. / Pichiule M. / Ruiz M. / Ordobas, M., 2010: *Monitoring influenza activity in Europe with Google Flu Trends: comparison with the findings of sentinel physician networks.* http://www.eurosurveillance.org/images/dynamic/EE/V15N29/art19621.pdf (Zugriff am 17. August 2010).

MDR, 2010: *Warum scannt Google WLAN-Netze?* http://www.mdr.de/mdr-info/7272942.html (Zugriff am 17. August 2010).

Miller, R., 2008: *Google Data Center FAQ.* http://www.datacenterknowledge.com/archives/2008/03/27/google-data-center-faq/ (Zugriff am 28. August 2010).

Miller, R., 2009: *Who Has the Most Web Servers?* http://www.datacenterknowledge.com/archives/2009/05/14/whos-got-the-most-web-servers/ (Zugriff am 28. August 2010).

N-TV, 2010: *Keine Privatsphäre bei Buzz - Google steuert gegen.* http://www.n-tv.de/technik/Google-steuert-gegen-article809464.html (Zugriff am 17. August 2010).

Pieper, C., 2008: *Krankendaten bei Google speichern? In den USA sind digitale Krankenakten im Kommen.* http://www.aerztezeitung.de/praxis_wirtschaft/telemedizin/?sid=500981 (Zugriff am 17. August 2010).

Pingdom AB, 2010: *Google facts and figures.* http://royal.pingdom.com/2010/02/24/google-facts-and-figures-massive-infographic/ (Zugriff am 28. August 2010).

Pingdom AB, 2008: *Map of all Google data center locations.* http://royal.pingdom.com/2008/04/11/map-of-all-google-data-center-locations/ (Zugriff am 28. August 2010).

Pluta, W., 2010a: *Neue Klage gegen Googles Buchangebot - US-Fotografen klagen wegen Urheberrechtsverletzung in gescannten Büchern.* http://www.golem.de/1004/74347.html (Zugriff am 17. August 2010).

Pluta, W., 2010b: *Buzz-Opfer: Wie nutzte Obamas Vize-CTO sein Mailkonto?* http://www.golem.de/1004/74420.html (Zugriff am 17. August 2010).

Rheinische Post Online, 2009: *Massive Sicherheitspanne: Google Docs lässt fremde Nutzer mitlesen.* http://www.rp-online.de/digitale/internet/Google-Docs-laesst-fremde-Nutzer-mitlesen_aid_771753.html (Zugriff am 17. August 2010).

Roßnagel, A., 2009: *Modernisierung des Datenschutzes.* http://www.datenschutz.rlp.de/de/wissenschaftspreis/bisherige_arbeiten/2009_Preisrede_Prof_Rossnagel.pdf (Zugriff am 19. Januar 2011).

Sagawe, A., 2009: *Das Google Phänomen - Im Spiegel des Mikropolis-Modells.* http://agis-www.informatik.uni-hamburg.de/fileadmin/asi/Bachelorarbeiten/Bachelorarbeit_Arno_Sagawe_Das_Google_Phaenomen_im_spiegel_des_mikropolis_modells.pdf (Zugriff am 17. August 2010).

Sander, R., 2010: *Google Street View - Wie widerspreche ich?* http://www.stern.de/digital/online/google-street-view-wie-widerspreche-ich-1592130.html (Zugriff am 17. August 2010).

Schwan, B., 2010a: *Streit um TV-Angebot - Alle gegen Google TV.* http://www.taz.de/1/netz/netzkultur/artikel/1/alle-gegen-google-tv/ (Zugriff am 11. Januar 2011).

Schwan, B., 2010b: *Dienst anonymisiert Google-Nutzung.* http://www.heise.de/newsticker/meldung/Dienst-anonymisiert-Google-Nutzung-991935.html (Zugriff am 11. Januar 2011).

Siegenheim, Veit., 2010: *Pro-Kopf-Umsatz bei Google dreimal so hoch wie bei Yahoo.* http://www.google-oekonomie.de/pro-kopf-umsatz-bei-google-dreimal-so-hoch-wie-bei-yahoo/ (Zugriff am 28. August 2010).

Steinlein, C., 2010: *Datenschutz: Aigner kritisiert Google Buzz.* http://www.focus.de/digital/internet/google/datenschutz-aigner-kritisiert-google-buzz_aid_482344.html (Zugriff am 17. August 2010).

Stern Online, 2010: *Kuriose Fundstücke bei Google Earth: Google sieht dich auch beim Nacktbaden.* http://www.stern.de/digital/online/kuriose-fundstuecke-bei-google-earth-google-sieht-dich-auch-beim-nacktbaden-1551944.html (Zugriff am 17. August 2010).

Stöcker, C., 2009: *Google will die Weltherrschaft.* http://www.spiegel.de/netzwelt/netzpolitik/0,1518,665813,00.html (Zugriff am 17. August 2010).

Stuttgarter Zeitung, 2008: *Google Health: Suchgigant will Gesundheitsdaten speichern.* http://www.stuttgarter-zeitung.de/stz/page/1651370_0_2147_google-health-suchgigant-will-gesundheitsdaten-speichern.html (Zugriff am 17. August 2010).

Tagesschau, 2010: *Datenschützer entsetzt über Google-Street-View - Google erfasst sämtliche WLAN-Netze in Deutschland.* http://www.tagesschau.de/inland/google248.html (Zugriff am 17. August 2010).

Thommes, F., 2010: *Google stellt Notebook CR-48 mit Chrome OS vor*. http://www.pc-magazin.de/news/google-stellt-cr-48-notebook-mit-chrome-os-vor-1039219.html (Zugriff am 4. Januar 2011).

Tikoim, 2009: 10 *Vorteile von Blogspot alias Blogger | Blog-System-Tipps*. http://www.tikoim.de/2009/08/10-vorteile-von-blogspot-alias-blogger.html (Zugriff am 11. Januar 2011)

The Economic Time, 2010: *Twitter snags over 100 million users, eyes money-making*. http://economictimes.indiatimes.com/infotech/internet/Twitter-snags-over-100-million-users-eyes-money-making/articleshow/5808927.cms (Zugriff am 28. August 2010).

Thomi, M., 2009: *Street View: Autonummern vor Bordell erkennbar*. http://www.derbund.ch/digital/internet/Street-View-Autonummern-vor-Bordell-erkennbar/story/25335165 (Zugriff am 17. August 2010).

Tsotsis, A., 2010: *With Great Power Comes Great Responsibility: A Facebook Bill Of Rights.*. http://techcrunch.com/2010/09/07/facebook-bill-of-rights/ (Zugriff am 8. September 2010).

Türk, A., 2010; *Street View startet in Kürze: Tipps zum Melden von Bildern*. http://google-produkt-kompass.blogspot.com/2010/11/street-view-startet-in-kurze-tipps-zum.html (Zugriff am 11. Januar 2011).

Unabhängiges Landesamt für Datenschutz Schleswig-Holstein, 2009: *Google Analytics Services – Webtracking auf dem Prüfstand*. 2009. https://www.datenschutzzentrum.de/material/tb/tb31/kap07.htm#72 (Zugriff am 17. August 2010).

Wandiger, P., 2009: *Google Wave - Die neue Killer-App von Google*. http://www.selbstaendig-im-netz.de/2009/06/11/google/google-wave-die-neue-killer-app-von-google/ (Zugriff am 17. August 2010).

Weber, V., 2010: *Google Wave wird eingestellt*. http://www.heise.de/newsticker/meldung/Google-Wave-wird-eingestellt-1050992.htm (Zugriff am 17. August 2010).

Wikipedia, 2010a: *Datenschutz*. http://de.wikipedia.org/wiki/Datenschutz (Zugriff am 23. August 2010).

Wikipedia, 2010b: *Soziales Netzwerk (Internet)*. http://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet) (Zugriff am 7. September 2010).

Willenbrock, S., 2009: *Engineering Java Byte Code to Detect Implicit Information Flow*. http://www.datenschutz.rlp.de/de/wissenschaftspreis/bisherige_arbeiten/2009_Bachelorarbeit_Willenbrock_Stefan.pdf (Zugriff am 19. Januar 2011).

Witt, B. C., 2010: *Datenschutz kompakt und verständlich*. Wiesbaden: Vieweg+Teubner Verlag.

Worldsites GmbH - Suchmaschinen Marketing Agentur, 2010: *Google macht $ 1,34 Million Umsatz pro Mitarbeiter.* http://news.worldsites-schweiz.ch/google-macht-134-million-umsatz-pro-mitarbeiter.htm (Zugriff am 28. August 2010).

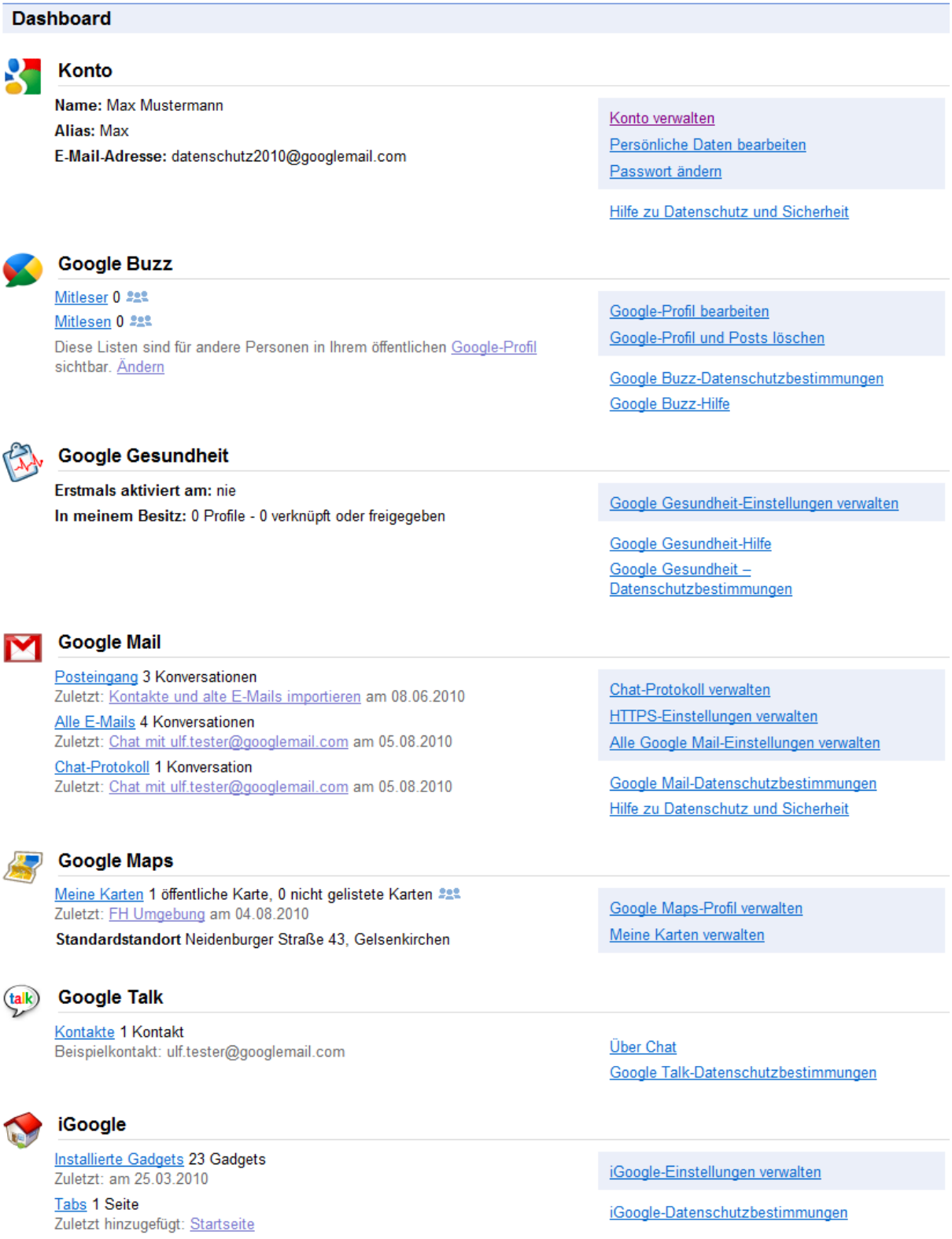
Zeit Online, 2010: *Facebook hat eine halbe Milliarde im Netz.* http://www.zeit.de/digital/internet/2010-07/facebook-mitglieder-zuckerberg (Zugriff am 28. August 2010).

Zeuch, C., 2009: *Robert Koch Institut zu Google's Frühwarnsystem für Influenza.* http://www.altona.info/2009/10/google-bringt-fruhwarnsystem-fur-grippewellen/ (Zugriff am 17. August 2010).

Abbildungsverzeichnis

Abbildung 1: Weitere wirtschaftliche Daten 17
Abbildung 2: Near me Now - Die ortsbezogene Suche 22
Abbildung 3: Ortungshinweis von Google, den man nach dem Latitude-Start per Mail erhält 24
Abbildung 4: Google Navigation auf einem Android-Endgerät 25
Abbildung 5: Google Navigation in der Ansicht "Street View" 26
Abbildung 6: Datenschutzoptionen bei Blogger.com 33
Abbildung 7: Webhistorie für Google Books 34
Abbildung 8: Google Desktop 39
Abbildung 9: Integration von Street View in Google Earth 6 40
Abbildung 10: Google Finanzen 41
Abbildung 11: Das Finanzportfolio im Google Dashboard 42
Abbildung 12: Profil, das bei Knol angezeigt wird 47
Abbildung 13: Google Maps in der Webhistorie 49
Abbildung 14: Datenschutzoptionen bei Orkut 50
Abbildung 15: Der Google-Dienst Panoramio 50
Abbildung 16: Sieger eines Kontests bei Panoramia 51
Abbildung 17: Persönliche Informationen in Google Profiles 53
Abbildung 18: Kontaktinformationen in Google Profiles 53
Abbildung 19: Das Google Profil 54
Abbildung 20: Vertraulichkeit bei Google Talk 56
Abbildung 21: Von Google auf Basis von Cookies abgeleitete, persönliche Interessen 62
Abbildung 22: Verknüpfung des YouTube-Kontos mit dem Google-Konto 62
Abbildung 23: YouTube-Kanal 64
Abbildung 24: Die GUI von Google Chrome OS 66
Abbildung 25: Kontakte bearbeiten 70
Abbildung 26: Kritikpunkte am Volkszählungsurteil 72
Abbildung 27: Repersonalisierung durch Korrelation 79
Abbildung 28: Fehlerhaftes Persönlichkeitsbild durch das Fehlen von Informationen 80
Abbildung 29: Wöchentliche Besucher auf google.com und facebook.com 88
Abbildung 30: Monatliche Google- und Facebook-Besucher von März 2009 bis März 2013 88

Anhang A: Die Google-Webhistorie



Dashboard

Konto

Name: Max Mustermann
Alias: Max
E-Mail-Adresse: datenschutz2010@googlemail.com

Konto verwalten
Persönliche Daten bearbeiten
Passwort ändern

Hilfe zu Datenschutz und Sicherheit

Google Buzz

Mitleser 0
Mitlesen 0
Diese Listen sind für andere Personen in Ihrem öffentlichen Google-Profil sichtbar. Ändern

Google-Profil bearbeiten
Google-Profil und Posts löschen

Google Buzz-Datenschutzbestimmungen
Google Buzz-Hilfe

Google Gesundheit

Erstmals aktiviert am: nie
In meinem Besitz: 0 Profile - 0 verknüpft oder freigegeben

Google Gesundheit-Einstellungen verwalten

Google Gesundheit-Hilfe
Google Gesundheit – Datenschutzbestimmungen

Google Mail

Posteingang 3 Konversationen
Zuletzt: Kontakte und alte E-Mails importieren am 08.06.2010
Alle E-Mails 4 Konversationen
Zuletzt: Chat mit ulf.tester@googlemail.com am 05.08.2010
Chat-Protokoll 1 Konversation
Zuletzt: Chat mit ulf.tester@googlemail.com am 05.08.2010

Chat-Protokoll verwalten
HTTPS-Einstellungen verwalten
Alle Google Mail-Einstellungen verwalten

Google Mail-Datenschutzbestimmungen
Hilfe zu Datenschutz und Sicherheit

Google Maps

Meine Karten 1 öffentliche Karte, 0 nicht gelistete Karten
Zuletzt: FH Umgebung am 04.08.2010
Standardstandort Neidenburger Straße 43, Gelsenkirchen

Google Maps-Profil verwalten
Meine Karten verwalten

Google Talk

Kontakte 1 Kontakt
Beispielkontakt: ulf.tester@googlemail.com

Über Chat
Google Talk-Datenschutzbestimmungen

iGoogle

Installierte Gadgets 23 Gadgets
Zuletzt: am 25.03.2010
Tabs 1 Seite
Zuletzt hinzugefügt: Startseite

iGoogle-Einstellungen verwalten

iGoogle-Datenschutzbestimmungen

Kontakte

Kontakte 2 Einträge

Am häufigsten kontaktiert:
Max Mustermann
ulf.tester@googlemail.com

Kontakte verwalten

Picasa-Webalben

Alias: Max Mustermann
Galerie-URL http://picasaweb.google.com/101138159800740661446
Alben 2 insgesamt: 0 öffentlich, 2 nicht gelistet, 0 nur mit Anmeldung
Zuletzt: images um 16:33
Fotos 2 insgesamt: 0 öffentlich, 2 nicht gelistete Fotos, 0 nur mit Anmeldung

Datenschutzeinstellungen verwalten
Alle Einstellungen für Picasa-Webalben verwalten

Einstellungen für die Sichtbarkeit von Picasa-Webalben
Picasa-Webalben – Datenschutzbestimmungen
Picasa-Webalben-Hilfe

Profil

Über mich 11 Einträge
Name: Max Mustermann
Profil-URL: http://www.google.com/profiles/datenschutz2010
Kontaktdaten
E-Mail: 2 E-Mail-Adressen
Adresse: 2 Adressen

Profil bearbeiten
Weitergabe von Kontaktinformationen verwalten

Über den Zugriff auf Profile und den Datenschutz bei Profilen

Text & Tabellen

Von mir geöffnet 1 Dokument
Zuletzt: Test am 05.08.2010

Dokumente verwalten

Webprotokoll

Webprotokoll Aktiviert nur für Suchanfragen
Web
Zuletzt: test am 05.08.2010
Bilder
Zuletzt: google earth am 30.07.2010
Karten
Zuletzt: Neidenburger Straße, Gelsenkirchen -> M... am 04.08.2010
Bücher
Zuletzt: datenschutz am 29.07.2010

Elemente entfernen oder Webprotokoll leeren
Google Goggles-Suchverlauf deaktivieren

Webprotokoll-Hilfe
Webprotokoll-Datenschutzbestimmungen
Häufig gestellte Fragen zum Datenschutz beim Webprotokoll
Google Goggles - Datenschutzbestimmungen

YouTube

Profileinrichtung
Nutzername: 2010datenschutz
Geschlecht: Männlich
Alter: 109
Gesehene Videos
Favoriten 1 Favorit
Zuletzt: Datenschutz im Internet am 06.08.2010
Abonnements 1 öffentlich
Zuletzt: Datenschutz am 06.08.2010

YouTube-Konto verwalten
Datenschutzeinstellungen verwalten
Aktivität und Freigabe verwalten

YouTube-Datenschutzbestimmungen

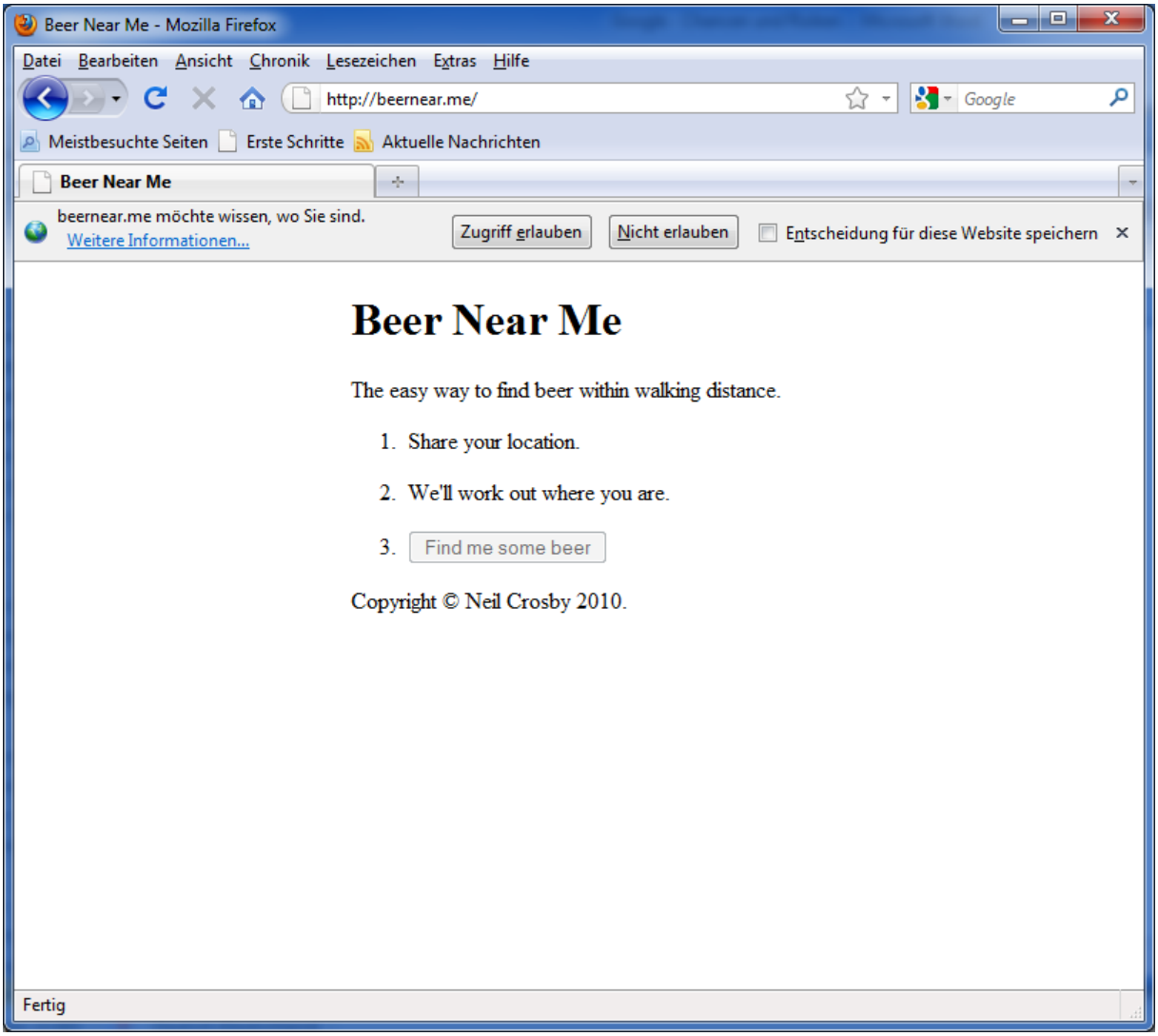
Sonstige Produkte

Die folgenden Produkte sind noch nicht in diesem Dashboard verfügbar.

Google Wave

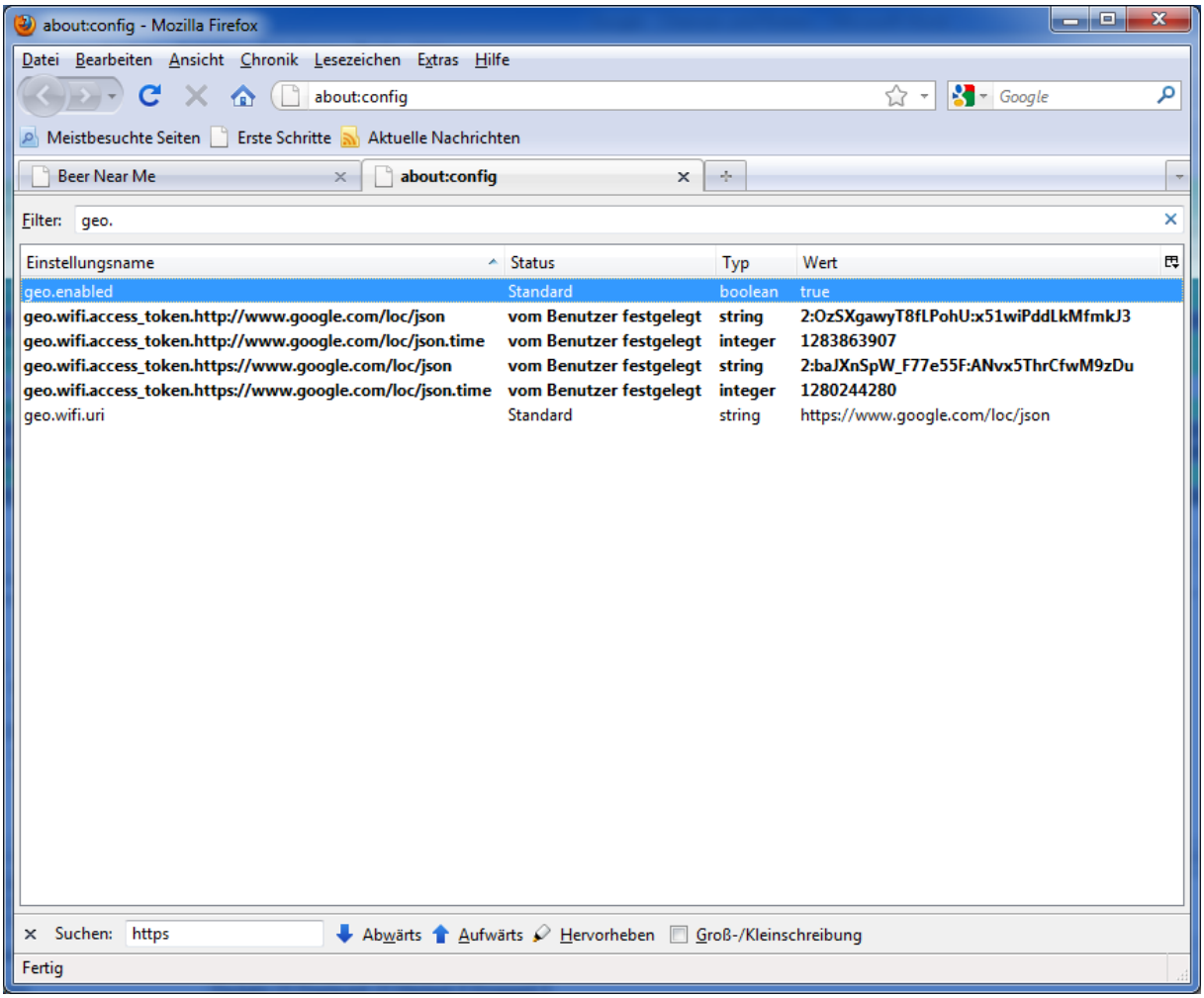
Anhang B: Lokalisierung mit Firefox und der Google Geolocation API

Anhand einer Beispielanwendung soll ein Firefox-Nutzer lokalisiert bzw. geortet und der vollständige Ablauf untersucht werden. Die Lokalisierung mit Firefox funktioniert ab Version 3.5. Basis dafür ist die Google Geolocation API mit der dahinterliegenden WLAN-Datenbank. Bei der Untersuchung war ein Blogeintrag von Denilson Figueiredo de Sá sehr hilfreich, in dem unter anderem beschrieben wurde, wie man die SSL-Verschlüsselung deaktivieren kann, um die Inhalte der Kommunikation zwischen Firefox und der Google Geolocation API einzusehen (http://my.opera.com/CrazyTerabyte/blog/2009/07/23/how-google-firefox-geolocation-api-works). Jede beliebige Webseite kann den Aufenthaltsort eines Firefox-Nutzers nun per JavaScript abfragen. Wer das entsprechende Skript sehen möchte, kann einfach eine Seite aufrufen, die die Lokalisierungs-Funktion nutzt (z.B. www.beernear.me) und sich den Quelltext anzeigen lassen. Im nächsten Schritt fragt Firefox den Nutzer, ob er seinen Aufenthaltsort mitteilen möchte.



Erlaubt man der Webseite (www.beernear.me) den Zugriff, so sendet Firefox einen JSON-Request an die Geolocation API von Google und übermittelt die Messdaten des WLAN-Adapters. Voraussetzung dafür ist natürlich, dass ein entsprechender WLAN-Adapter vorhanden und aktiviert ist. Andernfalls wird nur die IP-Adresse übertragen und die Geolocation API

versucht, anhand dieser Information den ungefähren Aufenthaltsort abzuschätzen. Eine Lokalisierung auf Basis der IP-Adresse ist allerdings sehr unpräzise und ermittelt im besten Fall eigentlich nur die Stadt als Aufenthaltsort. Der entsprechende JSON-Request an die Geolocation API, der die WLAN-Messdaten enthält, soll nun einmal etwas näher betrachtet werden. Dazu wurde die Kommunikation mit Wireshark mitgeschnitten und analysiert. Da die Kommunikation zwischen Firefox und der Geolocation API verschlüsselt ist, muss man die Verschlüsselung sinngemäß deaktivieren.

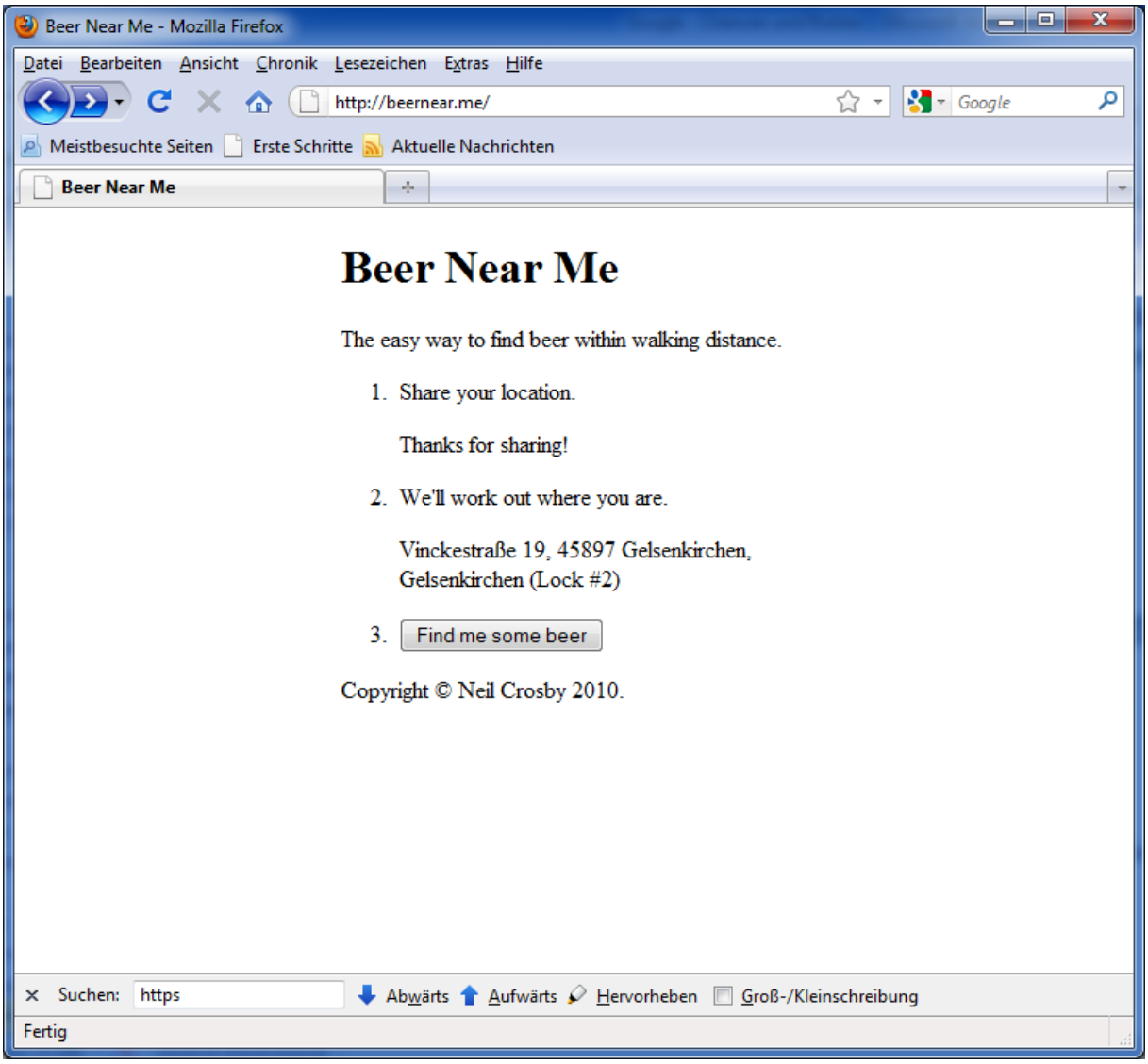


Dazu muss man die Webadresse für die Google Geolocation API anpassen und HTTP statt HTTPS verwenden. Dementsprechend muss der Firefox-Parameter `geo.wifi.uri` von https://www.google.com/loc/json in http://www.google.com/loc/json abgeändert werden. Nun kann man sich die Inhalte des JSON-Request angucken. Interessant sind dabei die Parameter für die Messdaten:

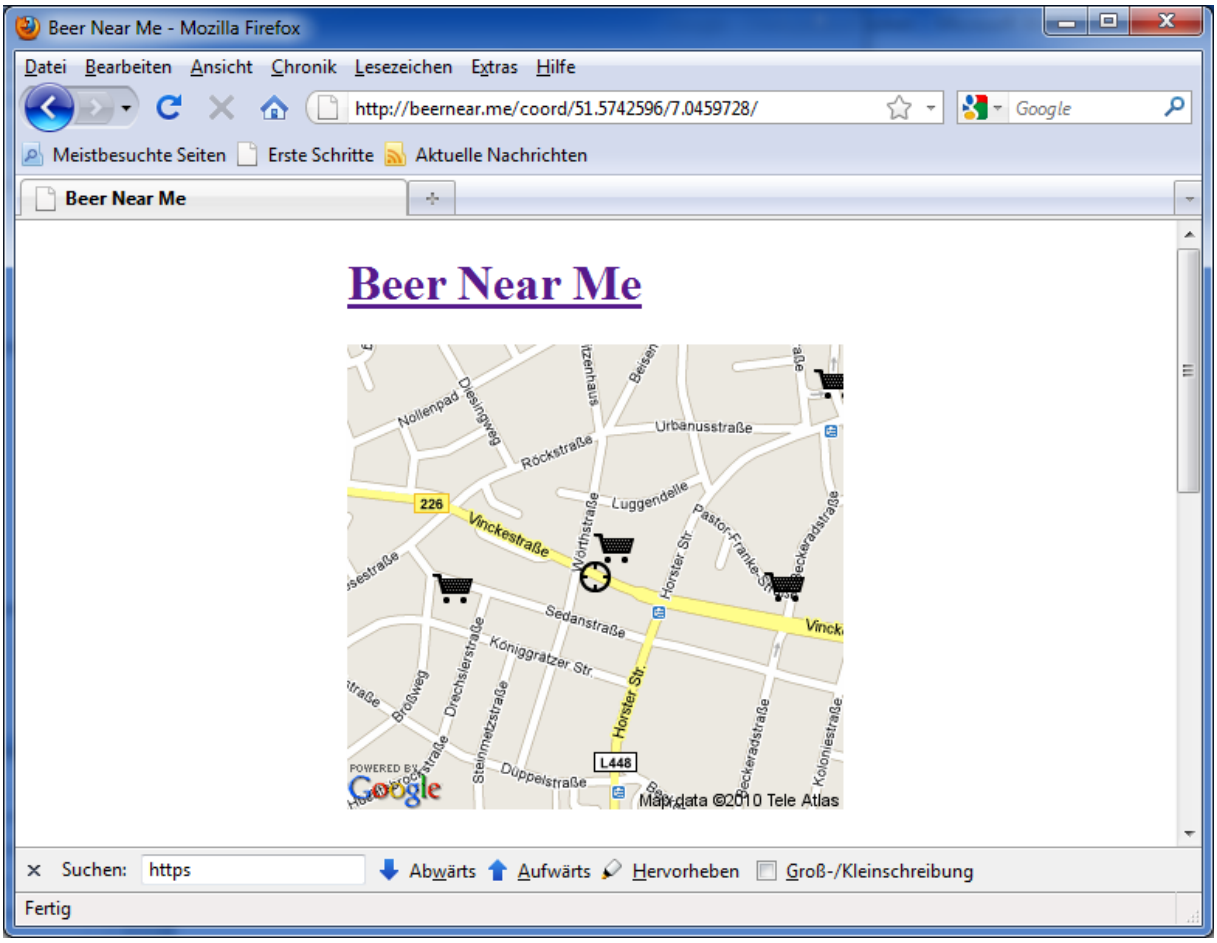
```
"version":"1.1.0",
"request_address":true,
"access_token":"2:aRfVDUMuUHD3h0oX:ZztN0PNaCP4UYmmu",
"wifi_towers":[
        {"mac_address":"00-23-08-c5-18-89","ssid":"EasyBox-XY","signal_strength":-66},
        {"mac_address":"00-1a-2a-1e-a2-71","ssid":"WLAN-123","signal_strength":-84},
        {"mac_address":"00-1f-3f-a0-be-b7","ssid":"AP-0815","signal_strength":-44}
]
```

Der Parameter `wifi_towers` enthält eine Liste mit allen gemessenen WLAN-Netzen in der Umgebung des Endgerätes, auf dem Firefox ausgeführt wird. Dazu gehören die jeweilige MAC-

Adresse, die SSID und die Signalstärke. Die eigentlichen SSIDs wurden hier anonymisiert. Die Geolocation API antwortet nun mit den berechneten Koordinaten zu den übermittelten Messdaten. Diese Daten sendet der Firefox wiederum an die Webseite, die die Lokalisierung initiiert hat (www.beernear.me). Dazu wird eine zuvor definierte URL inkl. entspr. Parameter verwendet: www.beernear.me/data.php?lat=51.574277&lon=7.0459568&accuracy=42. Der erste Parameter enthält den Breitengrad (Latitude = 51,574277), der zweite den Längengrad (Longitude = 7,0459568) und der dritte die Genauigkeit der ermittelten Koordinaten. Die Koordinaten werden weiterverwertet, in dem sie an Google Maps gesendet werden, um die dazugehörige Adresse zu erhalten. Diese wird dann auf der folgenden Seite angezeigt.



Als letzten Schritt kann man sich nun (endlich) das anzeigen lassen, nachdem man gesucht hat. In der Beispielapplikation werden alle Geschäfte angezeigt, in denen man Bier erwerben kann. Diese Suchergebnisse werden auf einer entsprechenden Karte von Google Maps präsentiert. Die Namen und Adressen der gefundenen Geschäfte werden weiter unten auf der Seite angezeigt. Lokalisierungsfunktionalitäten mit der Google Geolocation API sind übrigens auch in Opera und Google Chrome verfügbar.


Beer Near Me - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
http://beernear.me/coord/51.5742596/7.0459728/
Google
Meistbesuchte Seiten
Erste Schritte
Aktuelle Nachrichten
Beer Near Me
Beer Near Me
Nollenpad
Dieslingweg
Röckstraße
Urbanusstraße
Luggendelle
226
Vinckestraße
Horster Str.
Sedanstraße
Königgrätzer Str.
Drechslerstraße
Steinmetzstraße
Düppelstraße
L448
Beckeradstraße
Kolonnenstraße
POWERED BY Google
Map data ©2010 Tele Atlas
Suchen:
https
Abwärts
Aufwärts
Hervorheben
Groß-/Kleinschreibung
Fertig